Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confedraziun svizra

armasuisse
Science and Technology

CYD
CYBER DEFENCE CAMPUS

# Cyber-Defence Campus

## 2023 Annual Report

# Editorial

Dear readers,

2023 was an eventful year for Switzerland in cyberspace. The number of reported cyber incidents increased to almost 50,000 reports. Swiss organisations and authorities were the target of a coordinated DDoS attack in two weeks over the summer. Hackers were able to steal sensitive data from security authorities through the Swiss IT service providers Xplain AG and Concevis. Federal government and the cantons decided on a new National Cyber Strategy (NCS) and the Armed Forces adopted its overall cyber concept as an important milestone in the development of its Cyber Command.

These events underline the importance of our mission at the Cyber-Defence Campus to reinforce cyber security in Switzerland and to help shape the advancing digitalisation of our country. In particular, we are more challenged than ever to anticipate and drive forward the technological developments in the cyber area and, with our knowledge, to strengthen cyber resilience in Switzerland.

We have succeeded in this in several areas this year. Thanks to our numerous events, we contributed to an active exchange and networking of the Swiss cyber community. One of our highlights was our conference on 26 October, at which we welcomed more than 350 participants from industry, the Armed Forces, business, the government and research sectors in Bern in order to drive forward the discourse on the role of artificial intelligence in security. In autumn, we were also able to offer multi-day cyber training sessions on highly topical issues such as the security of the energy sector and the cyber security of cars. These trainings were accompanied by hackathons at which representatives from industry, operators of critical infrastructures, universities and the Armed Forces took part and gained valuable experience.

Numerous innovative start-ups and talented students were incentivised to apply to us this year and take part actively in Swiss cyber defence through our challenges and student programmes. The topic of this year's Cyber Start-up Challenge was the security of smartphones and the company Ostorlab finally won through in the final at the CYD Campus Conference. More than 60 students were given the opportunity to spend several months researching as part of their student research project or internship at the Cyber-Defence Campus and gain their first practical experience on the topic of cyber.

To support the National Cyber Strategy (NCS), we created a new team which focuses on technology monitoring in the cyber area. Under the leadership of this new team, for example, a detailed trend analysis on the technologies for encrypting and protecting data in the digital age was carried out with more than 50 experts from universities and industry, which appeared this year as a book ("Trends in Data Protection and Encryption Technologies"). Other technological and trend analyses in the area of artificial intelligence and quantum technologies are already underway.

This year, our research programmes, which incorporate the contributions of universities and industry, helped to detect new cyber threats and their impact in the area of cyber security and data sciences early on, as well as to develop possible solutions. In 2023, the Cyber-Defence Campus published, together with its partners, more than 80 scientific papers in various disruptive technology areas such as artificial intelligence, generative LLM (large language models), 5G security, the cyber security of space technologies, and the security of future network technologies. Numerous security vulnerabilities in software and devices were also found and reported to the concerned orgnisations.

This year, we went live with our new website with a fresh design at cydcampus.admin.ch. This enables us to provide more prompt and transparent information on our activities and results.

I look forward to presenting you with interesting insights into our daily work and our projects and hope that you will enjoy reading and discovering about the Cyber-Defence Campus.

Thun, December 2023

Dr. Vincent Lenders
Head of Cyber-Defence Campus

# Table of Contents


| | |
|---|---|
| 1. About the Cyber-Defence Campus | 4 |
| 2. Highlights | 10 |
| 3. Students & Fellows | 14 |
| 4. Talent Promotion | 22 |
| 5. Cyber Security | 24 |
| 6. Data Science | 30 |
| 7. Technology Monitoring | 38 |
| 8. Innovation | 46 |
| 9. International Scouting and Cooperations | 50 |
| 10. Customer & Portfolio Assessment | 52 |
| 11. Security Services | 54 |
| 12. Laboratories | 56 |
| 13. Activities | 58 |
| 14. Presentations | 60 |
| 15. Academic papers | 62 |
| 16. Communication | 68 |
| Outlook | 70 |

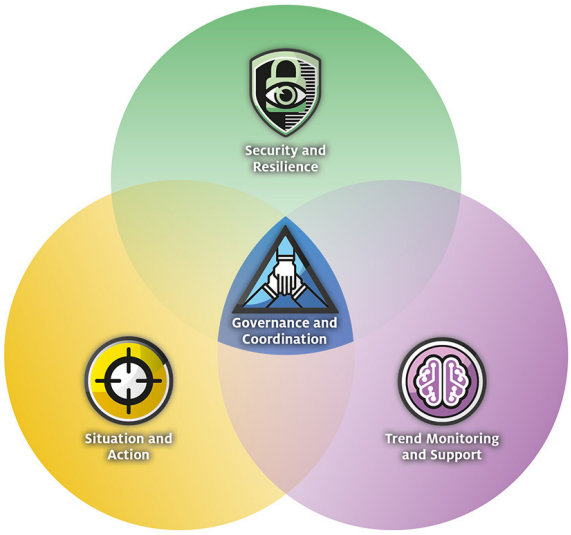

# 1. About the Cyber-Defence Campus

## Strategy and Mission

As a result of the evolving digital ecosystem and the increasing threat of cyber attacks in every aspect of life, the Swiss government has declared cyber security to be a central and national safety issue. The Swiss Federal Department of Defence, Civil Protection and Sport (DDPS) is increasing the use of resources for cyber defence and making it a strategic and operative priority. To this end, the first plan of action for cyber defence (APCD) was created in 2016. In view of the rapid development of the cyber threat situation over the last five years, a new "DDPS Cyber Strategy" was developed for the time period 2021-2024, based on the action plan. Both the action plan and the new "DDPS Cyber Strategy" are aligned with the overarching National Cyber Strategy NCS.

As a part of these strategies, the Cyber-Defence Campus (CYD Campus) has been developed and operated in the DDPS for the last five years. It is part of the Federal Office for Defence Procurement (armasuisse Science and Technology). The CYD Campus offers the DDPS an anticipation and knowledge platform to identify and assess technological, scientific and social cyber trends. In order to be able to work together as closely as possible with universities, the DDPS and industry, the CYD Campus is represented at three locations: At the main location of Thun (armasuisse Science and Technology), in the Innovation Park at EPFL in Lausanne and near ETH in Zurich. This enables it to build efficient know-how and provide cyber expertise according to the needs of the Swiss Confederation.

The CYD Campus functions as a link between industry, public administration and science. According to the "DDPS Cyber Strategy", the Head of the DDPS, Federal Councillor Viola Amherd, defines the areas of activity and the corresponding distribution of tasks.




DDPS Cyber Strategy 2021- 2024

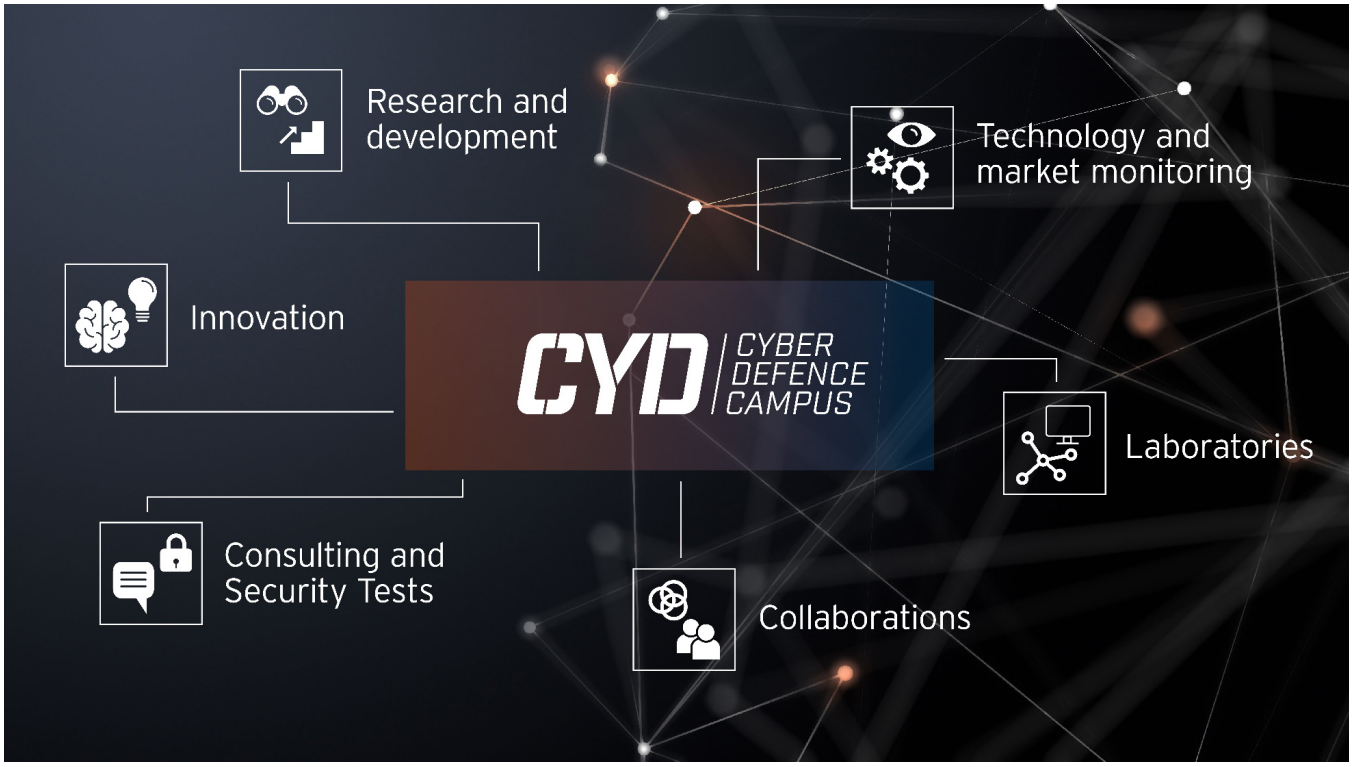
The CYD Campus currently has the following three key tasks:

Early identification of trends in the cyber area: This includes comprehensive technology and market monitoring, international scouting of start-ups and maintaining a cooperation network.

Research and innovation of cyber technologies: Through the cooperation with universities and industry, emerging cyber risks are identified and innovative solutions developed to effectively counter threats in cyberspace. In addition, it is the goal of the CYD Campus to guarantee and increase the security and resilience of existing cyber systems.

Training of cyber specialists: At the CYD Campus, talents are educated at master, PhD and postdoc level, and academic interns are trained for future challenges. In addition, joint cyber training sessions (such as hackathons) are offered.

The goal of this annual report is to grant insights into the implementation of the above-mentioned key tasks of the CYD Campus in 2023. A brief overview of the CYD Campus team as well as some of the highlights of 2023 will be provided. The public activities in research projects, customer orders and demonstrators will also be outlined. The work in 2023 will also be addressed with regard to the expansion of the laboratory infrastructures and the activities of the technology and market monitoring will be presented. In the last chapters of this report, an overview of events, publications, presentations and an outlook for 2024 will be provided.




Core competences of the Cyber-Defence Campus

# Our Partners

## National

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

## International

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

# Faces behind the CYD Campus

## CYD Campus Management

From left to right

**Dr. Colin Barschel**
Head of Innovations and Industry Collaborations

**Giorgio Tresoldi**
Head of International Relations

**Dr. Vincent Lenders**
Head of CYD Campus

**Dr. Bernhard Tellenbach**
Head of Cyber Security

**Dr. Gérôme Bovet**
Head of Data Science

**Dr. Alain Mermoud**
Head of Technology Monitoring

**Stefan Engel**
Head of Business Development and Deputy Head of the CYD Campus

## Project Managers and Experts

**Cédric Aeschlimann**
Cyber Training

**Dr. Albert Blarer**
Data Science

**William Blonay**
Cyber Security

**Dr. Martin Burkhart**
Cyber Security

**Lucas Crijns**
Innovation

**Dr. Ljiljana Dolamic**
Data Science

**Daniel Hulliger**
Cyber Security

**Dr. Julian Jang-Jaccard**
Technology Monitoring

**Dr. Miguel Keer**
Cyber Security

**Dr. Jonas Liechti**
Data Science

**Dr. Raphael Meier**
Data Science

**Dr. Roland Meier**
Cyber Security

**Dr. Daniel Moser**
Cyber Security

**Valentin Mulder**
Technology Monitoring

**Damian Pfammatter**
Cyber Security

**Llorenç Roma**
Cyber Security

**Dr. Hông Ân Sandlin**
Data Science

**Ivo Stragiotti**
Data Science

**Dr. Martin Strohmeier**
Cyber Security

**Dr. Etienne Voutaz**
Data Science

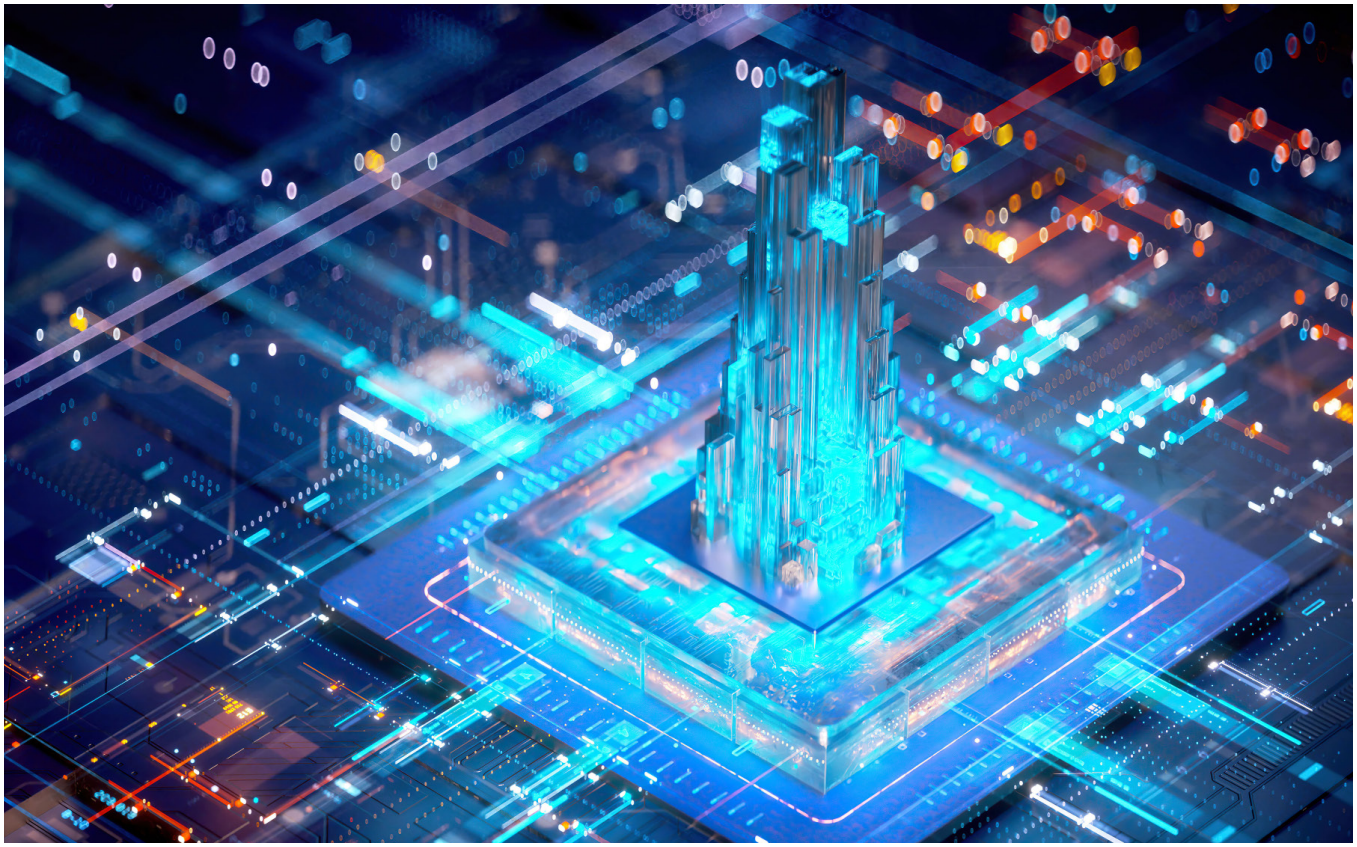
## Support Team

**Yasemin Akin**
Assistance Zurich

**Monia Gieriet**
Head of Administration and
Event Management

**Amina Kabashi**
Assistance Lausanne

**Priska Weber**
Assistance Thun



# 2. Highlights

## CYD Campus Conference on Artificial Intelligence

On 26 October 2023, the CYD Campus organised its annual conference in the Kursaal in Bern. The topic of the conference was "Security in the age of artificial intelligence". More than 350 people took part in the event. The topic is very relevant for the Cyber-Defence Campus as artificial intelligence in cyber security is ubiquitous today. On the one hand, systems can be made more secure by using AI algorithms. Examples of this are the recognition of malware or anomalies in communication networks. On the other hand, artificial intelligence can also present a security risk. Malicious players have the opportunity to influence the behaviour of algorithms for AI in various ways, for example, through data poisoning. To better understand the problems, we have invited various partners from the academic sector and industry to share their views on the subject with us.

The conference began with a presentation from Christophe Nicolas, CIO of the Kudelski Group. As CIO of one of the largest security companies in Switzerland and based on his experience, he offered interesting insights into the sector. He was followed by Juri Ranieri, who showed us how Google combines security and AI in many of its products to make them more secure. Carmela Troncoso from EPFL gave us some insights into data protection in machine learning (ML) – an important challenge in the development of ML systems with personal data. This year, we also offered some of our students the opportunity to present their work in the form of an elevator pitch. We had the honour of welcoming Lieutenant General Thomas Süssli, Chief of the Armed Forces, who presented us with his vision of security and AI in the Swiss Armed Forces. The topic of quantum is associated with many open questions today. Christa Zoufal from IBM therefore explained how AI can benefit from the progress in quantum computing. In addition to data protection, explainability is another key challenge that has to be solved before AI can be used on a broad basis. Philippe Cudré-Mauroux from the University of Fribourg gave us some suggestions on how the problem could be solved. Christine Choirat from the Federal Statistical Office then spoke as a representative of the Competence Network for Artificial Intelligence of the Swiss Confederation about her experiences in the implementation of AI in the Federal Administration. As is generally known, large language models (LLMs) have become easily accessible since the introduction of ChatGPT. To better understand what is at stake in cyber defence, three experts in this area debated the opportunities and risks of LLMs in a panel discussion.

Lieutenant General Thomas Süssli (Chief of the Armed Forces) talks about the challenges of the Armed Forces in the area of artificial intelligence at the CYD Campus conference

## Innovation in Secure Smartphone Communication

One main focus this year was on the security of smartphone communication, in particular with sensitive information. Three innovation projects should be highlighted:
The first project was about secure smartphone communication. The project focused on the development and use of a messaging app for sending sensitive data. In its solution, the CYD Campus uses the messaging app Threema and the SCION network, two technologies with a Swiss background. In a second project, the American start-up Ostorlab won over the jury of the CYD Campus start-up challenge this autumn and presented their innovative methods on the security analysis of mobile applications at the CYD Campus Conference on 26 October 2023. Ostorlab has developed a scanner for mobile applications which enables organisations to efficiently identify security loopholes in mobile applications, both in Android and in iOS applications. The third project is concerned with the security of smartphone operating systems. The smartphone ecosystems Android and iOS widely used today offer a high degree of functionality and flexibility. While Android and iOS are widely used to store and process non-classified data, usage in the area of classified data is currently not possible at all or only on a very restricted basis.

## Cyber Training @ Cyber-Defence Campus

The DDPS assigned the pilot project "Cyber training @ Cyber-Defence Campus"[1] to the Cyber-Defence Campus as part of the National Cyber Strategy (NCS). The project aims to strengthen the cyber training offering in Switzerland by developing a concept for coordinating cyber training in the Federal Administration (civil and military positions). In addition, it aims to demonstrate the possibilities for integrating civilian partners, such as cantonal authorities and operators of critical infrastructures in the training landscape of the Federal Administration. The CYD Campus thus provides a solid training programme. Here, cyber training is not intended to be an individual basic training – rather, it concerns specific group exercises focusing on important interfaces (such as the interface between technology and management). To achieve this goal, the CYD Campus works together closely with the National Cyber Security Centre (NCSC) on designing technical exercises as well as strategic simulations and uses synergies with industry as well as the cyber training range of the Swiss Armed Forces.

How will the CYD Campus proceed? Up to the summer of 2024, various analyses will be carried out and assorted training formats tested to validate the needs of the target groups, as well as to be able to create the ideal framework conditions for cyber training in the Federal Administration. The CYD Campus was able to successfully conduct two technical training sessions in autumn 2023 (on industrial control systems and car security) in combination with relevant hackathons. A crisis simulation in cooperation with a cantonal authority is planned for early 2024. The knowledge gained from this should ultimately form the basis for the further development of the "Cyber Training @ Cyber-Defence Campus" project.

1 https://www.cydcampus.admin.ch/en/cyber-training-cyd

Insights from the cyber training/hackathon on the security of electric cars in October in Thun

## Setup of the Technology Monitoring Team

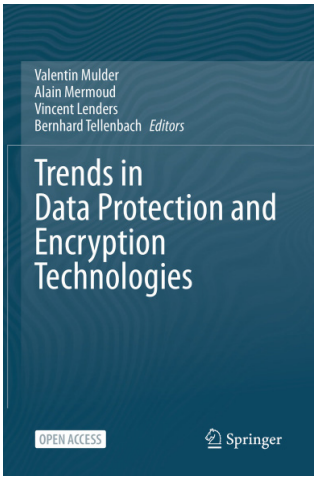
This year a new team was formed in the Cyber-Defence Campus, headed by Dr. Alain Mermoud, is dealing with the analysis of trends, risks and the dependencies of digital technologies. Cyber threats which utilise the latest information technologies are developing faster than ever before in today's digital world. It is a challenge to stay up to date when recognising these threats and assessing their potential impact. Valentin Mulder joined the Technology Monitoring team (TM team) as a full-time employee in mid-2023 after previously completing an academic internship at the CYD Campus. In October 2023, the team was further expanded by Dr. Julian Jang-Jaccard, a former Professor and head of the cybersecurity lab at Massey University in New Zealand. In February 2024, Perceval Faramaz, likewise a former academic intern of the CYD Campus, was hired to monitor the international developments. The team is also supported by a number of scientists, academic interns, fellows and students from various different universities.

This year, the team focused on three important technological trends: encryption technologies, generative artificial intelligence and quantum computing. A study conducted by the TM Team provides an overview of the developments, the current state of the art and the cyber defence implications of generative language models, known as large language models (LLM).

This published study[1] was written in cooperation with Effixis SA, EPFL, HEC Lausanne as well as HES-SO Valais-Wallis and provides industry, public administration and science in Switzerland with detailed insights into the development and risks of LLMs.

A scientific book on trends related to 38 encryption technologies and technologies for protecting data appeared this year in cooperation with more than 50 experts from higher education institutions and industry.

Quantum technologies are monitored on an ongoing basis.




The book "Trends in Data Protection and Encryption Technologies" is available in Open Access at the following address: https://link.springer.com/book/10.1007/978-3-031-33386-6

1 https://arxiv.org/abs/2303.12132

## Quantification of the Cyber Security Research Landscape in Switzerland

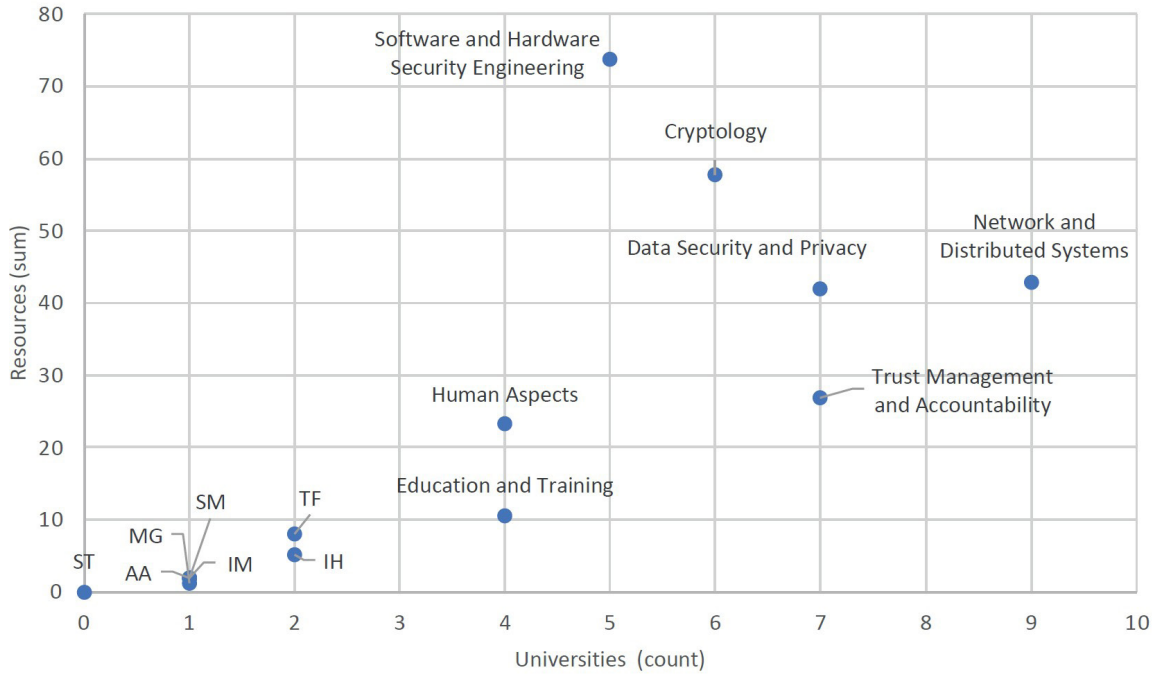
The National Cyber Strategy (NCS) of Switzerland underscores the central role of cyber security research for defence against digital threats, economic growth and the innovation strength of Switzerland. But who will invest how much in which research areas? These questions are difficult to answer as the Swiss universities enjoy broad autonomy in defining their key research areas.

The CYD Campus is involved in a leading role in various NCS measures and was first confronted with the problem of data collection. It therefore performed an extensive quantitative survey on cyber security research in Switzerland together with the Swiss Academy of Engineering Sciences (SATW).

In the study, 22 Swiss universities were surveyed and their research activities in 14 different areas of cyber security examined. The results show that Switzerland employs altogether 297 full-time equivalents (FTE) in academic cyber security research.

The majority of the research efforts are concentrated on just three areas: software and hardware security technology, cryptology as well as network and distributed systems. Together, they account for 174 FTE. In contrast to this, the five least researched areas, such as Security Management and Governance, come to a combined total of only 7.2 FTE. Measured against the number of universities involved, the research area networks and distributed systems is most popular – no less than nine universities are active in this area.

The study provides an important database for political decision-makers, universities and stakeholder groups from industry and funding institutes. Now, disparities can be discussed, strategic areas specifically strengthened and possible blind spots identified, with the goal of positioning Switzerland as one of the leading countries in the global cyber security landscape.




Number of Swiss universities and overall resources in FTE who are provided for each research area. (TF: Theoretical Principles; IH: Incident Handling and Digital Forensics; AA: Assurance, Audit, and Certification; IM: Identity Management; SM: Security Measurements; MG: Security Management and Governance; ST: Steganography, Steganalysis and Watermarking)

# 3. Students & Fellows

## Academic Interns

In order to increase the cyber expertise of students and to strengthen Switzerland's resilience to cyber threats in the long-term, the Cyber-Defence Campus offers academic internships at all three locations. In 2023, 39 students were able to complete an internship at the Cyber-Defence Campus. The interns came from different universities.

## Students

CYD Campus employees define and supervise student projects at bachelor, master and PhD levels. The students conduct their projects on the premises of the CYD Campus at EPFL, near to ETHZ and at the Campus in Thun. In 2023, work by 28 students was supported by the CYD Campus.

## CYD Fellows

In 2020, the CYD Campus launched a CYD Fellowship Programme together with EPFL to give students the opportunity to delve deeper into cyber-defence topics and to strengthen the competences in Switzerland in this area. This means that the students can already make a research contribution to Switzerland's cyber defence during their studies. In the meantime, the ninth call for the CYD Fellowship Programme could already be set in motion. The CYD Fellowship is a competitive talent programme which provides students with a CYD expert to supervise the research work. The CYD fellows are enrolled at a Swiss university and conduct their research on the premises of the CYD Campus in the EPFL innovation park in Lausanne, at Zollstrasse in Zurich as well as at the headquarters in Thun. CYD fellowships are assigned several times a year for master students, doctoral candidates and postdocs and grant an allowance for living expenses.

The new CYD Proof of Concept fellowships are aimed in particular at supporting applied research that leads to an innovative product or service, with the intention of making a real impact on cyber defence in Switzerland and assessing the potential for the commercialisation of such products or services.

**Twelve fellows** were active in 2023:

**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

**Guillaume Dubuis**
CYD Master Fellow
February 2023 – July 2023
Project title: Topological Data Analysis for Attack Detection in Energy Systems

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

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

**Dina Mahmoud**
CYD Doctoral Fellow
September 2020 – August 2023
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

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

**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

**Simran Tinani**
CYD Doctoral Fellow
September 2021 – August 2023
Project title: Non-Abelian Groups in Cryptography

**Jodok Vieli**
CYD Master Fellow
October 2022 – March 2023
Project title: Systematisation of DNS DoS: Attack Characterization, Mitigation and Measurement

## Academic Interns

Sami Abuzakuk

Khalid Aleem

Camille Arruat

Thomas Berkane

Cristian-Alexandru Botocan

Daniel Celeny

Victor Carles

André Charneca

Lucas Crijns

Isis Daudé

César Descalzo

Max Duparc

Marc Egli

Perceval Faramaz

Nicholas Sperry Grandhomme

Francesco Intoci

Sarah Ismail

Inan Kadioglu

Simon Kindhauser

Maxime Laval

Louis Leclair

Erik Wadell Ledin

Michiel Lüchinger

Léo Meynent

Valentin Mulder

Iana Peix

Octave Plancherel

Bruno Ploumhans

Guillaume Régnier

Evgueni Rousselot

Etienne Salimbeni

Martin Sand

Simon Sommerhalder

Igor Szymanowski

Alessandro Tavazzi

Andrea Alexis Thäler

Maxime Würsch

Marc Xapelli

Naima Zingg

## Students

Patrick Louis Aldover

Dominique Alguacil

Robin Bisping

Marc Bollhalder

Sebastian Brunner

Isis Daudé

Luc Desmeules

Daniel Dorigatti

Kaya Ercihan

Timothy Felix

Silvan Flum

Sébastien Gillard

Valentin Huber

Jan Kreischer

Tobias Lüscher

Fabia Müller

Silvan Niederer

Pascal Schärli

Franklyn Sciberras

Oliver Senn

Benjamin Simmonds

Mihhail Sokolov

Simon Sommerhalder

Stefan Weber

Adrian Zanga

Qianjun Zheng

Vladyslav Zubkov

## Doctoral Candidates

Despoina Giarimpampa

Eric Jedermann

Giacomo Longo

# 4. Talent Promotion

**Dr. Lucianna Kiffer - Post-doctoral Fellow at the CYD Campus and at ETH Zurich**

### Which trends do you see as relevant in the cyber sector in the next 5-10 years?

In the area in which I work, I see a growing trend towards more distributed applications. This also means that the traditional financial sector is being more heavily integrated in the blockchain area and these interconnected networks are moving towards a future in which global users have the opportunity to interact more quickly and cost-effectively. I also see a trend moving away from centralised service providers and to more control by users over their own data and its usage.

### In your opinion, what is the most important contribution by the CYD Campus to cyber issues?

One of the most important contributions is that the students have access to very topical research problems and the infrastructure. They have the chance to research and work in various different areas with the physical infrastructure of the CYD Campus. What is just as important is the wonderful support by the experts at the CYD Campus.

### Which areas did you focus on in your work as a fellow?

Through the cooperation with ETH and the supervision of master and bachelor theses, I deal with a variety of topics. In general, however, I deal with the usability of crypto currency and blockchain systems. This includes measuring the networks on which these systems are based, examining details at protocol level and measuring how new protocols are published and how these protocols influence the entire system and its users. But in broader terms, I am also interested in peer-to-peer and distributed networks in general, not only their application in block chain systems.

### What were the highlights of your fellowship so far?

One of the highlights was that around about a year ago, a few months before my fellowship began, I was able to participate in a workshop on the topic of decentralised finances, where I held a presentation. The idea was that researchers came together for one week at a remote location and worked together on problems. As a result, I started a cooperation with people from various different universities, which is still ongoing. That was really fantastic. The access to opportunities like this is clearly a highlight, as it offers the option to network on an international basis with different students, graduates and doctoral candidates who are doing great work and the possibility of exploring their work with them.

### Which interesting research topics and questions do you see for potential new fellows?

In general, I work in an area in which there are ever more questions for researchers, as things are constantly changing and more and more protocols and measurements are required. One topic that I would see as an interesting research area at the CYD Campus is the fact that more and more institutions are working and interacting with crypto currencies and block chain protocols and creating their own versions of approved systems in order to interact with existing systems.

### Why would you recommend the fellowship?

My experience was that you have an incredible amount of freedom in research which you might otherwise not have. In addition, the connections between the research centres and the universities offer many resources and the opportunity to exchange ideas with different people is very valuable.

## Simon Sommerhalder - CYD Master Fellow from ETH Zurich

### How did you find the application for the CYD fellowship?

In retrospect, it was a huge effort, but it was definitely worth it. In the meantime, it has probably become easier, as one year ago the registration platform was still in its infancy.

### Which topic are you writing your thesis about?

My thesis deals with the question of whether you can detect devices infected with trojans via their network traffic. This is very challenging, as practically all applications, including viruses and trojans, encrypt their network traffic. We therefore try to determine, using artificial intelligence, behavioural patterns which these trojans have in common and which distinguish them from other programmes.

### What appealed to you about the CYD Campus that made you wanted to write your thesis here?

Before I had the actual job, I already knew that I wanted to do a project in the area of "network intrusion detection", as this topic covers almost all of my interests and study focuses. When I was looking for a master thesis, I stumbled across the CYD Campus conference on the Internet, but unfortunately I was no longer able to obtain a ticket. One day later, I met Bernhard Tellenbach from the CYD Campus at an event of the cyber group of ETH and that's how the ball got rolling. Bernhard is now also my supervisor, by the way.

### Which interesting insights have you had so far?

Above all, I've realised how wide-ranging the area of cyber security actually is. Thanks to the various events of the CYD Campus, I was able to gain insights into several research projects. In particular, I also found the research which the CYD Campus conducts in the area of LLMs and their risk potential interesting. In addition, one highlight was that I was able to take part in a hackathon in which we checked the cyber security of various car models.

### How do you find the exchange of ideas with your supervisors?

I find the regular exchange with my supervisors very valuable. It can sometimes also be unpleasant, because you're not always of the same opinion, but for precisely this reason it's the ideal place for personal development and to prepare myself for the working world. I am very grateful for the various persons with whom I can work together here.

### How would you like to develop in future and how is the CYD Campus helping you in this?

I don't know yet what I will do after my master thesis. Up to now, I've found that the right door will open at the right time. I can't rule out that the CYD Campus might play a significant role in this, as I have been able to meet many different people and companies here.

# 5. Cyber Security

The research at the CYD Campus represents an investment for securing the required expert knowledge and the scientific and technical skills for Switzerland's tasks in the area of cyber defence in the long term. As an important component of technology management, it serves to create detailed plans for future technologies and innovation projects of the DDPS. This research contributes to the development of necessary operational skills in cyber defence and supports scientific and technical planning and procurements in the DDPS. The research projects are implemented in cooperation with universities and industry partners.

## Quantum-proof Cryptography

Progressive research in the area of quantum computers harbours cryptological risks. Up to now, digital signature schemes and asymmetric crypto systems (public key encryption), which are secure against traditional computers could be broken by quantum computers.

Over the last few years, the National Institute of Standards and Technology (NIST) has for this reason driven forward the research and standardisation of those cryptographic procedures for which it is assumed that they are secure against such attacks. In August 2023, for three of the proposed procedures which it considers sufficiently mature for standardisation, NIST published corresponding drafts as Federal Information Processing Standards (FIPS 203 based on CRYSTAL-KYBER, FIPS 204 based on CRYSTAL-Dilithium and FIPS 205 based on SPHINCS*). According to the NIST, other methods need more time for the evaluation, in particular the approximately 40 new signature procedures that were submitted as part of a call to submit further methods between September 2022 and June 2023. The goal of the project is to examine the security of the proposed procedures and to explore methods for combining traditional and quantum-safe procedures.

In this year, the focus was on the in-depth examination of the security of code-based procedures (such as finalist "Classic McEliece" and "BIKE") and of procedures based on multi-variant polynomials. With regard to the combination methods, the current status of research as well as current and planned standards for multi-key encryption and multi-key signature schemes were examined.

### Secure and Sovereign Smartphone Platforms

A smartphone consists of modules and products of a variety of software and hardware providers. If a smartphone is used to store and process sensitive data, such as classified data, this requires a high degree of trust in several or, in the best case, all of these providers. However, modern smartphone platforms today offer increasing options to reduce this trust to individual providers in ideal cases, such as to hardware manufacturers, to implement what are known as "Trusted Execution Environments" (TEE). The goal of the project is to examine the possibilities and limits of current TEE technologies and to propose a solution for the seamless integration of existing smartphone ecosystems ("insecure world") and highly-sensitive applications ("secure world"). This year, a first prototype was implemented on a current smartphone. While the proposed solution works in principle, several more challenges in the areas of performance and access to peripheral devices (such as screen and network) which must be jointly shared by the secure and insecure worlds need to be solved next year.

### Secure Mobile Operating Systems

The widely used smartphone ecosystems Android and iOS today offer a high degree of functionality and flexibility. While Android and iOS are widely used to store and process non-classified data, usage in the area of classified data is currently not possible at all or only on a very restricted basis. However, as there is a need in Switzerland, a project has been launched with the goal of identifying and examining possible solutions to cover the need. The biggest challenge is finding the best architecture for a secure mobile operating system which offers a balance between security, feasibility and ease of use.

Two approaches are pursued to protect sensitive data: The first approach consists of a compartmentalisation of the components. This means that the point of attack is interleaved to the system, so that the impact of attack can be minimised. Two architectures for a secure mobile operating system have been developed for this purpose, including a risk analysis. Cyber security not only comprises the mobile operating system but also the hardware, the cryptographic components and hardening of the boot chain (signatures). The second approach attempts to separate the execution of an application from the operating system and the manufacturer, in order to ensure sovereignty over the application and increase security.

### Security Analysis of Firmware of Mobile Devices

Software security is an important element in achieving a high level of cyber self-protection. The identification of software vulnerabilities, be they intentional (for example, by compromising the supply chain) or unintentionally introduced, makes an important contribution to this. While various approaches and tools already exist for the (automated) static or dynamic analysis of applications, this is not at all or only partially the case in other areas, such as the firmware of mobile end devices and the (system) applications pre-installed on them. In this project, novel approaches for automated analysis of the firmware of mobile devices, focusing on the dynamic analysis, have thus been examined, in order to minimise the risk of vulnerabilities in firmware. This year, a systematic literature analysis on the state of research was conducted and a prototype on dynamic testing of pre-installed Android apps developed. The prototype comprises a service that extracts the pre-installed apps from an Android firmware and imports the extracted apps into a user-defined firmware.

### Cyber Security in Domotics and Building Technology

The ever-growing networking and digitalisation of building technology makes this an increasingly interesting target of attacks. In order to better understand the opportunities and risks of current and future technologies in this area, also known as domotics, and to be able to meet them proactively, it must be possible to examine and test them. The goal of this project is to create the conditions for this. For this purpose, the planning, design and implementation of a test bench for building automation was started this year. The test bench aims to depict the building automation and control systems used in the Federal Administration as accurately as possible. The concept developed in the project comprises various "suitcases" which represent the individual building automation systems: Plant automation, room automation, metering systems, fire alarm systems, IoT, etc. Each suitcase is connected with a backbone that represents the technical network. In the coming year, it is aimed to implement the test bench and submit it to its first endurance test as part of a hackathon.

### Cyber Forensics in Industrial Control Systems

While a variety of tools and instructions for the forensic analysis of cyber incidents are available for traditional Windows and Linux-based IT systems, there are somewhat fewer tools for the environment of industrial control systems. The goal of the project was to identify effective forensic techniques and tools for operational technology (OT) and substation automation systems. In addition, a training model has been developed and successfully tested, which introduces participants with various levels of prior knowledge to forensic analysis in the context of OT environments. Tools to perform three forensic tasks have been developed and refined: Artefact collection and hard disk analysis, analysis of IEC61850 data packages and storage analysis.

### Security of Wide Area Networks

Many public and private organisations use geographically distributed networks (Wide Area Networks, WANs) to connect their locations with each other. As these WANs are often critical for operating the organisation, their security with regard to confidentiality, integrity and availability is of crucial importance.

In order to achieve a good level of security, such networks are often set up with a dedicated network infrastructure. However, this approach is very cost-intensive. Over the last few years, newly developed technologies promise more cost-effective and flexible solutions with comparable security. In this project, the CYD Campus is examining how new technologies (such as SCION from ETH Zurich research) and programmable network architectures (SDN/P4) can be used for secure WANs.

After the CYD Campus set up its own test network with SCION between its three locations in 2022, the focus this year was on the further development of SCION in cooperation with ETH Zurich and in the combination of SCION with other technologies (for example, to conceal metadata). Among other things, an extension for SCION has been developed, which enables network traffic to only be sent via devices with certain properties. This enables, for example, an organisation to send traffic between its locations only through devices that are equipped with the latest software and thus have no known security loopholes.

### Automation of Cyber Defence Teams

Cyber attacks are on the increase, and becoming more and more sophisticated and difficult to detect. This makes it difficult for the defenders to keep pace. They are forced to automate your defence capabilities as much as possible in order to improve your reaction capability and efficiency.

In this project, we examine different ways of how the defence of cyber infrastructures can be automated. As the development and testing of new methods directly in real cyber attacks is difficult and risky, we are instead using a cyber defence exercise that takes place every year as a test environment. In this exercise called "Locked Shields", around 25 defence teams defend their infrastructure against numerous attacks by an attacking team. Normally, the Blue Teams (the defenders) consist of experts with wide experience in the area of cyber defence. Together with researchers from the Dutch Military Academy and the NATO CCDCOE, the CYD Campus is now examining the potential of a completely automated team which can take part in Locked Shields without human involvement.

During this year's Locked Shields, the basic principles for the further development of the "virtual" Blue Team were defined. The basic structure of the team was thus implemented and the researchers obtained important data for further development. The goal is now to have the virtual Blue Team participating in Locked Shields next year. However, it will still take a few years until it can seriously compete with the "traditional" Blue Teams.

### Automation of Security Operation Centres (SOCs)

The rapid development of the cyber security threats and the increasing complexity of the attacks are forcing the Security Operation Centres (SOCs) to explore innovative approaches in order to improve their detection and reaction capabilities. The Security Operation Centre (SOC) is still the first line of defence against these dynamic and sophisticated threats, which requires continuous innovation and adjustment. In this context, the integration of artificial intelligence (AI) in SOC practices has attracted much attention and promises to revolutionise the effectiveness and efficiency of cyber security operations in comparison with the application of rule-based tools.

In view of the increasing demand for AI-controlled solutions in the area of SOC, we are examining where and how AI can be used in automation and to simplify the processes. This year's review examines various different research questions and attempts to identify the prevailing trends and application patterns by examining the current state of the art in the application of AI in SOCs in a survey. In addition, models based on neural networks and LMM are being examined experimentally using historic data.

### Hacking Micro-drones

Unmanned aerial vehicles (UAVs), also called drones, represent a revolution in the security and military areas. Due to the latest advances in miniaturisation and the declining costs, mini UAVs have also become very popular in the civilian sector. These drones can even be equipped with lethal weapons, as can be observed in the war in Ukraine. They also represent a threat for the military and the security authorities, as they are equipped with powerful sensors and can be used for infiltration or data collection over restricted areas. The military and security authorities are therefore endeavouring to develop skills to counter threats using mini UAVs. The goal of this project is to research various techniques for blocking and adopting mini UAVs, in order to neutralise the threat they present. In particular, it is being examined whether it is possible to use the control and navigation channels through advanced signal interference, signal spoofing and signal manipulation attacks for this purpose. This year, the focus was on complex multi-drone GPS spoofing, which was demonstrated successfully in the laboratory.

### Automatic Exploit Generation for the Linux Kernel

The Linux operating system kernel today forms the basis of various operating systems which are in turn used on a variety of devices (desktop PCs, server systems, mobile and electronic small devices, etc.). As a result of this broad distribution, the Linux kernel is an interesting target for attackers who want to compromise a system.

As part of a joint research project with IBM Research Zurich, a method is being researched to assess whether a possible bug in the Linux kernel is security-relevant, in other words, whether it can be effectively exploited or not. One of the reasons the answer to this question is important is because a large number of open bugs are publicly accessible for the current kernel, and could be used for the prioritised elimination of exploitable bugs.

As a result of this year's research activities, a research paper has been created which summarises the specialist knowledge obtained to date in the area of Automatic Exploit Generation (AEG) with regard to the Linux kernel. In addition, work has continued on a proof of concept tool whose applicability could be verified by means of an initial kernel bug for which corresponding exploits have been generated. An expansion of the applicability to further bugs and vulnerability classes is planned for the coming year.

Likewise as part of the research project, a new sub-project has also been launched this year, which is to search for data-only attack vectors on an automated basis. Attacks by means of data-only techniques have recently become more popular, as they can be used to avoid modern security mechanisms of the Linux kernel (such as Control Flow Integrity - CFI). The functionality of the implemented approach could already be proven with initial results — the first unknown kernel objects to date have been found which can be manipulated to expand the capacities of an attacker.

### Protection of Insecure Avionics Systems

This research project is concerned with the analysis of vulnerabilities in avionic hardware and the associated protocols. In the past few years, CYD Campus researchers have analysed attacks on the technologies ADS-B (Automatic Dependent Surveillance–Broadcast), CPDLC (Controller-Pilot Data Link Communications) and FLARM together with the Avionics Laboratory in Thun both theoretically and in practice. FLARM is a collision warning device for light aircraft and drones, which was developed in Switzerland and has attracted worldwide attention and distribution. In 2023, the researchers pursued a practical analysis of the Traffic Collision Avoidance System (TCAS), which is used in larger aircraft. They were able to show the first realistic attack outside of theoretical observations and simulations. A similar approach was achieved in cooperation with Skyguide and Eurocontrol on the topic of CPDLC. In addition, the impacts of high-frequency disturbances of the Global Positioning System (GPS) in commercial aircraft, particularly after the outbreak of the Ukraine war, have been examined.

### Cyber in Aerospace

Cyber security in aerospace has been a key research topic since the CYD Campus was founded. In Aerospace there are many fundamental similarities, including the area of cyber security. Thus, for example, many obsolete technologies are utilised, which often have been used unchanged for 20 or even 40 years. Particularly in the area of wireless communication technologies, this leads to fundamental security problems, as the contents are neither encrypted nor authenticated. But even where contents are encrypted, this is often not conducted with open, secure standards but with weak proprietary systems which contradict Kerckhoff's principle of secure crypto systems. This year, the CYD Campus has identified several such procedures as part of its work on the avionics data connection ACARS (Aircraft Communication Addressing and Reporting System), which can be automatically recognised in a stream of mixed data (encrypted, unencrypted and weakly encrypted). Further work is underway to decode some of the codes found.

In the area of satellites, the CYD Campus was very active in various segments in 2023. An attack was thus shown for the first time on LEO systems (Low Earth Orbit), which can also localise passive users. Localisation was also a topic to detect GPS interference using drones and directional antennas. Finally, new practical attacks have been developed on ground stations, which can be executed via the wireless interface and the backgrounds of the rapidly increasing security problems in the satellite area have been analysed in detail.

### The Human Factor in Security and Safety

Phishing attacks are becoming increasingly sophisticated and aim to attack people in a targeted fashion while exploiting cognitive distortions, for example by conveying the impression of authority or urgency. Earlier methods of user training focused on URL warnings, text-based or click-based training and led to mixed results. For interactive training that is not bound to the screens of users, we examine the potential of Augmented Reality (AR) technologies to improve phishing detection. By visually displaying the distortions which attackers typically exploit and the haptic interaction of the users with it, the training aims to put users in a position where they can combat cognitive distortions through increased awareness and mistrust. In a laboratory study with 100 users, we evaluated the phishing detection rates, the user interaction and the assessment of the AR-based training in comparison with a click-based version and a control condition. Our results show that an interactive phishing training, which takes into account cognitive distortions, can increase the detection rates by 33% and that interactive elements are well perceived. AR technologies also improve the training, but more research is required to confirm this.

### Security of Electric Vehicles and Charging Infrastructures

As part of the changeover to electric vehicles in the DDPS, the security of the existing charging infrastructure must also be examined. Preliminary work has already shown that in certain systems with power line communication (PLC), the data flow can be intercepted wirelessly from a distance. This can have various impacts on the security and data protection 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 what is known as a denial of service (DoS) attack interrupts and ends the charging process wirelessly and with little effort. The attack with the name Brokenwire was reported to the National Cyber Security Centre (NCSC) and the researchers involved are in contact with vehicle and charger manufacturers to mitigate the attack. The analysis of such attacks and potential countermeasures was conducted in 2022.

The security analyses were expanded in 2023. The CYD Campus researchers thus examined the impacts of wireless attacks on battery management systems with their partners and a research paper dealt with the security of Bluetooth systems in civilian vehicles. A car hackathon was also conducted once again, in which the firmware of cars and charging stations was jointly examined using modern fuzzing methods.

### Self-Sovereign Identity (SSI) as the Basis for National Digital Identity

After the population rejected the e-ID concept of the time back in 2021, the Swiss Confederation conducted a public consultation on the e-ID target image. A majority of the 60 participating cantons, parties, universities, organisations and companies declared themselves in favour of SSI as the technological basis of the new e-ID. The Federal Council then made a landmark decision in favour of SSI and anchored this approach in the new e-ID Act. The EU is also pursuing the path towards SSI as part of EIDAS 2.0.

SSI is a new paradigm which focuses on the sovereignty of users over their identities and their digital credentials. Key infrastructure elements which can control, correlate and monitor the actions of certain individuals, are avoided as far as possible. SSI combines several basic technologies such as block chain-based Distributed Ledgers (DLT), cryptographic proofs of identity attributes (zero-knowledge proofs), PKI with distributed key management as well as various software components such as mobile wallets and agents connected in a P2P network. Accordingly, the technology stack of SSI is very complex and there are several possible characteristics.

SSI is a new technology and the international standardisation is still in progress. In order for SSI to become a secure technological basis for critical infrastructures such as the national electronic identity card, various aspects need to be researched. These include the security of protocols and the implemented systems, the scalability for millions of users, the protection of privacy and the usability. The CYD Campus networked this year with the e-ID team and the SSI Community of Switzerland. As a member of the Technical Advisory Circle, it analyses technologies and advises FEDPOL and BIT in technological decisions.

Open research questions will be examined as part of a PhD fellowship and various master theses in cooperation with Swiss universities.

### Security in 5G

With the latest update for 5G networks, a new security function called Authentication and Key Management for applications (AKMA) will be introduced. This function aims to establish secure connections between telephones or other devices and certain applications by using the initial security check when the device connects with the network.

However, our examinations show that AKMA in its current form has several severe vulnerabilities which could be exploited by attackers. These vulnerabilities could enable someone to eavesdrop and follow communications, intercept data or even to find out which device is attempting to establish a connection with an application. We have identified these problems and submitted proposals on how they could be eliminated in order to make AKMA more secure and to prevent these types of attacks.

One of the main problems that we have found is that the compromising of an application function in a 5G network can impair the security of all connections between applications and devices. This means that an attacker who gains access to a part of the network could potentially access a large amount of sensitive information or wire-tap communication. It is important to eliminate these vulnerabilities before a broad introduction in order to protect the users and their data.

### Data Protection with Lawful Interception

When prosecution authorities need to access information from telephone companies to support investigations, this is called lawful interception (LI). The latest 5G mobile phone networks contain new data protection functions which make it difficult for the prosecuting authorities to obtain this information without risking it landing in the wrong hands. This study presents a new method for prosecution authorities to request information from telephone companies without jeopardising privacy. It uses a special method which establishes a balance between the receipt of required information and the safeguarding of privacy in the 5G network system.

Lawful interception is a legal regulation for communication service providers (CSPs) to support the prosecution authorities (LEAs) in accessing network data in criminal investigations. In the 5th generation mobile phone networks (5G) the improvement of data protection in network identifiers presents a challenge for the LEAs, as sensitive information might be forwarded to non-trustworthy CSPs. In this study, a system was presented which enables LEAs to request the resolution of network identifiers of CSPs privately. The system uses a novel protocol which balances the request for information and the consideration of data protection aspects, thus improving the performance, while trustworthiness is safeguarded within the 5G LI infrastructure.

This research offers a solution for prosecution authorities to conduct lawful interception in the 5G core network and simultaneously protect their operations from non-trustworthy communication service providers. Through a novel procedure for information procurement, the system optimises the balance between data protection and performance. Experiments show an increased performance in the resolution of identities while simultaneously protecting sensitive information, guaranteeing adaptability to various operating scenarios and managing large data records. Altogether, this solution addresses data protection concerns in conjunction with enabling LI within the 5G core network.

The CYD Campus' research deals with the cyber security of aircrafts

# 6. Data Science

Machine learning and artificial intelligence have become integral parts of our society. Numerous algorithms and tools are available for general use in the meantime. One example of this is ChatGPT, which is used by many people to create texts or answer questions. The area of large language models (LLMs) has developed particularly well over the last twelve months. These models can be used in various situations to support users. We should not underestimate their capabilities or trust blindly in the answers and texts they generate. AI is another area which is developing rapidly. Various models are available for creating artificial images from texts. Examples of these are Dall-E and Midjourney.

In our research programme Data Science, we attempt to recognise trends and assess their future potential in various application areas of data analysis. The research programme aims to provide us with the necessary skills to be able to advise our partners from the DDPS or the rest of the Federal Administration on how, through data analysis, they can obtain information which offers them added value in their activities. We use various methods, depending on the type of data and the task to be solved. Some questions can be answered with statistical approaches, while other problems require more progressive methods such as Deep Learning. The first step is to obtain a deeper understanding of the data, as this considerably influences the choice of procedure, depending on its type, structuring and distribution. To further develop our skills, we work together closely with academic partners and include a number of students (Master, PhD and postdocs). In this chapter, we will address the most important topics from the area of Data Science which we dealt with in 2023.

## Robustness and Trustworthy AI

### Impact of Data on the Robustness

This project is about defending neural networks against enemy attacks. We explore the impact of structural changes. Here, we focus on which data should be used for training robust models. Our work was based on the following **four approaches:**

**Threshold network:** Activation functions are modified during the test period, in order to generate a local linear behaviour that is based on biological neurones. The goal is to increase robustness by suppressing low values and thus prevent their exploitation by attackers. Although this approach is susceptible to the very cost-intensive EOT (Expectation Over Transformation) attacks, there is a threshold value from which the robustness of the model can be considerably improved against typical and less cost-intensive attacks (such as PGD, AutoAttack...) without additional costs and with comparable accuracy.

**Feedback network:** As the label distillation improves the robustness of a model, we want to achieve similar results by preprocessing the images to improve their quality. A separate player assesses which measures should be implemented to improve the image quality, whereby both the loss improvement and the forecast correction are taken into account. Our experiments show that data should not be adjusted in order to better match the label, although the opposite would be helpful.

**Data generation with diffusion models:** In this method, we modify diffusion models to achieve more robustness through more discerning training data. With this approach, disturbances are introduced by attackers during the diffusion process. We succeed in generating new images which deceive the model and considerably differ from the images which were generated without our method. The only observed disadvantage is an increase in Out of Distribution (OOD) samples, which cannot be addressed systematically.

**Sampling in embedding space:** To avoid the generation of OOD samples, we work in the embedding space in this approach and use CRATE, a linearly separable embedding model. We have established that samples located in the vicinity of the boundary frequently have an incorrect label. In addition, random uniform sampling in embedding space leads to a lower image diversity. Finally, we show that – contrary to what is claimed in literature – the robustness is not simply improved by removing or adding discerning samples.

### Adversarial Distributed Federated Learning

Federated learning (FL) is a distributed paradigm in the area of machine learning (ML) which enables the development of models by using data from several entities while retaining their data ownership. With FL, there is a designated federator node which is defined in advance. In distributed federated learning, this federator is determined dynamically and can change over time.

However, FL is susceptible to external attacks due to its distribution, in particular with decentralised FL (DFL). We therefore concentrate on novel attacks and protective mechanisms for DFL which are necessary both from an offensive and a defensive perspective. Our activities this year were split up into **four areas:**

**The development and implementation of a module for robustness analysis for a DFL platform (Fedstellar):** The robustness module consists of i) the component for malicious attacks and ii) the component for robustness aggregation. Several malicious attacks have been integrated in the respective component, including targeted/untargeted label flipping attacks, targeted/untargeted sample poisoning attacks, backdoor attacks and model poisoning attacks. In addition, certain protocols on robustness aggregation, such as Krum, Median, Trimmed-Mean, FLTrust, Sentinel, and SentinelGlobal were integrated in the component for robustness aggregation in order to protect the DFL platform from poisoning attacks.

**The development and implementation of an approach based on moving target defence (MTD) to contain poisoning attacks on DFL (Voyager):** Voyager consists of three main components: an anomaly detector, a network topology explorer and a connection provider. If an abnormal model is discovered in the network, then the topology explorer reacts strategically by establishing connections with trustworthy participants to protect the model.

**The development and implementation of a protocol for robustness aggregation for defending DFL against poisoning attacks (Sentinel):** Sentinel uses the accessibility to local data and defines a three-level aggregation protocol, consisting of similarity filtering, bootstrap validation and normalisation to protect the model from malicious updates. Sentinel has been evaluated with various data records as well as with different types of poisoning attacks and threat levels and was able to improve its resistance against untargeted and targeted poisoning attacks compared with the current state of the art.

**The assessment of robustness against poisoning attacks for a federated reinforcement learning (FRL) framework:** During the course of this work, a FRL-based approach to contain malware attacks on resource-limited devices has been developed and used as a prototype. The robustness of FRL was analysed thoroughly here.

### Development of more Trustworthy AI

Trustworthy AI is an emerging concept that combines several existing principles, such as:

i) Human action and supervision
ii) Technical robustness and security
iii) Data protection and data management
iv) Transparency
v) Diversity, non-discrimination and fairness
vi) Social and ecological well-being
vii) Responsibility

Here, we concentrated on the development of novel solutions for assessing the trustworthiness of conventional models for AI and federated learning (FL). We focused on the following **three main goals:**

**Trustworthiness of federated learning:** An extensive taxonomy was introduced for this purpose which consists of six pillars (data protection, robustness, fairness, explainability, accountability and federation) and more than 30 metrics to calculate the trustworthiness of FL models. An algorithm called FederatedTrust was then developed which is based on the pillars and metrics mentioned in the taxonomy. A prototype of FederatedTrust was implemented and integrated in the learning process of a proven FL framework. Finally, five experiments with different configurations of FederatedScope (with different participants, selection rates, rounds of training and differential data protection) were conducted to prove the benefits of FederatedTrust.

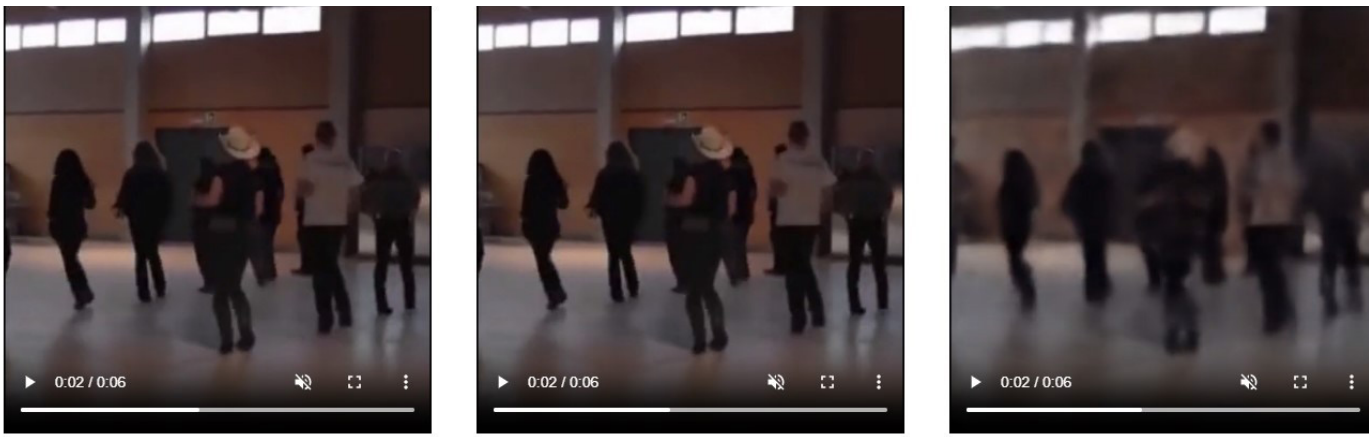
**Sustainable and trustworthy federated learning:** The pillar of sustainability was introduced into the current taxonomy for trustworthy FL. This work is thus the first in which all requirements that were set out by a group of AI experts of the European Commission were met. The pillar of sustainability assesses the ecological impact of the FL system taking into account terms and metrics for hardware efficiency, complexity of the federation and carbon intensity of the energy network. An algorithm to assess the trustworthiness of FL models was then developed and implemented, which incorporates sustainability. Comprehensive evaluations with the FederatedScope framework and various scenarios with different federation participants, complexities, hardware and energy networks prove the benefits of the proposed solution.

**Assessment of trustworthy AI with missing data record:** In this work, a generator for synthetic data records was developed which aims to calculate the trustworthiness of models with missing data. The solution developed offers two possibilities for generating a synthetic data record (MUST and MAY) that differ in the number of statistical characteristics of the original data record, which serves as input, to achieve the compromise between data protection and accuracy. The generation of the data record and the assessment of trustworthiness was tested and assessed in two scenarios. The results from four different trust assessments (True Score, Limited Score, Advanced Score MUST and Advanced Score MAY) are compared, analysed and discussed for each assessment scenario.

### Efficiency and Robustness of Deep Learning Algorithms for Steganography in Video Data

Steganography, in other words, the concealment of cryptographic signatures in media contents (such as a video) can be implemented today using modern deep learning algorithms. Particularly in the area of video data, these algorithms still have major limitations with regard to their runtime (efficiency) and robustness with regard to various different transformations of videos (such as compression at upload to a social media platform). This project focused on methods that can be used to conceal a digital signature in videos. Using such a signature, it is possible to check the authenticity of video data (in other words, its origin and the integrity of the content). With the emergence of ever more powerful generative AI for generating synthetic video data and its use in the context of influencing operations, the significance of such digital signatures is increasing. Video contents that are officially produced thus could, for example, be furnished with a digital signature which in turn can be verified electronically by the recipient.

In this project, an established method for generating video signatures has been expanded so that the signatures remain even after compression through common algorithms (such as H264 compression). In addition, an algorithm has been developed that enables the signature for high-resolution video data to be generated as is typical for professionally produced content. This shows that in future, digital signatures for video data that have been generated via Deep Learning are a potential tool for safeguarding authenticity in the age of social media.




Example application of an efficiency-enhanced Deep Learning algorithm for the digital signature of video data. From left to right: Original video (cover video), video with hidden digital signature (container video), reconstruction of video content from hidden signature. The latter can be used to detect any manipulation of the contents.

## Generative AI

### Exploration of Deep Content Generation

Over the last few years, ever more powerful methods for generating synthetic image and video material have been published. In particular what are known as diffusion models (such as DALL-E or Stable Diffusion) are meanwhile able to generate deceptively real images and offer various mechanisms to present the result (such as via input text or image). These methods are now being increasingly used by threat actors as part of influencing operations. Image and video material is generated to make false claims more credible and thus to have a lasting influence on the information space.

In this project, an inventory of the methods currently available was taken and a series of deployment scenarios was defined from the perspective of a threat player. This catalogue of scenarios was the basis for deriving the threat potential and characterising the limitations of the available algorithms. The results of this project offer the basis for further measures for defending against influencing operations with synthetic image contents (for example, for tabletop exercises, development of detection algorithms, etc.). Findings from this project have also been provided to various internal federal working groups.

### Opportunities & Risks of Generative AI

Generative artificial intelligence (AI) comprises methods which i) are able to estimate probability distributions from large amounts of data and ii) can generate new synthetic data examples based on this. These methods offer both opportunities and risks for the cyber defence of Switzerland.

Modern generative models are usually trained on data sources with different modalities (such as image and text data). These models can thus be customised increasingly flexibly to various different application scenarios. What should be highlighted here is the evaluation support of various data sources for answering military and intelligence questions. Thus, for example, satellite images and audio files could be furnished automatically with tags by generative AI which makes the content of the data characterised, filterable and searchable. In addition, generative models can also be used to deposit hidden digital signatures in files which can be used for authentication purposes in the service of information security.

Apart from these opportunities, these methods also bring new challenges and risks for cyber defence. In particular, methods for synthetic generation of image and video material can be used by threat players for various purposes as part of hybrid warfare. An increase in AI-generated media contents will make it increasingly difficult for citizens to be able to distinguish between true and false/fictitious contents. Analysts in military and intelligence units will likewise be challenged. Synthetic image and video material could be used in future by threat actors for purposes of military deception. Propaganda material can be increasingly automated, produced on a large scale and distributed via channels into social media. Social engineering can also gain credibility through the use of synthetic media content and bring the human factor further under pressure in cyber attacks. Initial studies also show subtle influencing vectors, for example, through the use of text modules which have been generated using large language models. In summary, it can be said that the information space will in future be increasingly interspersed with synthetic content. The uncertainty of which source and information can be viewed as credible will also increase.

Synthetic image generation with Stable Diffusion using the example of a HIMARS guided missile launcher. From left to right: Original image, canny-edge map, five different synthetic examples. The canny-edge map is used as input for Stable Diffusion and guarantees that the geometry of the vehicle is preserved as far as possible. Stable Diffusion can now change the original image such that the vehicle appears in a different environment than in the original image. In future, threat players could use such a method in combination with a targeted distribution over social media for the purpose of military deception.

## Distributed Learning

### Distributed Federated Learning

In contrast to the conventional approach of federated learning (FL), which is based on a centralised model in which a single entity aggregates data from various sources, DFL performs the aggregation over several nodal points on a peer-to-peer basis. The risks involved in central data processing, such as individual fault points and bottlenecks, are thus reduced and as a result data protection improved and the robustness of the system increased.

In this framework, we have developed a novel platform called Fedstellar, which provides scientists with a tool to experiment with DFL. Thanks to this innovative open source platform, realistic DFL scenarios can be created more easily in virtual and physical devices, where a cluster of Raspberry Pis is used as the underlying infrastructure to improve the cooperation in model training while at the same time ensuring data protection. The fact that Fedstellar is used by more than 20 researchers in various institutions bears witness to its efficiency and usability. Based on this platform, we cannot emphasise enough how important it is to integrate robust security measures into the DFL framework and to accept the critical challenges which the Internet of Things presents us with regarding data protection and data security.

In addition, we are introducing an innovative security module, seamlessly integrated in Fedstellar, in which the latest encryption and moving target defence techniques are combined. This module considerably improves the security of DFL networks and demonstrates the adaptability and resilience of the platform to complex cyber threats. One very important contribution that we make with Fedstellar is that we enable users to create customised topologies with which they control the decentralised aggregation of model parameters and can thus improve the efficiency and the data protection of federated learning processes. Future work will deal with the examination of mobility and adaptive dynamic topologies based on reputation conditions or model similarity, the creation of lightweight models and user-defined aggregations as well as other techniques for optimising the federation.

### Protection from IoT Devices

In the dynamic and continuously growing world of the Internet of Things (IoT), two different yet complementary lines of research stand out in the area of individual IoT fingerprinting: Identification and authentication. Both research lines pursue the same goal of creating additional security for networks by using innovative identification and authentication methods based on machine and Deep Learning techniques (ML/DL). These research lines go in two directions. (1) First, we will deal with the complex topic of device identification in IoT networks. A LSTM-CNN architecture is used for this purpose, which aims to analyse the performance behaviour of the hardware of IoT devices using a time series approach and to learn from it. The breakthrough of this research work lies in the achievement of outstanding identification accuracy, which indicates a robust capability for the correct identification of legitimate devices with simultaneous minimisation of false identifications. In addition, the resilience of the architecture to attacks is examined in this research. This is an important aspect in view of the ever more sophisticated cyber threats. Although the system is distinguished by its resilience to context-related attacks, such as those based on temperature fluctuations, it proved more vulnerable to extended ML/DL evasion techniques, such as MIM, BIM and ISMA. Countermeasures have been introduced, such as adversarial training and model distillation, to improve system defence. These measures have proven to drastically reduce the success rate of the most effective attacks and thus increase the security of IoT devices against evasion attempts without significantly impairing performance. (2) We will now concentrate on the authentication of individual IoT devices. The new line of thought of this research work consists of the use of transformer autoencoders, to create unique fingerprints of the hardware behaviour for each device. The innovative use of transformer models, which are particularly suited for processing time series data, enables the specific faults and fluctuations in the hardware performance to be recorded and used as a reliable means of authentication. A high true-positive rate (TPR) in connection with a low false-positive rate (FPR) clearly proves how effectively transformer autoencoders can distinguish between authentic and non-authentic devices. It also underscores the potential of this approach to significantly improve the security and thus the trustworthiness of applications within the IoT ecosystem.

## Processing and Understanding Natural Language

### Opportunities and Risks of Large Language Models (LLMs)

Language modelling, in other words, the assignment of probabilities to the tokens of natural languages, has for some time been a sub-task of numerous pipelines for processing natural language (Natural Language Processing - NLP), for example, in machine translation or in answers to questions. However, with the advent of conversational agents such as ChatGPT (end of 2022), it has moved into the spotlight. The transformer model with its encoder-decoder architecture and self-awareness revolutionised language modelling, although the era of large language models already started in 2018 with the ELMo model. Even if the transformer was originally used for neural machine translation, models which do not necessarily use such sequence-to-sequence transformation could use either only the decoder part, if the goal is to understand the text structure, or the encoder part where text generation is concerned. These models could thus be used for a variety of NLP tasks, provided that the pipeline is well defined.

However, text generation, particularly in conversation environments, appears to be the most interesting case of application. Even if LLMs display a remarkable capacity for generating high-quality texts, they still only remain very clever rate algorithms which have been trained in an immense amount of written text. If they are used intelligently, however, and with retrieval in the form of retrieval augmented generation or not coupled with text but with other data modalities, this would open up enormous potential. But the models themselves are not search engines or tools for checking facts, knowledge stores, etc.. They generate results from the patterns obtained from the data, without understanding their meaning. This means that they also retain the distortions contained in the training data or save the information from the inputs, which makes them susceptible

for the disclosure of confidential data, the generation of inappropriate contents or hallucinations.

### Recognition of Artificially Generated and Misleading Text in Social Media

The latest advances with large language models such as ChatGPT – the fastest expanding consumer product of all time, have shown that text generated by LLMs cannot, at first glance, be distinguished from text written by humans. The fact that it is not possible to distinguish between generated texts and texts written by humans harbours numerous dangers in various different areas. One of these dangers is, for example, the ability of automated bots to impersonate humans and to manipulate public opinion through rapidly created, misleading posts, or to create academic texts which are declared to be genuine by a fraudulent author. This problem is exacerbated by hallucinating LLMs, which make hardly verifiable factual claims. The main goal of the proposed project is to develop techniques for recognising text with misinformation which is generated by large language models, as well as to examine persuasive posts in social media. Investigations have shown that the majority of adults cannot distinguish whether a text has been written by a person or generated by a LLM. This presents us with numerous challenges, starting with the possibility of fraudulent authorship to the automatic dissemination of targeted false information. The efficiency and suitability of current detectors for recognising text generated by LLM is still an active research area. An adaptable benchmarking data record which can handle the influx of LLMs and covers various potential tasks is indispensable for the effective assessment of such recognition systems. One contribution of this project is not least the introduction of a comprehensive data record tailored for the benchmarking of detectors for "Instruction-tuned" LLMs.

### Efficient Language and Dialect Identification for Languages which are Written in Less Widespread Writing Systems

In this project, we concentrate on exploring solutions of dialect classification in non-Latin languages, with a special focus on the Arabic language. The goal is to examine the options of current multi-language models in non-Latin languages. The pre-trained language recognition models to date mainly focus on English and Latin languages (alphabetic fonts are the most frequent font and are used in at least 85% of languages). Experience shows that less widespread fonts could impair the performance of multi-language models, which is why we still have a broad field of research ahead of us. In some cases, the problem is exacerbated by the lack of resources in the target languages (or dialects). This applies in particular for languages which do not use the Latin alphabet known to us. Arabic, which uses a consonant script called Abjad, is spoken by a large community of around 400 million people distributed over several countries and is extraordinarily diverse in its regional language varieties. Arabic is the official language in 22 countries, dialects of which are, however, mutually incomprehensible. Together, they are designated as colloquial or spoken Arabic, as they are only used in conversations and verbally. The main goals of this project are to analyse the multi-language models for non-Latin languages (in this project Arabic), to examine the current solutions for classifying Arabic dialects as well as identifying and developing approaches to improve their performance.

### Assessment of the Robustness of a Large Language Model against its Misuse in the Swiss Cyber Defence Landscape

This project aims to create the initial foundations for the Swiss cyber defence system to be able to prepare for the large-scale deployment of LLMs and the new points of attack associated with such a deployment. This also contributes to the tasks of the CYD Campus to develop resources for defending against novel cyber attacks. To achieve this goal, manual and automatic LLM red teaming, the screening of domain-specific knowledge, and the assessment of distortions at generation and self-censored generation will be used in this project to assess the robustness of the current generation of LLMs against misuse in offensive cyber operations.

The fine tuning of conversation agents of LLMs promises to provide the solution to a long-existing problem in all user interfaces — the ability to hold a complete natural language conversation. Although the advantages of using such applications are tempting, they also harbour a number of vulnerabilities. LLMs are known for the fact that they are susceptible to the circumvention of restrictions — what are known as "jailbreaks". A further LLM application that has attracted much attention and provided for extensive presentations was enabled by its text-to-code abilities. Through the fine tuning of conversation agents, it became more accessible and was made more powerful by further basic LLM pre-training on code-documentation-code pairs. Even if everything seems to point to the fact that some state of the art LLMs can generate sufficiently functional codes to be included in functioning products, the general robustness of these codes against cyber attacks has not been systematically examined to date. The creation of the basis for such a systematic assessment is a further goal of this project. Last but not least, information operations must overcome an important language barrier to be successful in Switzerland. Whether this is possible through the use of LLMs is a question that this project also aims to answer.

### MAXIM: Improvement and Explanation of NMT Systems

The goal of this project is to make the description of the vulnerability of neural machine translation systems (NMT systems) easier. The aim is to clarify how important it is to develop strong defence mechanisms and more robust NMT systems for applications in real life.

In this project, we present various methods for generating attacks on NMT systems. NMT models are susceptible to carefully planned disturbances in their inputs, what are known as adversarial attacks. Even if the adversarial example is semantically similar to the original sentence, the quality of the translation can drastically deteriorate in the case of an untargeted attack, or in the case of a targeted attack lead to the use of certain terms. Untargeted adversarial disturbances will be created in this project such that the adversarial examples contain meaning in the source language and destroy meaning in the target language.

The project provides for two types of adversarial attack. On the one hand, there is the optimisation-based method for generating disturbances, while on the other, the classification-led approach for attacks on neural machine translations. Both methods display an impressive success rate in attacks, both in black box and in white box scenarios.

The disturbance generated in this manner can then be used to make the underlying models more robust in the future.

## Fit on Duty

### Prediction of Collapse

Military staff can be exposed to physically strenuous situations which result from a combination of factors such as sleep deprivation, sustained physical activity, psychological and physical stress, etc.. To reduce the risk of accidents and injuries, it would be advantageous to have a warning system. This should be able to recognise when a person is in such a situation. Based on an assessment of the current state of health, it should be able to establish whether the activity should be interrupted and the person should rest. The goal of the project "Fit on duty" is to develop such a warning system using portable sensors and machine learning (ML). The sensors record the biomedical data of the wearer (heart rate, temperature, acceleration, etc.), on the basis of which a ML algorithm for individual assessment of the current state of health is trained. This year's initial study enabled practical experiences to be obtained by recording biomedical data of military personnel and developing a basic understanding of its quality and the information it contains. The study brought to light some of the logistical and technical challenges with regard to a broad-based application of such a warning system and provided important findings on the requirements which such a warning system needs to meet.

### Biomedical Edge AI

In this cooperation with a Swiss university, we are developing, as a feasibility study, a portable device that is capable of assessing the state of health of its wearer and of issuing warnings in critical situations to avoid accidents and injuries in an ideal case. Thanks to its ability to function autonomously over several days and to analyse, learn and classify the relevant sensor data collected, this device is able to provide information about the wearer's state of health in real time. In addition, it can function as a data collector and a research resource in a distributed framework and enables training of more complex models for machine learning as necessary. Through the use of technologies such as IoT and embedded systems, as well as the utilisation of frameworks such as edge computing and distributed ML, this study shows in an application how the risk of accidents and injuries can be reduced by modern technology.

### Deep Learning for security

In the rapid development of artificial intelligence, large language models (LLMs) have become key elements of modern computer-based linguistics and AI applications. Their unparalleled success in the processing of natural language has not only breached the performance standards but also driven forward integration in various software solutions. While industry uses LLMs to manage user interactions and automate decision processes, this integration also involves new security risks. One outstanding threat is "prompt injection", which is being intensively examined by security centres worldwide. In contrast to conventional attacks on machine learning, this attack can have far-reaching consequences, from unauthorised access to private information to the execution of injected code. In a prompt injection attack, an attacker diverts the LLM from its intended task by injecting a specially designed string which executes an injected payload instead.

We demonstrate that a motivated attacker can considerably increase the effectiveness of such attacks by generating triggers using neural networks, which reliably activate payloads, even in complex prompts. In addition, research projects are underway to examine and possibly increase the robustness and security of LLMs against such attacks.


Dr. Gérôme Bovet welcomes the participants of the CYD Campus conference on AI in Bern


# 7. Technology Monitoring

Cyber threats which utilise the latest information technologies are developing faster than ever before in today's digital world. It is a challenge to stay up to date when analyzing these threats and assessing their potential impact.

**Mission statement** of technology monitoring at the CYD Campus:

| | |
|---|---|
| **Mission** | Our mission to identify, monitor, analyse and forecast trends related to cyber technologies. |
| **Vision** | Our vision is to become a recognised technology observatory in Switzerland and abroad. |
| **Goal** | Our goal is to provide community-driven and technology intelligence that can be translated into action for national security policy, horizon scanning, market research and strategic management. |
| **Values** | Our community works with the following values: scientific, quantitative, exclusive, open (access, sources, data, offices) and collaborative: we connect academia, industry, and government. |

Our mission statement is based on the strategic goals of the National Cyber Strategy (NCS) set out in 2023, which are focused on the analysis of trends, risks and dependencies.[1]

1 https://www.ncsc.admin.ch/ncsc/en/home/strategie/cyberstrategie-ncs.html

The previous NCS for the years 2018 to 2022 underscored the significance of the "Early identification of trends and technologies and knowledge building" in measure 1. To comply with this, the Technology Monitoring team (TM team) is focusing its efforts on the Cyber Strategy DDPS[1] and is specifically addressing the important task of "Trend monitoring and support". This includes carrying out thorough technology and market monitoring, international scouting of start-up companies and maintaining a collaboration network using the different approaches:

### A Scientific and Quantitative Approach

Traditional technology monitoring is based heavily on manual and qualitative methods. To address this, we use the latest advances in big data and artificial intelligence, not only to enable a more quantitative approach but also to integrate predictive procedures and thus improve our technology monitoring. Our approach is mainly based on open data and scientific methods.

Our technology monitoring provides actionable technological foresight to the following decision-makers in Switzerland:

- Swiss Armed Forces (for example, Chief of the Armed Forces, Armed Forces Staff, Armed Forces Cyber Command)
- National Cyber Security Centre (NCSC)
- Federal Office for Defence Procurement armasuisse

In addition, the activities of the technology monitoring contribute to cyber strategies at different levels:

1. National cyber strategy (NCS)
2. Strategy cyber DDPS
3. Overall cyber concept of the Swiss Armed Forces
4. Business architecture of the CYD Campus

### An Approach for an Exclusive Technology and Market Monitoring platform

Our approach is also based on our own internal platform named as Technology and Market Monitoring (TMM), which we develop and maintain in collaboration with government, industry, and academic partners. Our TMM platform aggregates valuable insights which our technology analysts combine with their findings and their scouting expertise to produce comprehensive analyses.

## Large Language Models in the Area of Cyber Security: Threat, Exposure and Mitigation

The TM team carried out a study to provide an overview of the developments, the current state of the art, and the cyber defence implications of generative language models, also known as Large Language Models (LLM).

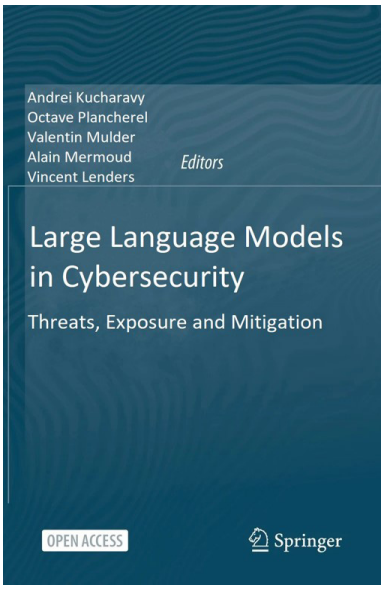
This study, which is publicly available online, provides industry, the federal administration, and academia in Switzerland with detailed insights into the development and risks of LLM.

The study focuses on the impact for Switzerland and the development and current status of the AI models concerned. It provides insights into their capabilities and future threats. Here are some of the insights of the study:

• LLMs can generate misinformation based on unbalanced data in training. On the other hand, this technology can also be misused for active disinformation campaigns. The publication of private information also represents a potential threat. LLMs are trained not only with data that is publicly accessible on the Internet, but also indirectly with user entries in the system. Private data should therefore not be entered in LLMs.

• Search engines with LLM extensions can search the Internet more efficiently and deeply. This means that even "hidden" information such as databases and programme codes only available in the Deep Web — the part of the Internet that is not well indexed and is undetected using a normal search engine search function — can be made public.

• Many of the known threats in cyberspace have become more accessible and better scalable using LLMs. In order to protect the technology from misuse, the use of LLMs must be continuously monitored. People must be made aware of their risks and no private information may be entered. The complete study contains a detailed analysis of the LLM landscape, the limits of LLM, as well as the risks of this technology for cyber defence in Switzerland.




Preview of the new book on LLMs in the area of cyber security, which was compiled in 2023 as part of technology monitoring

1 https://www.vbs.admin.ch/en/sicherheit/cybersicherheit.html#dokumente

## Extension of the TM Team


The technology monitoring activities have been continuously expanded since the CYD Campus was founded in 2019. The team is headed by Dr. Alain Mermoud (front right in the photo). Valentin Mulder (front left in the photo) joined the TM team in mid-2023 as a full-time employee following a successful internship at the CYD Campus in the previous year. In October 2023, the team was further expanded with the joining of Dr. Julian Jang-Jaccard (front center in the photo), a former Professor in New Zealand.

University interns make a key contribution to the technology monitoring team and are involved in a wide range of projects. The names of our interns and their projects (top row from left to right) are as follows:

**Evgueni Rousselot**
Quantum computing monitoring and implementation of Shor's Algorithm

**Daniel Celeny**
Measurement of cyber risks and their costs for stock markets

**Maxime Würsch**
Benchmarks for technology mining using data extraction

**Octave Plancherel**
«Large Language Models in Cybersecurity» Springer book

**Martin Sand**
«Trends in Quantum Technologies and Implications for Cyber-Defense» Springer book

**Thomas Berkane**
Emergence of cybersecurity technologies from an evolutionary perspective

The following short interviews with the two new members of the TM team provide insights into their backgrounds and their contributions.

## Interview with Valentin Mulder

### Which topics did you work on during your internship?

During my internship, I was able to work on various different projects. There were three particularly interesting projects that are worth mentioning. First of all, publishing and coordinating the book "Trends in Data Protection and Encryption Technologies" was a good opportunity to understand how the CYD Campus works together with industry, universities and the public sector. The second of these projects was the start-up challenge, where I learned how the technology transfer of innovative start-up companies to the defence sector can be achieved. And finally, I supported the scouting activity where I built up a network.

### What general advice would you give to future interns for their time at the CYD Campus?

Be flexible and open, because that's the only way to enjoy their internship and realise their full potential. Projects which do not seem so interesting at the beginning can actually often comprise interesting challenges. The fact that we maintain offices in various cities is a major advantage, which can offer great opportunities for establishing a network.

### What was your motivation for accepting an internship at the CYD Campus?

I wanted to work in the area of cyber defence. For me, considerations on how a nation should protect its citizens and its critical infrastructures in a constantly changing technological environment are a problem that is both complex and interesting.

### How did your internship prepare you for your full-time position at the CYD Campus?

The internship was the ideal preparation for my work. I was lucky to be able to work closely with my current supervisor and I have learned a lot from him. In addition, the projects in which I have worked were an amazing test. These two factors have given me a good start for my work in the TM team.

### What position do you currently hold, what do you enjoy most about it and to what extent have your expectations been met in this full-time position?

I would like to pick out three different aspects. The first is the variety of the work, which is never boring. The second is that we can carry out work on our projects independently according to the specified goals. As a result, we are very flexible. And finally the fast development in the cyber defence sector. It is extremely exciting to be at the centre of these changes.

### Where do you see yourself in ten years?

I would like to continue to explore the interfaces between cyber defence, technical progress and their strategical implications.

## Interview with Dr. Julian Jang-Jaccard

Tell us something about your background and your professional experience to date.

Before I joined the CYD Campus, I was a professor and head of the cybersecurity lab at Massey University in New Zealand. Previously, I was a senior researcher at the Commonwealth Scientific and Industrial Research Organization (CSIRO) in Australia. Between my degree in computer sciences and my doctorate, I also worked as a professional software developer for several years.

What can you tell us about culture shocks, experiences or differences between your previous work in New Zealand and the CYD Campus?

The work at the CYD Campus is more structured and customer-oriented than my previous positions. An important part of the working life at the CYD Campus (or generally in Switzerland) seems to be maintaining networks, which includes many events. In addition, this is my first experience with an open office environment as opposed to individual offices. In my opinion, this has both advantages and disadvantages.

What was your motivation for wanting to work at the CYD Campus?

I applied because I can continue my research here in the area of cyber security, which I have been doing for the last 25 years. The CYD Campus appealed to me because it belongs to the Federal Administration and I feel that my work is thus given greater weight at national level.

What position do you currently hold, what do you enjoy most about it and to what extent have your expectations been met in this full-time position?

I am a scientific project manager in the technology monitoring (TM team). Most of all, I enjoy the opportunity of working with new and disruptive technologies and having access to the best experts in Switzerland and beyond.

Where do you see yourself in ten years?

In ten years, I would still like to be doing what I enjoy the most. I would like to carry out research and development work in the area of cyber security, interact with the next generation of cyber security talents and work together with the best people in this field.

## Research Projects

The TM team researches actively together with various organisations. These include both domestic and international partners.

### Benchmark for Technology Mining by Means of Data Extraction

The ever-changing landscape of cybersecurity creates new threats for organizations in maintaining secure and reliable systems. Trends of new threats therefore need to be tracked in real time or as closely as possible. Various technology monitoring methods have been used for this purpose, in particular bibilometric-based trend analyses. It all started with the attempt to observe the development of the technologies behind LLMs with existing methods using Google Trends and OpenAlex. However, the results showed that standard methods were not sufficient. The application of entity extractors to specific texts was therefore examined. First of all, existing entity extractors with pre-prints in the computer sciences (cs) category were examined on arXiv, including LLM-based ones. The results suggested that the entity extractors do not supply any qualitative expressions with which scientific articles could be grouped, due to the non-scientific data records with which they had been trained. That was why a method for extracting relevant compound substantives was implemented, which was based on the structure of sentences and statistical analyses. Using this method, the arXiv listings relevant for cyber security can be more precisely recognised. From the result, it can be concluded that the method provides important findings in a very rapidly developing area such as cyber security. We could thus assume that it is possible to develop knowledge graphs which can be used to measure the indirect impact of technologies.

### Emergence of Cyber Security Technologies from an Evolutionary Perspective

In the dynamic world of cyber security, the emergence and development of technologies takes place very quickly, so that the entire scenario is subject to continuous fluctuations. Traditional methods for monitoring newly emerging technologies and predicting future trends were not sufficiently equipped for dealing with these rapid changes. To address this issue, the project aimed to develop an innovative approach for observing the development of cyber security technologies was initiated. The method was inspired by the theory of evolution and includes concepts such as genetic coding, mutations and adaptation. To test the method, an investigation was carried out into code repositories related to cyber security, such as the platforms on which the source code under development was hosted. Through the analysis of the development of these repositories from the perspective of the new method, important mutations could be recognised which drive development forward.

The insights gained offer the opportunity to predict newly emerging repositories and identify those likely to increase in significance in the future.

### Measurement of Cyber Risks and their Costs for the Stock Markets

In view of the increasing frequency and cost of cyber attacks, cyber insurances contracts become more important. However, the contracts concerned require an in-depth understanding of the systemic cyber risks in the economy as well as the cyber risks at company level. There is currently no readily available score for cyber risks, and only a few or no standardized reporting regulations exist for the rapidly evolving landscape of cyber risks. For this reason, estimating the cyber risks of companies has been challenging using traditional methods that rely on historical data and expert evaluations. To improve this situation, a machine learning model has been trained such that it can quantify the cyber risks of listed stock companies using the disclosures of these companies. By connecting these risk parameters with the fluctuations in the share prices, it is possible to determine the costs of the cyber risks incurred for specific companies and the overall economy. This approach can help cyber insurances, regulators and political decision-makers to better estimate cyber risks and their costs.

### Scientific and Technical Observation with Flowatcher and the Corresponding Tracking of LLM Development

The study aimed to identify influential publications that facilitate the analysis of significant advancements in large generative language models. This study also aimed to enhance our understanding of the potential impact of the developments on the latest technologies and, consequently, on cyber defense in the upcoming years. Traditionally, the widely used platforms such as ScienceDirect, Springer Link, the ACM Digital Library and the bibliographical collection of DBLP are searched for this type of research. This process often works with structured queries of pertaining databases to find relevant publications. As part of this study, we have examined the usefulness of Flowatcher as a supporting tool for the efficient execution of these tasks. Flowatcher is a monitoring platform which enables monitoring results to be collected, processed and disseminated. Flowatcher offers various types of monitoring tools such as alarms, RSS feeds, meta search engines and adding field observations.

### Super Computers and Quantum Computing with regard to Cyber Security using the Database of Web of Science

The goal of the study was the comprehensive investigation of development trends in quantum computing, super computers and cyber security based on the combination of bibliometric and scientometric analysis. As part of the study, we conducted analyses on social networks, performing keyword and cluster analyses to recognize complex links within the scientific subject area. Using the results, key researchers can be recognised who work at the interface of quantum computing and cyber security. They offer insights into the work of the key players in this field. Moreover, the study unveils the world's most influential investors in the relevant areas, making a significant contribution to understanding the research landscape.

### Swiss Technology Observatory and Cooperation with Swissintell

The Swiss Technology Observatory[1] which was established at the Cyber-Defence Campus brings together an interdisciplinary and international research community. Today, the website of the Swiss Technology Observatory is maintained together with Swissintell, the Swiss Association for Market Research, Competitive Intelligence and Strategic Planning (SMCS). This cooperation leads to numerous synergies, particularly in the area of technology monitoring.


Insights into the technology monitoring conference

1 https://technology-observatory.ch/

CYD Campus team members at EPFL


The booth of the CYD Campus at CONNECTED in August 2023, the largest exhibition of the Armed Forces on the topic of digitalisation and cyber in the Swiss Armed Forces

# 8. Innovation

## Results of the Innovation Projects

### Secure Smartphone Communication via 5G/SCION/Threema

Our innovation project centred around two scenarios with Swiss security solutions: Enabling secure communication between private smartphones and an internal Threema setup via the SCION network and 5G.

To test these scenarios, a Threema server was installed at the premises of the CYD Campus which can only be accessed by the SCION network. SCION (Scalability, Control, and Isolation On Next-Generation Networks) is an innovative network architecture which aims to solve several of the problems of the current Internet architecture. It is mainly developed by researchers from ETH Zurich with the goal of creating a more secure, scalable and reliable Internet. Our cooperation with the mobile network operators Swisscom and Sunrise enabled us to connect our setup with the mobile network operators and to offer a seamless user experience. The controlled test environment is an important component in assessing the security of this approach.

As part of this project, we also carried out an evaluation to determine the most robust architecture for a secure smartphone. Here, the workability of the use of a hypervisor for simultaneous execution of several instances of Android on modern smartphones was demonstrated. Our cooperation with partners from industry and students from EPFL in the last two years has led to this approach, which separates the risks effectively.

The availability of secure smartphones with these functions has now become reality and represents an important milestone in our efforts.

### Cyber Toolkit

The exercise Locked Shields offers the perfect opportunity to test new software and configurations, as the infrastructure to be defended (which is made available by the organisers) is representative and the attacks carried out correspond to the latest state of the art. In this context, we conducted Proof-of-Concepts in which we provided various software (both COTS as well as customised software) to the Blue Team of the Swiss Armed Forces for Locked Shields to test during the exercise. The various software components offer an orchestration and harmonised configuration of cyber defence tools. This results in a cyber defence system with extended pro-active anti-virus malware functionalities and network clarification. The most important functionalities include, for example, automated dynamic malware analyses, anticipation through prior analysis of C2 channels, as well as the reconnaissance and monitoring of OT networks and web application firewalls to protect perimeters. The automated defensive endpoint defence is based on AI.

### Blue Team Automation

The project Blue Team Automation aims to automate cyber security tasks and create an autonomous system for cyber defence exercises. By analysing Locked Shields data from 2022, the platform assesses the visibility and detection of Red Team attacks and develops new cyber security methods. A modular defence solution is also being developed which integrates the warnings, IT details and measures for quick reaction to threats. By accessing and consolidating Locked Shields data, decisive findings were obtained on the challenges of Blue Teams. The automated platform identified Red Team activities which led to realisable warnings for automated cyber security reactions. This comprehensive study offers extensive security insights and provides normalised data for broader research utilisation and improved project transparency. It underscores the necessity of events at a deeper level for connecting warnings and introduces rationalised methods for warnings. These achievements pave the way for autonomous cyber security systems which improve attack recognition and response and emphasise the modularity in dealing with threats.

### Perimeter Monitoring with Automatic Object Detection

The innovation project focused on the application of modern technologies of machine learning for reliable object detection in monitoring images. The goal was to create a functioning proof of concept and to build up expertise in the area of machine learning operations. The initiative arose from the necessity of monitoring military airfields and training areas for potentially disruptive objects such as animals or people. A Minimal Viable Product (MVP) was developed within a short time and tested qualitatively in the field. The approach enabled real time monitoring with existing surveillance cameras and AI technology to represent imminent dangers on a 2D map. The system was tested successfully at the military airfield Dübendorf and functioned reliably under various different conditions. The project also improves the knowledge about AI in various areas of the Armed Forces. The aim is to extend the system to include automated camera monitoring and in future to also integrate thermal imaging and infrared cameras to further improve the functionality.

## Cyber Start-up Challenges

### Smartphone Security

The Cyber Start-Up Challenge was held this year for the fourth time. In June 2023, the CYD Campus launched its call for the topic of innovative solutions in the area "Security of smartphone applications and their potential threats". Ten start-ups responded to the call and presented their solutions to the jury, which consisted of cyber experts of the DDPS.

The American start-up Ostorlab won over the jury and presented their innovative methods on the security analysis of mobile applications at the CYD Campus Conference on 26 October 2023. Ostorlab has developed a mobile application scanner which enables organisations to efficiently identify security loopholes in mobile applications, both in Android and in iOS applications.

Ostorlab uses static and dynamic analysis methods to identify vulnerabilities which can cause considerable damage to the security and reputation of companies. These range from security breaches to data leaks and compromised communication. Other potential vulnerabilities are unauthorised accesses, obsolete software components, exposed sensitive information, poor encryption practices and insecure data transmissions.

Ostorlab's mobile application scanner also supports Software Bill of Materials (SBOM) files to detect obsolete and vulnerable dependencies. In addition, the scanner also has automated app interactions for comprehensive security tests and holds a strong track record in detecting and reporting critical vulnerabilities, which underscores its efficiency.

### Firmware Security Analysis

The security of networked devices such as building controls, access control systems and surveillance cameras presents a major challenge, as these devices can often not be seamlessly integrated into monitoring processes. This leads to potential risks through unclear security standards in local networks.

One solution is offered by the firmware analysis platform of ONEKEY, which detects vulnerabilities in devices without being connected with the sensitive networks.

During a ten-month proof-of-concept as part of the Cyber Start-up Challenge 2022, the CYD Campus put the effectiveness of the ONEKEY platform to the test. An assessment scheme has been developed which can be used to classify the networked devices easily and display compliance with the minimum security requirements. During the PoC, the firmware images of more than 60 IoT devices were analysed with regard to vulnerabilities and compliance violations. In the course of this, numerous vulnerabilities were identified and were assigned Common Vulnerabilities and Exposures numbers (CVE numbers).

Finally, processes regarding patch management, vulnerability management and asset management were outlined, to demonstrate how such a platform can be integrated on an automated basis.

### Privacy-preserving Cyber Threat Intelligence Sharing

Work with the young Swiss company Decentriq, the winner of the Cyber Start-up Challenge 2021, was continued. The challenge focused on the topic "Boost your Information Sharing and Analysis Center (ISAC)". Decentriq offers a Software as a Service (SaaS) platform which enables secure and private data cooperation. Decentriq offers "data clean rooms" which enable event data to be exchanged and anonymous findings to be obtained without jeopardising data protection. Decentriq uses a "confidential computing" technology to ensure that nobody, including the platform operator, has direct access to the data. The platform thus offers a solution for the target conflict between the joint use of sensitive data and its protection. We have completed successful cooperation with important players in the Swiss financial sector: the Zurich Cantonal Bank, the Swiss National Bank and SIX. Our joint focus was on sensitive cyber attack data, with the goal of increasing the security of critical infrastructures in our country and simultaneously protecting the privacy of its data. Building on this success, we are continuing to expand our partnership with Decentriq and are aiming to implement this initiative throughout the entire financial sector.


Dr. Colin Barschel (right in the photo) when the winner of the Start-up Challenge 2023 was announced

Group photo of the Ostorlab teams, winner of the Cyber Start-up Challenge 2023

# 9. International Scouting and Cooperations

## Scouting

In 2023, CYD Campus start-up scouting focused on Switzerland, the USA, Israel, the United Kingdom and France, with some companies in other countries. The scouting focused on new technologies in the areas of cyber security and AI, to identify the most important trends and players at an early stage. Interviews were held with around 100 start-ups and companies. The results of these interviews were forwarded in structured form to potential interested parties in public administration.

To gain access to the most interesting start-ups and to identify companies in the early phase, the CYD Campus relies on a broad network that extends from venture capitalists to accelerators and embassies as well as business support organisations. The most important partners include the Swisscom branch office in Silicon Valley and the Swissnex network. A further important scouting instrument is the participation in leading world conferences such as the RSA Conference in San Francisco, Black Hat, Defcon, USENIX Security, Cybertech and Cyberweek in Tel Aviv as well as the European Cyber Week in Rennes. These events offer the opportunity to meet a large number of companies and partners within a short time.

The start-ups identified in the scouting activities led to several proof-of-concepts. In addition, the information gained was used to support the procurement process and for better understanding of the cyber market.

## International Cooperation

Cooperation with international partners is essential in cyberspace. As threats and malicious players do not respect national borders, Switzerland relies on close cooperation. The international cooperation is also one of the three strategic pillars of the newly launched Swiss Armed Forces strategy 2030.

### Research Partnerships

The CYD Campus conducts research projects with scientists from the world's leading universities such as the University of Oxford, the University of Southern California and the Ruhr University Bochum.

### Multinational Cooperation

The CYD Campus also works together with international organisations. The CYD Campus thus represents Switzerland at the CapTechs Cyber and Information of the European Defence Agency. As required, the discussions on specific projects will be intensified and CYD Campus researchers will check whether a contribution from Switzerland is appropriate. These bodies also serve as platforms for informal exchange between experts. The CYD Campus is thus leading Swiss efforts for possible participation in a future PESCO project in the area of the Cyber Ranges Federation (CRF). The goal of the CRF is to improve the performance of the European Cyber Ranges (CR) by merging existing national Cyber Ranges into one larger cluster. NATO is also an important cooperation partner. The CYD Campus makes an important contribution to the activities of the CCDCOE in Tallinn, both through the local presence of our researcher William Blonay as well as through research contributions to their work programme. In 2023, William Blonay was promoted to "Green Team Leader" for the cyber exercises of the centre. In addition, the Campus also participates selectively in interesting STO work groups of NATO. These projects are supported by the armasuisse executive office in Brussels.

### Bilateral Exchanges

The bilateral exchange with partner organisations of the DDPS in selected countries in Europe, America and Asia is also of major importance. The CYD Campus works together both with larger countries which it provides with highly-specialised expertise, as well as with smaller, agile partners who are faced with similar challenges. Depending on the partner country, the aim is to find researchers with similar interests in order to exchange expertise, methods and data or, in certain cases, to conduct research projects together. This work encompasses all areas and domains of the campus, from technology and market surveillance to cyber security, data knowledge and applications of machine learning. The CYD Campus works together closely with the armasuisse office in Washington, the Swiss embassies and the defence attachés all over the world to coordinate and manage the projects.

### The Cyber-Defence Campus as a Model Example

Ultimately, the CYD Campus is a leading global example of successful cooperation between the government, universities and industry. Each year, delegations from various countries visit the CYD Campus to learn about its best practices. In efforts to strengthen global cyber resilience, the CYD Campus is endeavouring to share its knowledge with like-minded people and partners.

### Advanced Course in Engineering (ACE)

The Advanced Course in Engineering (ACE) is a summer internship programme focusing on cyber defence and management which is organised by the United States Air Force Research Lab. The programme combines training in the basic principles of cyber security with practical applications in simulated cyber scenarios. The trainees take part in lectures, research projects, deployments in a simulated cyber war zone and leadership seminars, which culminate in a final exercise. The programme focuses on the development of technical, leadership and problem-solving skills in a contested cyber environment. Simon Kindhauser, intern at the CYD Campus, led the Swiss Delegation in the advanced course in engineering in summer 2023 and made an important contribution to the programme.

# 10. Customer & Portfolio Assessment

The cyber deployment of the Swiss Confederation is split up into three areas in accordance with the cyber strategy:

- Cyber security (FDF)
- Cyber defence (DDPS)
- Cyber prosecution (FDJP)

The CYD Campus, as part of cyber defence, provides its primary service for its direct organisations of armasuisse, the military organisations of defence and the Federal Intelligence Service. A key feature of the customer orders 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.

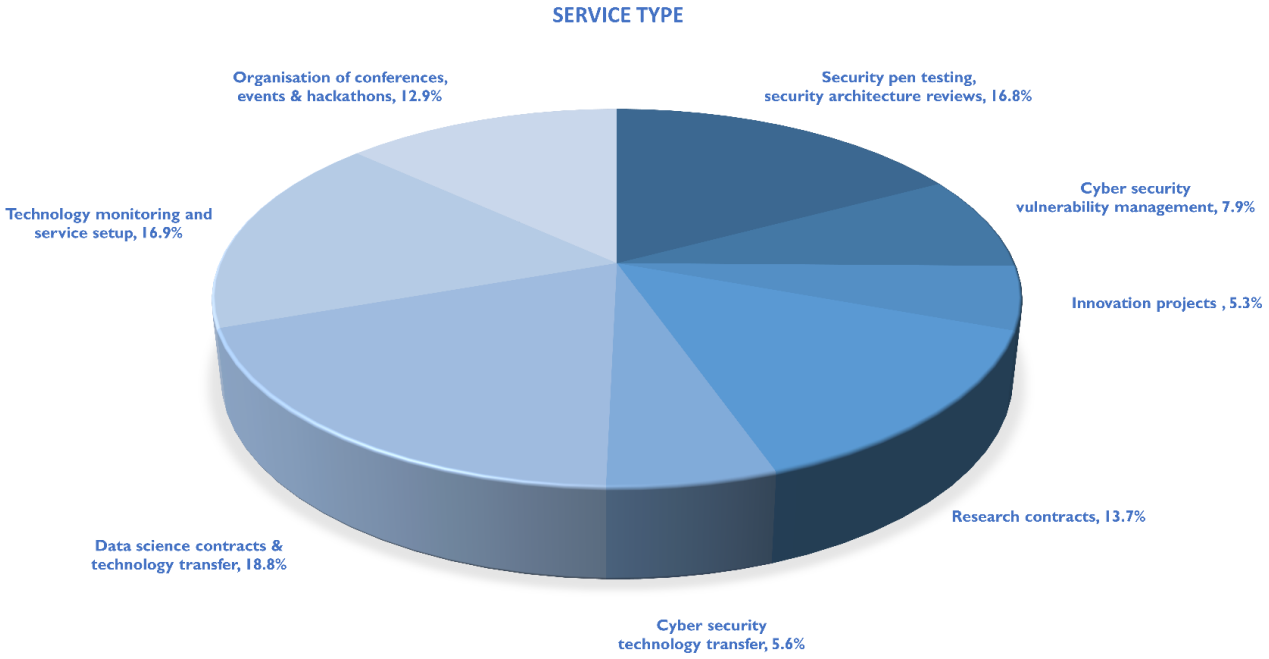
The Cyber Security group provided its services in 2023 - for the various customer groups in the key topics of security assessment in applications and thus made an important contribution to security in the systems examined.

In its work, the data science group supported technology transfer to build new capabilities in defence as well as studies for the use of new AI technologies for image, language, signal and data evaluation.

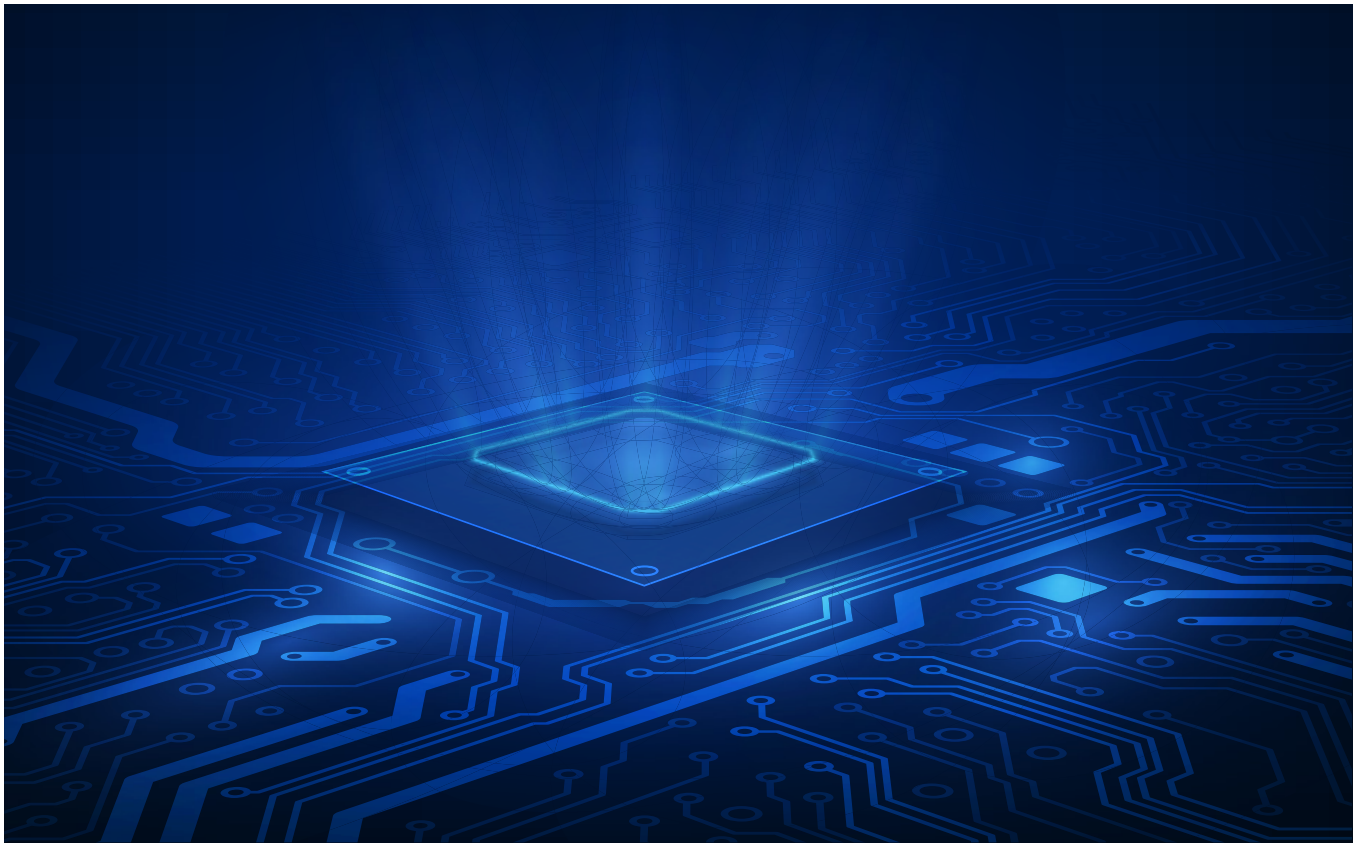
Technology monitoring – as a new group of the Cyber-Defence Campus – has been increasingly used by various organisations in defence and made a contribution in the early phase of procurement to clarify the usability of new cyber technologies and for overarching studies on the proof of the technological maturity level in designated areas of cyber defence.

In 2023, the CYD Campus provided work for the following organisations:

- Federal Office for Defence Procurement armasuisse
- Group Defence
  - Armed Forces Staff
  - Armed Forces Cyber Command project
  - 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




Detailed display of the direct contractual services and services for all portfolio groups



# 11. Security Services

In 2023, employees of the CYD Campus examined the security of military systems which were processed as part of defence and ICT procurement in the DDPS. The examinations were conducted as security analyses, penetration testing and security consultations. In most cases, the clients were the purchasing bodies of armasuisse.

In 2023, there were more than 30 investigations, in particular of the following objects:

- Web applications
- Specialist applications
- Middlewares
- Computer networks
- Various end devices and server systems
- Communication solutions
- Security solutions and architectures
- C2 systems
- Vehicles
- Aviation and satellite communication systems

Unfortunately, the objects examined, as well as the results of the examinations, may not be listed by name for classification reasons, nor may their vulnerabilities be shown. The exceptions are Commercial-of-the-Shelf (COTS) products, for which the discovered vulnerabilities are reported via CVE number and advisory and attributed to the CYD Campus as discoverer.

However, to gain an insight into the highlights of the work, two examples will be presented in anonymised form and the list of published vulnerabilities included:

### Pentesting of a Specialist Application

The goal of the task was to conduct pen testing on a newly developed web-based application, to check the associated web application firewall and its authentication solution. The examination was conducted according to a white box approach.

The vulnerability with the highest level of criticality used the key of a hard-coded RSA key which was accessible in a code repository, and which was used by the attacker who created their own user to acquire the rights of an existing user. As the underlying Identity and Access Management solution has been used for other applications, the vulnerability shown was overarching and had to be eliminated immediately as an emergency measure.

### Security Assessment Secure Boot

In the security assessment Secure Boot, the suitability of hardware-based security measures in the boot process was analysed in a customer end device. To what extent the measures allow operation of a safe operating system should be verified.

In the examination of the security solution, eight medium and two critical vulnerabilities were identified, whereby the critical vulnerabilities allowed an attacker to manipulate the boot process and to degrade the security solution. With the degraded security solution, a compromised boot process is possible and the secure operating system is deprived of the basis for operative use.

Both examples illustrate the added value of the safety assessments and the indispensability of checking systems, products and software components of security-critical systems and providing proof of secure operative usage.

The table below lists the vulnerabilities published in 2023. The vulnerabilities marked with * were found by several entities and reported to the manufacturer before they became known. In such cases, the CVE number is typically attributed to the entity which reported the vulnerability first.

| Hardware / software | CVE & reports | Date | CVSS |
|---|---|---|---|
| Fortiguard | CVE-2022-40682 | March 23 | 7.1 |
| Fortiguard | CVE-2022-40682 | April 23 | 7.8 |
| Sharekey (19 vulnerabilities) | Report | April 23 | 10 |
| OPSWAT MetaDefender Kiosk | CVE-2023-36657 | September 23 | 5.9 |
| OPSWAT MetaDefender Kiosk | CVE-2023-36659 | September 23 | 6.2 |
| FortiClient (Windows)* | CVE-2022-40681 | October 23 | 7.1 |
| Bleachbit | CVE-2023-47113 | October 23 | 7.8 |
| FortiClient (Windows)* | CVE-2023-41840 | November 23 | 7.4 |

List of the published and reported vulnerabilities of hardware and software components examined in 2023

# 12. Laboratories

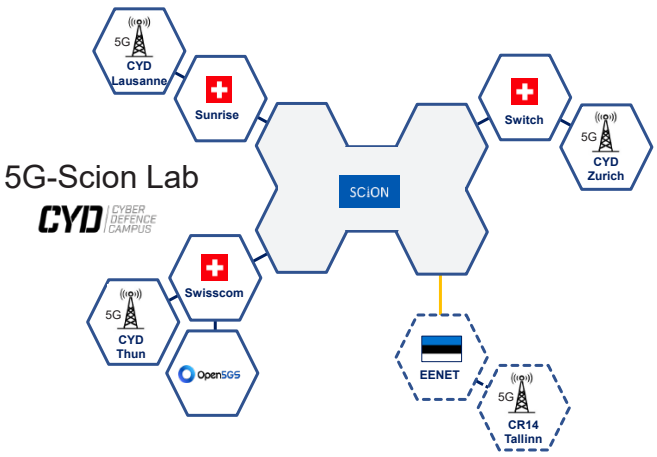
The Cyber-Defence Campus operates a variety of laboratory infrastructures and permanent test infrastructures at its three locations, which are available for research projects, tests and demonstrations:

- WAN SCION Testbed (Thun, Lausanne and Zurich)
- 5G Lab (Thun)
- Cyber Avionics Laboratory (Thun)
- SATCOM Laboratory (Thun, Lausanne and Zurich)
- Hardware Security Lab (Thun)
- Data Science Laboratory (Thun)
- Security Lab (Thun)
- Hardware Security Lab (Thun)
- ICS Laboratory (Thun)
- IoT Laboratory (Thun)

This year, these laboratories were expanded in various areas.

## WAN SCION Test Bed

In order to demonstrate international use cases via SCION, an extension of the SCION WAN test bed was performed with a new SCION network node in Tallinn, Estonia. The network node in Tallinn connects the Estonian cyber range of Cybexer with the CYD Campus at its three locations via a native SCION network. The international SCION connection to Tallinn is established via Switch and Géant and demonstrates the ability to provide a secure SCION-based WAN over several countries and Internet providers.

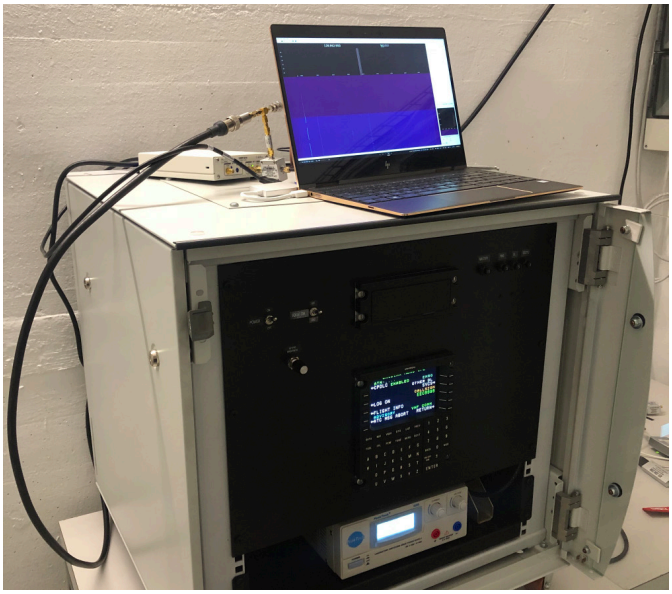



## 5G Lab

In 2023, the 5G laboratory was extended by a 5G standalone core network (5G SA) with the open source software Open5GS and two radio access points with several mobile devices. The radio access points are in Thun and Zurich and are connected with the 5G core via SCION. We could thus test and explore this important new technology and use it for training purposes. The core is virtualised and runs in our data centre. This enables end-to-end tests of the security of this new protocol to be conducted. Part of the work is carried out in cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and the German Central Office for Information Technology in the Security Sector (ZITiS).

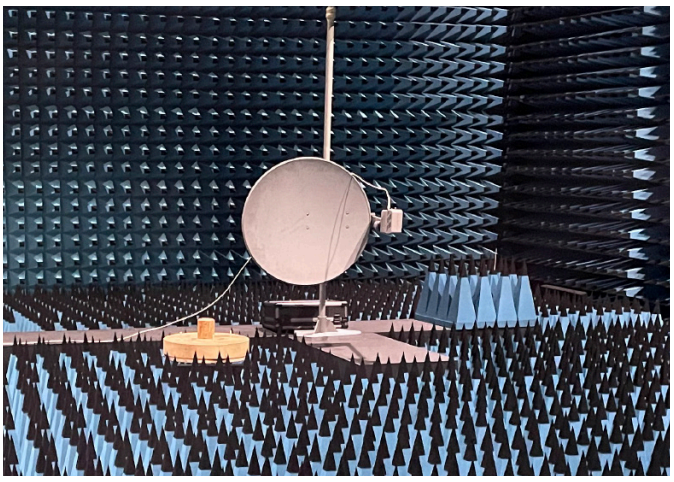

## Cyber Avionics Lab

The Cyber Avionics Lab was extended by two commercial multilateration systems (MLAT) in the canton of Zurich. The MLAT systems were tested in practice for their resilience against spoofing. Cyber attacks against the collision avoidance system TCAS were successfully tested for the first time in the Cyber Avionics Lab in Thun. The examination of countermeasures is underway. The data link CPDLC was examined in the lab in cooperation with Skyguide and Eurocontrol with regard to its practical security. Hardware and software tools have been developed for the data bus ARINC 429 of the laboratory, which enable full control over the bus. This helps in the analysis of attacks and countermeasures.



## SATCOM Lab

The SATCOM Lab was expanded by the installation of a stationary 2.4 metre antenna on the roof of our office in Thun. This enabled a broad reception and analysis of various satellite systems. Mobile extensions are planned for 2024. In addition, various cooperations with commercial operators of ground stations were started. A security analysis of the aviation data link ADS-C has been carried out. It was demonstrated how unprotected satellite connections are used to accept satellite modems from a distance.



## Hardware Security Lab

In our new Hardware Security Lab, analyses and tests can now be performed to check the security of embedded systems and IoT devices. The aim is to identify vulnerabilities in hardware and software components, as well as examine potential physical attacks and the associated possible extraction of data and information. The laboratory will make a contribution to checking secure and protected hardware components for procurement and vulnerability research in order to comply with the high requirements for information security.

## Data Science Lab

The Cyber-Defence Campus operates a Data Science Lab (DSL). In the DSL, various components have been renewed as part of life cycle activities. In order to meet the ever-increasing demand for storage space, the storage space will now be provided by Storage Area Network (SAN) and the data backup will be carried out via a hardware platform, which will provide up to one petabyte of disk storage in a minimum of space. This infrastructure enables big data and AI projects to be conducted in the lab.

# 13. Activities

### Visits

- 25/1/2023: Visit Deputy Chief of Armament at the CYD Campus, Lausanne
- 13/2/2023: Visit Cyber Training Course, Thun
- 9/3/2023: Visit GCSP Military Attaché Training Course, Thun
- 22/3/2023: Cyber Hub of the Federal Armed Forces, Thun
- 5/4/2023: NTC visits the CYD Campus, Zurich
- 12/4/2023: Chief of Armament Finland, Thun
- 26/4/2023: Swisscom Ventures visits the CYD Campus, Zurich
- 26/4/2023: KaPo ZH visits the CYD Campus, Zurich
- 5/5/2023: Visit Officers' Association Cyber in the CYD Campus, Zurich
- 12/5/2023: Visit Head of Swisscom Ventures at CYD Campus, Lausanne
- 13/6/2023: Visit Federal Office for Civilian Service, Thun
- 13/6/2023: Visit SiPol GS DDPS, Thun
- 28/6/2023: Visit Accenture, Zurich
- 6/9/2023: Visit Lucerne University of Applied Sciences and Arts and AFCSO, Zurich
- 11/9/2023: Data Science: Data as an intervention resource, visit squad air force brigade 31, Thun
- 17/10/2023: Visit TLG Cyber, Thun
- 13/11/2023: Visit GS DDPS & participants ada Fellowship DDPS, Thun
- 15/11/2023: Visit Chief of AFCC Estonia, Thun
- 14/12/23: Visit A Plan, Thun

### Events

- 2/5/2023: Research report Data Science & Cyber Security
- 19 - 23/6/2023: Cyber-Alp Retreat, Sachseln
- 27/6/2023: Workshop on Deep Content Generation and Cyber Influence Operations, Zurich
- 16 - 20/08/2023: Connected 2023, Kloten
- 11 - 15/09/2023: ICS Trainings and Hackathon, Thun
- 20 - 22/09/2023: Swarm Intelligence Workshop, Zurich
- 08 - 14/10/2023: Data Science Hackathon
- 16 - 20/10/2023: Car Security Training and Hackathon, Thun
- 26/10/2023: CYD Campus Conference, Bern
- 16/11/2023: Technology Monitoring Seminar, Lausanne
- 23/11/2023: Year-end event, Bern

### Visits Abroad

- 25/1 – 2/2/2023: Technology monitoring and Cybertech, Israel
- 27/2 – 4/3/2023: SpaceSec Workshop and NDSS, USA
- 4/2023: Participation in Locked Shields, Estonia
- 23/3 – 24/3/2023: NATO STO SET-322, Paris, France
- 22/3 – 24/3/2023: University of Oxford, England
- 17/4 – 28/4/2023: RSA Conference und Scouting, USA
- 26/4 - 27/4/2023: CySat, Paris
- 16/5 – 18/5/2023: ICMCIS & NATO IST panel, Skopje, Macedonia
- 30/5 - 2/6/2023: CyCon, Estonia
- 1/6 - 18/08/2023: Air Force Research Labs, USA
- 15/6/2023: PESCO Federated Cyber Ranges, Estonia
- 29/6 - 30/6/2023: EDA CapTech Cyber, Luxembourg
- 19/7 – 27/7/2023: Army Research Office L & ICML, USA
- 6/8 - 14/8/2023: Usenix Security, Defcon, Blackhat, Swisscom Outpost, USA
- 2 - 5/10/2023: DASC Conference, Barcelona, Spain
- 4/10 - 10/10/2023: Scouting UK, London, England
- 5 - 14/10/2023: Data Science Hackathon, Spain
- 27/10 – 6/11/2023: Army Research Labs & MILCOM, USA
- 30 - 31/10/2023: OpenSky Symposium, Toulouse, France
- 6 - 09/11/2023: Conference VMWare Explore, Barcelona
- 20 - 23/11/2023: European Cyber Week Rennes, France
- 26/11 - 1/12/2023: ACM CCS, Copenhagen
- 4/12 - 08/12/2023: GLOBECOM, Malaysia


Participants in ICS hackathon 2023 in Thun

# 14. Presentations

- 28/2/23: Cyber Intelligence Europe conference & exhibition, Bern
- 03/3/2023: SCION National Testbed for Cyber Defence, Anapaya, Zurich
- 08/3/2023: Can legislation and standardisation support aviation becoming more cyber resilient?, Airspace World, Geneva
- 16/3/2023: Encryption 2025, ICT Warrior Tech Talk, Bern
- 21/3/2023: Cyber impacts on aircraft and Air Ops, AFST, Aarau
- 29/3/2023: ISSS Israeli and Swiss Innovation In Cyber Security, Rotkreuz
- 26/4/2023: Swiss Night @RSA, San Francisco
- 09/5/2023: Protecting data in the digital age, Digital Day 2023
- 14/6/2023: Workshop "ADINT", Emmenbrücke
- 27/6/2023: Workshop "Deep Content Generation and Cyber Influence Operations", Zurich
- 12/8/2023: Elon, Twitter and the PIA: How not to achieve Privacy in Aviation, DEFCON, USA
- 12/8/2023: Labs and Trust: How to build a successful aviation cybersecurity research programme, DEFCON, USA
- 13/8/2023: The Looming Perils for End Users in SATCOM, DEFCON, USA
- 30/8/2023: Protecting data in the digital age, NDB, Bern
- 01/9/23: Securing Critical Network Infrastructures, Uni Luxembourg
- 14/9/2023: SBFI Workshop Cyber Research Cooperation, Bern
- 19/9/2023: ERFA 2023, ar Immo, Airolo/Olivone
- 18/10/2023: Scion @ CYD Campus, Scion Day, Zurich
- 23/10/2023: Cyber Training @ CYD Campus, Bern
- 22/11/2023: Security Academy 2023 "IT Services of the Future in the DDPS", Bern
- 6 - 7/12/2023: Drone Remote ID spoofer and low cost receiver application, Black Hat Europe, London


Dr. Christa Zoufal from IBM Research presents on quantum machine learning at the CYD campus conference 2023


Dr. Martin Burkhart presents opportunities and challenges of self-sovereign identities (SSI)

# 15. Scientific Publications

## December

Behavioral fingerprinting to detect ransomware in resource-constrained devices
Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Jan von der Assen, Dennis Shushack, Ángel Luis Perales Gómez, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, Computers & Security 2023;135:103510

LLMs perform poorly at concept extraction in cyber-security research literature
Maxime Würsch, Andrei Kucharavy, Dimitri Percia David & Alain Mermoud, arXiv

## November

Efficient collective action for tackling time-critical cybersecurity threats
Sébastien Gillard, Dimitri Percia David, Alain Mermoud & Thomas Maillart, Journal of Cybersecurity 2023;9(1)

Watch This Space: Securing Satellite Communication through Resilient Transmitter Fingerprinting
Joshua Smailes, Sebastian Köhler, Simon Birnbach, Martin Strohmeier & Ivan Martinovic, CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Copenhagen, Denmark.

## October

A first look at exploiting the Automatic Dependent Surveillance-Contract Protocol for open aviation research
Marc Xapelli, Tobias Lüscher, Giorgio Tresoldi, Vincent Lenders & Martin Strohmeier, Opensky Symposium, Toulouse, France

Assessing the sustainability and trustworthiness of federated learning models
Alberto Huertas Celdran, Chao Feng, Pedro Miguel Sanchez Sanchez, Lynn Zumtaugwald, Gérôme Bovet & Burkhard Stiller, arXiv

Lessons learned in transcribing 5000 h of air traffic control communications for robust automatic speech Understanding
Juan Zuluaga-Gomez, Iuliia Nigmatulina, Amrutha Prasad, Petr Motlicek, Driss Khalil, Srikanth Madikeri, Allan Tart, Igor Szoke, Vincent Lenders, Mickael Rigault & Khalid Choukri, Aerospace 2023;10(10):898

MTD-Based Aggregation Protocol for Mitigating Poisoning Attacks on DFL
Chao Feng, Alberto Huertas Celdran, Michael Vuong, Gérôme Bovet & Burkhard Stiller, arXiv

OpenSky Report 2023: Low Altitude Traffic Awareness for Light Aircraft with FLARM
Xavier Olive, Martin Strohmeier, Junzi Sun & Giorgio Tresoldi, DASC 2023, Digital Avionics Systems Conference, Barcelona, Spain

P3LI5: Practical and confidEntial Lawful Interception on the 5G core
Francesco Intoci, Julian Sturm, Daniel Fraunholz, Apostolos Pyrgelis & Colin Barschel, 2023 IEEE Conference on Communications and Network Security (CNS), Orlando, USA

Scaling the Timing-Based detection of anomalies in Real-World aircraft trajectories
Lukas Baege, Patrick Schaller, Vincent Lenders & Martin Strohmeier, Opensky Symposium, Toulouse, France

Sentinel: an aggregation function to secure decentralized federated learning
Chao Feng, Alberto Huertas Celdran, Janosch Baltensperger, Enrique Tomas Martinez Beltran, Gérôme Bovet & Burkhard Stiller, arXiv

SKYPOS: Real-world evaluation of self-positioning with aircraft signals for IoT devices
Yago Lizarribar, Domenico Giustiniano, Gérôme Bovet & Vincent Lenders, IEEE Journal on Selected Areas in Communications 2023;42(1):134-145

Stealth Spectrum Sensing Data Falsification Attacks Affecting IoT Spectrum Monitors on the Battlefield
Pedro Miguel Sánchez Sánchez, Enrique Tomás Martínez Beltrán, Alberto Huertas Celdrán, Robin Wassink, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM), Boston, USA

## September

A Relaxed Optimization Approach for Adversarial Attacks Against Neural Machine Translation Models
Sahar Sadrizadeh, Clément Barbier, Ljiljana Dolamic & Pascal Frossard, 31st European Signal Processing Conference (EUSIPCO), Helsinki, Finland

A novel algorithm for informed investment in cybersecurity companies and technologies
Anita Mezzetti, Loïc Maréchal, Dimitri Percia David, William Blonay, Sébastien Gillard, Michael Tsesmelis, Thomas Maillart & Alain Mermoud, In: Cyberdefence: The Next Generation (p. 87-101)

Anticipating cyberdefense capability requirements by link prediction analysis
Santiago Anton Moreno, Dimitri Percia David, Alain Mermoud, Thomas Maillart & Anita Mezzetti, In: Cyberdefence: The Next Generation (p. 135-145)

Cybersecurity Ecosystems: A network study from Switzerland
Cédric Aeschlimann, Kilian Cuche & Alain Mermoud, In: Cyberdefence: The Next Generation (p. 123-134)

Decentralized Federated Learning: fundamentals, state of the art, frameworks, trends, and challenges
Enrique Tomás Martínez Beltrán, Mario Quiles Pérez, Pedro Miguel Sánchez Sánchez, Sergio López Bernal,Gérôme Bovet, Manuel Gil Pérez, Gregorio Martínez Pérez & Alberto Huertas Celdrán, IEEE Communications Surveys and Tutorials 25(4):2983-3013

Identification of future cyberdefense technology by text mining
Dimitri Percia David, William Blonay, Sébastien Gillard, Thomas Maillart, Alain Mermoud, Loïc Maréchal & Michael Tsesmelis, In: Cyberdefence: The Next Generation (p. 69-86)

Identifying emerging technologies and influential companies using network dynamics of patent clusters
Michael Tsesmelis, Ljiljana Dolamic, Marcus M. Keupp, Dimitri Percia David & Alain Mermoud, In: Cyberdefence: The Next Generation (p. 103-122)

Social media influence operations
Raphael Meier, arXiv

## August

CyberForce: a federated reinforcement learning framework for malware mitigation
Chao Feng, Alberto Huertas Celdran, Pedro Miguel Sanchez Sanchez, Jan Kreischer, Jan von der Assen, Gérôme Bovet, Gregorio Martinez Perez & Burkhard Stiller, arXiv

FABRID: Flexible Attestation-Based Routing for Inter-Domain Networks
Cyrill Krähenbühl, Marc Wyss, David Basin, Vincent Lenders, Adrian Perrig & Martin Strohmeier, 32nd USENIX Security Symposium, Anaheim, USA

Network fingerprinting via timing attacks and defense in software defined networks
Beytüllah Yiğit, Gürkan Gür, Fatih Alagöz & Bernhard Tellenbach, Computer Networks 2023; 232:109850

## July

Byzantine-Resilient Learning Beyond Gradients: Distributing Evolutionary Search
Andrei Kucharavy, Matteo Monti, Rachid Guerraoui & Ljiljana Dolamic, GECCO '23 Companion: Companion Conference on Genetic and Evolutionary Computation, Lisbon, Portugal

Evolutionary Algorithms in the Light of SGD: Limit Equivalence, Minima Flatness, and Transfer Learning
Andrei Kucharavy, Rachid Guerraoui & Ljiljana Dolamic, The 2023 Conference on Artificial Life, Sapporo, Japan

LWHBench: a low-level hardware component benchmark and dataset for single board computers
Pedro Miguel Sánchez Sánchez, José María Jorquera Valero, Alberto Huertas Celdrán, Gérôme Bovet, Manuel Gil Pérez & Gregorio Martínez Pérez, Internet of Things 2023;22:100764

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, arXiv

Moving Target Defense Strategy Selection against Malware in Resource-Constrained Devices
Jan Von der Assen, Alberto Huertas Celdrán, Nicolas Huber, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy

## June

A Federated Defense Framework Using Cooperative Moving Target Defense
Chao Feng, Jan von der Assen, Alberto Huertas Celdrán, Steven Näf, Gérôme Bovet & Burkhard Stiller, 8th International Conference on Smart and Sustainable Technologies (SpliTech), Split, Croatia

A Trustworthy Federated Learning Framework for Individual Device Identification
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, JNIC Cybersecurity Conference, Vigo, Spain

Building Collaborative cybersecurity for Critical Infrastructure Protection: Empirical evidence of Collective intelligence information sharing Dynamics on ThreatFox
Eric Jollès, Sébastien Gillard, Dimitri Percia David, Martin Strohmeier & Alain Mermoud, In: Critical Information Infrastructures Security. CRITIS 2022. Lecture Notes in Computer Science, vol 13723 (p.140-157)

FedStellar: a platform for decentralized federated learning
Enrique Tomás Martínez Beltrán, Ángel Luis Perales Gómez, Chao Feng, Pedro Miguel Sánchez Sánchez, Sergio López Bernal, Gérôme Bovet, Manuel Gil Pérez, Gregorio Martínez Pérez & Alberto Huertas Celdrán, arXiv

Forecasting Labor Needs for Digitalization: A bi-partite graph Machine learning approach
Dimitri Percia David, Santiago Anton Moreno, Loïc Maréchal, Thomas Maillart & Alain Mermoud, World Patent Information 73:102193

From scattered sources to Comprehensive Technology Landscape: A recommendation-based retrieval approach
Chi Thang Duong, Dimitri Perica David, Ljiljana Dolamic, Alain Mermoud, Vincent Lenders & Karl Aberer, World Patent Information 73:102198

GraphINC: Graph Pattern mining at network speed
Rana Hussein, Alberto Lerner, Andre Ryser, Lucas David Bürgi, Albert Blarer & Philippe Cudre-Mauroux, Proceedings of the ACM on Management of Data. 2023;1(2):1-28

LLM-Based Entity Extraction is Not for Cybersecurity
Maxime Würsch, Andrei Kucharavy, Dimitri Percia-David & Alain Mermoud, Joint Workshop of the 4th Extraction and Evaluation of Knowledge Entities from Scientific Documents and the 3rd AI + Informetrics (EEKE- AII2023), New Mexico, USA

MTFS: a Moving Target Defense-Enabled file system for malware mitigation
Jan von der Assen, Alberto Huertas Celdrán, Rinor Sefa, Gérôme Bovet & Burkhard Stiller, arXiv

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, arXiv

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, arXiv

Targeted Adversarial Attacks Against Neural Machine Translation
Sahar Sadrizadeh, AmirHossein Dabiri Aghdam, Ljiljana Dolamic & Pascal Frossard, ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Rhodes, Greece

## May

A Framework for Wireless Technology Classification using Crowdsensing Platforms
Alessio Scalingi, Domenico Giustiniano, Roberto Calvo-Palomino, Nikolaos Apostolakis & Gérôme Bovet, IEEE INFOCOM 2023 - IEEE Conference on Computer Communications, New York, USA

A lightweight moving target defense framework for multi-purpose malware affecting IoT devices
Jan von der Assen, Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Jordan Cedeño, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, arXiv

A Simplified Training Pipeline for Low-Resource and Unsupervised Machine Translation
Àlex R. Atrio, Alexis Allemann, Ljiljana Dolamic & Andrei Popescu-Belis, Proceedings of the The Sixth Workshop on Technologies for Machine Translation of Low-Resource Languages (LoResMT 2023), Dubrovnik, Croatia

Capturing Trends Using OpenAlex and Wikipedia Page Views as Science Indicators: The Case of Data Protection and Encryption Technologies
Sarah Ismail, Alain Mermoud, Loic Marechal, Samuel Orso & Dimitri Percia David, 27th International Conference on Science, Technology and Innovation Indicators (STI 2023), Leiden, Netherlands

Contrastive learning with self-reconstruction for channel-resilient modulation classification
Erma Perenda, Sreeraj Rajendran, Gérôme Bovet, Mariya Zheleva & Sofie Pollin, IEEE INFOCOM 2023 - IEEE Conference on Computer Communications, New York, USA

Early Detection of Cryptojacker Malicious Behaviors on IoT Crowdsensing Devices
Alberto Huertas Celdrán, Jan von der Assen, Konstantin Moser, Pedro M. Sánchez Sánchez, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, USA

Evaluating the security of power conversion systems against electromagnetic injection attacks
Marcell Szakály, Sebastian Köhler, Martin Strohmeier & Ivan Martinovic, arXiv

Evolutionary algorithms in the light of SGD: limit equivalence, minima flatness, and transfer learning
Andrei Kucharavy, Rachid Guerraoui, Ljiljana Dolamic & arXiv

FirmwareDroid: Towards Automated Static Analysis of Pre-Installed Android Apps
Thomas Sutter & Bernhard Tellenbach, 2023 IEEE/ACM 10th International Conference on Mobile Software Engineering and Systems (MOBILESoft), Melbourne, Australia

Modeling 5G Threat Scenarios for Critical Infrastructure Protection
Gerrit Holtrup, William Blonay, Martin Strohmeier, Alain Mermoud, Jean-Pascal Chavanne & Vincent Lenders, 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia

Optimizing the Size of Subword Vocabularies in Dialect Classification
Vani Kanjirangat, Tanja Samardžić, Ljiljana Dolamic & Fabio Rinaldi, Tenth Workshop on NLP for Similar Languages, Varieties and Dialects (VarDial 2023), Dubrovnik, Croatia

Satellite Spoofing from A to Z: On the Requirements of Satellite Downlink Overshadowing Attacks
Edd Salkield, Marcell Szakály, Joshua Smailes, Sebastian Köhler, Simon Birnbach, Martin Strohmeier & Ivan Martinovic, WiSec '23: Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Guildford, UK

SecBox: A Lightweight Container-based Sandbox for Dynamic Malware Analysis
Jan von der Assen, Alberto Huertas Celdrán, Adrian Zermin, Raffael Mogicato, Gérôme Bovet & Burkhard Stiller, NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, USA

Towards Generalizing Machine Learning Models to Detect Command and Control Attack Traffic
Lina Gehri, Roland Meier, Daniel Hulliger & Vincent Lenders, 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia

## April

Data in Transit Security
Roland Meier, In: Trends in Data Protection and Encryption Technologies (p. 135-139)

Differential Privacy
Valentin Mulder & Mathias Humbert, In: Trends in Data Protection and Encryption Technologies (p. 157-161)

Electronic Voting
Louis-Henri Merino, In: Trends in Data Protection and Encryption Technologies (p. 129-133)

Hardware Acceleration
Dina Mahmoud, In: Trends in Data Protection and Encryption Technologies (p. 109-114)

Identity-Based Cryptography
Bernhard Tellenbach, In: Trends in Data Protection and Encryption Technologies (p. 59-64)

In Pursuit of Aviation Cybersecurity: Experiences and lessons from a Competitive approach
Martin Strohmeier, Mauro Leonardi, Sergei Markochev, Fabio Ricciato, Matthias Schäfer & Vincent Lenders, IEEE Security & Privacy 2023; 21(4):61-73

Robust and explainable identification of logical fallacies in natural language arguments
Zhivar Sourati, Vishnu Priya Prasanna Venkatesh, Darshan Deshpande, Himanshu Rawlani, Filip Ilievski, Hông-Ân Sandlin & Alain Mermoud, Knowledge-Based Systems 266:11041

Scientometric and Wikipedia Pageview Analysis
Alexander Glavackij, Sarah Ismail & Percia David Dimitri, In: Trends in Data Protection and Encryption Technologies (p. 243-252)

Secure Multi-Party Computation
Louis-Henri Merino & José Cabrero-Holgueras, In: Trends in Data Protection and Encryption Technologies (p. 89-92)

Secure Operating System
Llorenç Romá & Bernard Tellenbach, in: Trends in Data Protection and Encryption Technologies (p. 115-120)

Secure Positioning and Localization
Martin Strohmeier, In: Trends in Data Protection and Encryption Technologies (p. 187-192)

TaxoComplete: Self-Supervised Taxonomy Completion Leveraging Position-Enhanced Semantic Matchin
Ines Arous, Ljiljana Dolamic & Philippe Cudré-Mauroux, Proceedings of the ACM Web Conference 2023 (WWW '23), Austin, USA

## March

A methodology to identify identical single-board computers based on hardware behavior fingerprinting
Pedro Miguel Sánchez Sánchez, José María Jorquera Valero, Alberto Huertas Celdrán, Gérôme Bovet, Manuel Gil Pérez & Gregorio Martínez Pérez, Journal of Network and Computer Applications 212:103579

Channel and hardware impairment data augmentation for robust modulation classification
Erma Perenda, Gérôme Bovet, Mariya Zheleva & Sofie Pollin, TechRxiv

CyBERSPEC: Behavioral fingerprinting for intelligent attacks detection on crowdsensing spectrum sensors
Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, IEEE Transactions on Dependable and Secure Computing

Early warning signals of social instabilities in Twitter data
Vahid Shamsaddini, Henry Kirveslahti, Raphael Reinauer, Wallyson Lemes de Oliveira, Matteo Caorsi & Etienne Voutaz, arXiv

Fundamentals of Generative large language Models and Perspectives in Cyber-Defense
Andrei Kucharavy, Zachary Schillaci, Loïc Maréchal, Maxime Würsch, Ljiljana Dolamic, Remi Sabonnadiere, Dimitri Percia David, Alain Mermoud & Vincent Lenders, arXiv

Measuring Security Development in Information Technologies: A Scientometric framework using ARXIV e-Prints
Dimitri Percia David, Loïc Maréchal, William Lacube, Sébastien Gillard, Michael Tsesmelis, Thomas Maillart & Alain Mermoud, Technological Forecasting and Social Change 188:122316

## February

A deep learning approach to predict collateral flow in stroke patients using radiomic features from perfusion images
Giles Tetteh, Fernando Navarro, Raphael Meier, Johannes Kaesmacher, Johannes C. Paetzold, Jan S. Kirschke, Claus Zimmer, Roland Wiest & Bjoern H. Menze, Frontiers in Neurology; 14

FederatedTrust: a solution for trustworthy federated learning
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Ning Xie, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, arXiv

Large-scale transient peri-ictal perfusion magnetic resonance imaging abnormalities detected by quantitative image analysis
Manuel Köstner, Michael Rebsamen, Piotr Radojewski, Christian Rummel, Baudouin Jin, Raphael Meier, Uzeyir Ahmadli, Kaspar Schindler & Roland Wiest, Brain communications;5(2)

QPEP in the Real World: A Testbed for Secure Satellite Communication Performance
Julian Huwyler, James Pavur, Giorgio Tresoldi & Martin Strohmeier, Workshop on Security of Space and Satellite Systems (SpaceSec) 2023

Spoofing Earth Observation Satellite Data through Radio Overshadowing
Edd Salkield, Sebastian Kohler, Simon Birnbach, Richard Baker, Martin Strohmeier & Ivan Martinovic, Workshop on Security of Space and Satellite Systems (SpaceSec) 2023, San Diego, USA

TransFool: an adversarial attack against neural machine translation models
Sahar Sadrizadeh, Ljiljana Dolamic & Pascal Frossard, arXiv

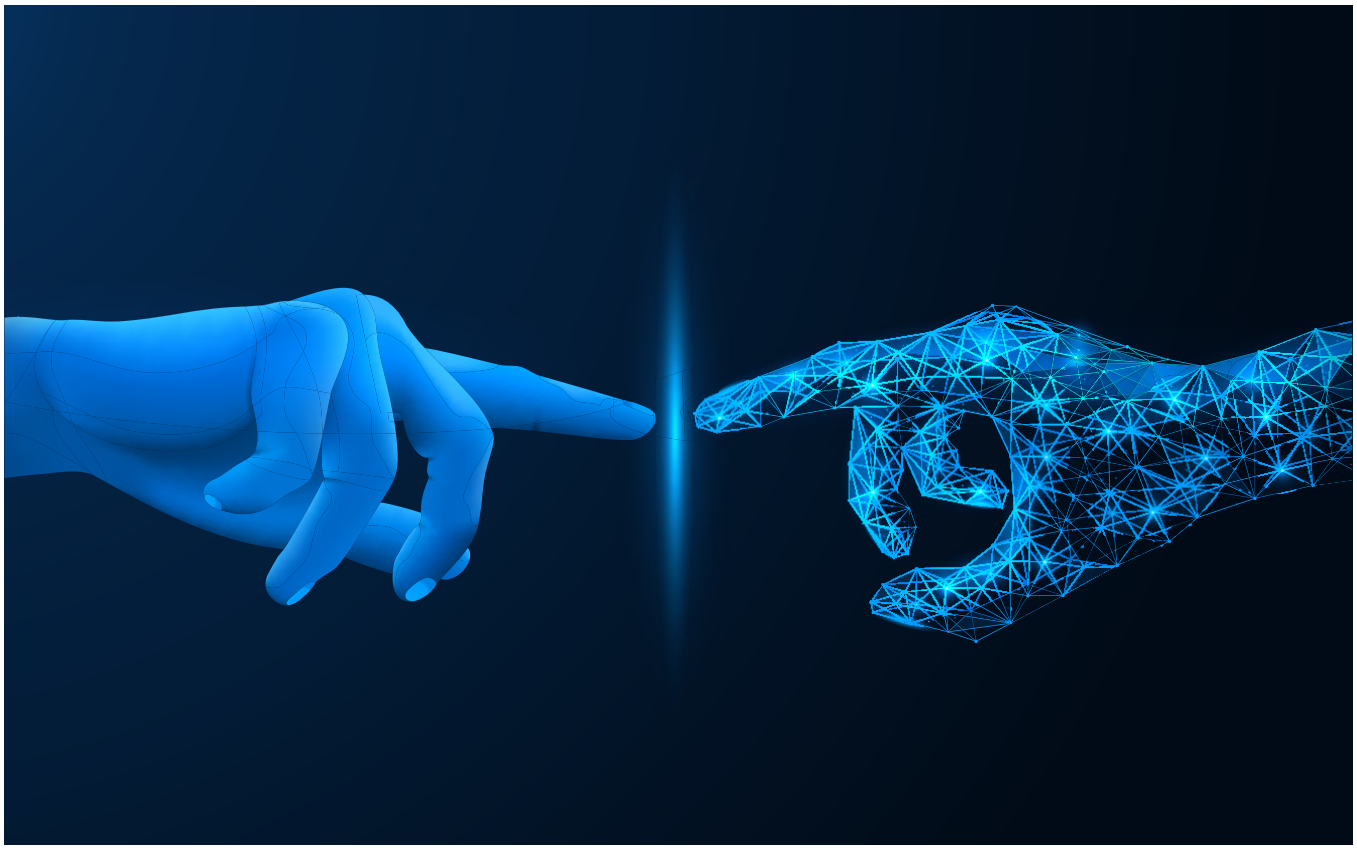
## January

Adaptive uplink data compression in spectrum crowdsensing systems
Yijing Zeng, Roberto Calvo-Palomino, Domenico Giustiniano, Gérôme Bovet & Suman Banerjee, IEEE ACM Transactions on Networking

Analysis of GNSS disruptions in European airspace
Michael Felux, Benoit Figuet, Manuel Waltert, Patric Fol, Martin Strohmeier & Xavier Olivé, Proceedings of the Institute of Navigation. International Technical Meeting, Long Beach, USA

Case-Based reasoning with language models for classification of logical fallacies
Zhivar Sourati, Filip Ilievski, Hông-Ân Sandlin & Alain Mermoud, arXiv

Robust federated learning for execution time-based device model identification under label-flipping attack
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, José Rafael Buendía Rubio, Gérôme Bovet & Gregorio Martínez Pérez, Cluster Computing



# 16. Communication

The significance of communication in the cyber area cannot be emphasised enough. The rapid development of technologies, as for example in the area of AI tools with ChatGPT, requires continuous reporting. It is also important, for example, to clarify potential risks to the public, as well as to promote the exchange between cyber experts and between the Swiss Confederation, industry, the Armed Forces and universities.

Pro-active communication plays a key role for the CYD Campus to make the public aware of cyber topics and to promote the cyber area both at a national and an international level. Over the last year, we have been able to successfully implement significant communication measures to increase the awareness of cyber defence in Switzerland, as well as globally.

## Increase in our Publication Activity

In 2023, we published an impressive 80 specialist articles and twelve public announcements dealing with current challenges and developments in the area of cyber security in Switzerland and the entire world.

## Growth on Social Media

Through the continuous publication of content on our social media channels, we have been able to increase our online visibility on a targeted basis. We were able to gain almost 2,100 new followers on LinkedIn and expand our reach in the cyber community to over 5,000 followers.

## Go Live with our Website

In September 2023 we were able to go live with our website cydcampus.admin.ch. Here, we offer comprehensive insights into our diverse projects and programmes through publications, cooperations and various events at the CYD Campus.

## Press Releases

The publication of Internet and press releases was important to inform internal as well as external target groups about important events and developments in the CYD Campus. We use press releases to provide insights into new studies, announce events such as hackathons or conferences and report on our cyber trainings.

## Selection of Public Announcements

### Press Releases

- Successful cooperation between the DDPS and the Swiss financial sector to protect privacy, 28/4/2023
- Cyber-Defence Campus launches 2023 Cyber Start-up Challenge, 8/6/2023
- Cyber Start-up Challenge 2023: Start-up Ostorlab convinces the DDPS, 26/10/2023

### Web Notifications

- Collaborative approach to eliminating gaps in cyber security, 27/2/2023
- The Cyber-Defence Campus publishes its 2022 Annual Report, 3/3/2023
- CYD Proof of Concept Fellowship, 16/4/23
- Call for the 2023 Cyber Start-up Challenge, 8/6/2023
- New Cyber-Defence Campus Internet presence, 20/9/2023
- CYD Campus examines the cyber security research landscape in Switzerland, 29/9/2023
- Cyber-Defence Campus Hackathon on Forensics in Energy Systems, 24/10/2023
- Security in the age of AI: Opportunities and risks, 2/11/2023
- Cyber threats of generative artificial intelligence, 22/11/2023

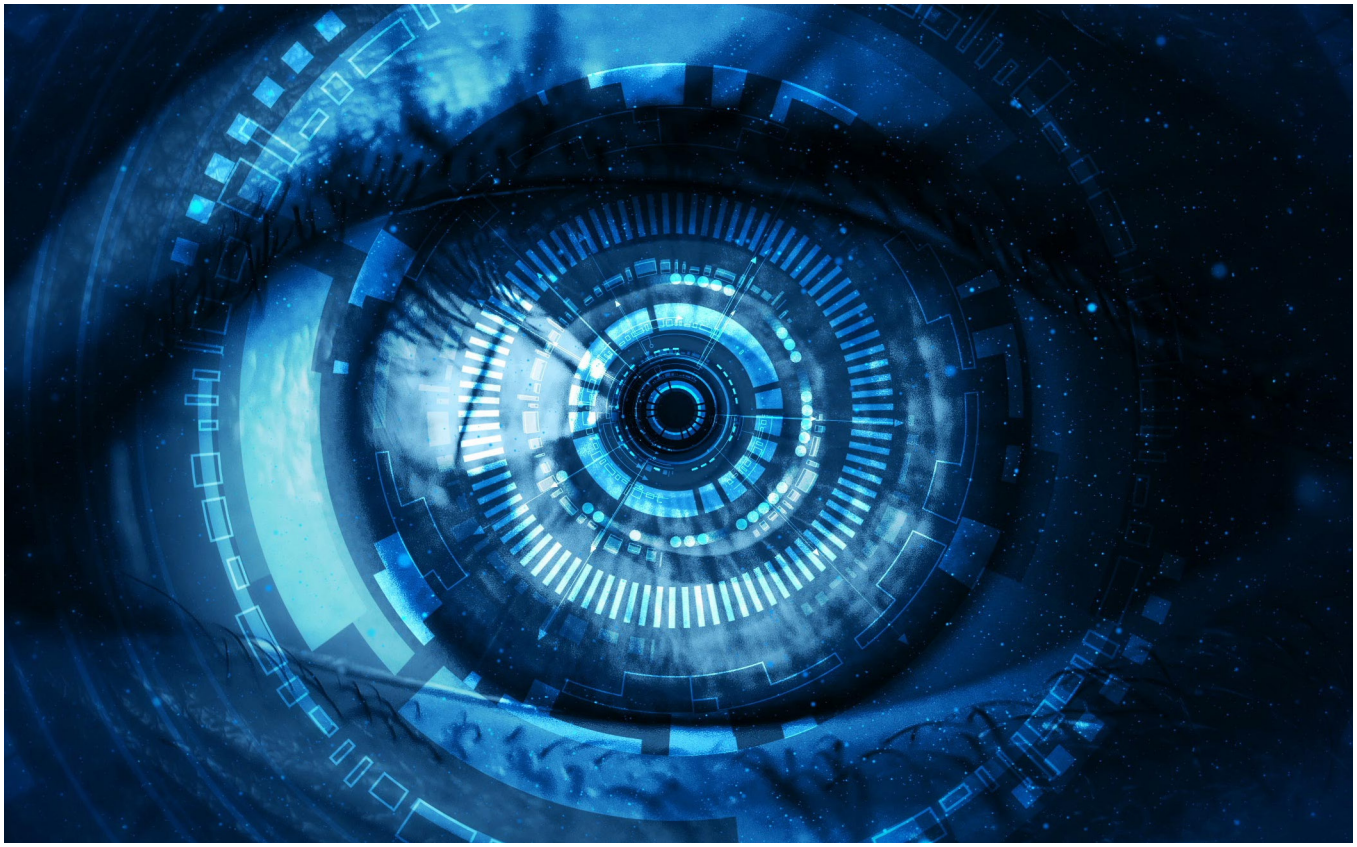
## Visit us on:

Our website

LinkedIn

X

The communication team of the CYD Campus at work



# Outlook 2024

In 2024, the Cyber-Defence Campus will celebrate its fifth anniversary. After five years, we will continue to focus on intensifying our collaboration with industry, universities and partners in Switzerland and abroad. We have set ourselves the goal of making an active contribution to security in the ongoing digitalisation to drive innovation in the field of cyber defence and to develop important foundations. The aim is to equip the Swiss cyber defence ecosystem and the Armed Forces for the future.

In 2024, the Cyber-Defence Campus will focus on implementing the cyber strategy of the DDPS Department, the National Cyber Strategy NCS of the Swiss Confederation and the overall cyber concept of the Armed Forces. This includes:

Training Experts and Driving Forward Innovations: Important events will be taking place again to specifically promote innovation and training of experts in the cyber area. A Cyber-Defence Conference for 2024 as well as various cyber training sessions and hackathons are already being planned. Students can also benefit from our programmes and attractive offers at various levels.

Monitoring Technological Trends: Due to the rapid development in the cyber area, it is relevant to recognise technological trends and developments early on in order to take efficient action against potential risks. The Cyber-Defence Campus will therefore continue to drive forward with the expansion of its Technology Monitoring Platform (TMM 2.0). The goal is to search through existing databases, websites and directories more efficiently to identify cyber technologies and trends early on and to classify their potential for Switzerland.

Strengthening International Cooperations: As in previous years, the Cyber-Defence Campus will focus its activities on strengthening international cooperations. The international cooperation in the area of cyber security, artificial intelligence and disruptive technologies will represent one of our priorities, be it with regard to bilateral relations or to multinational bodies (EDA, NATO, etc.).

Expansion of Communication: A further goal is to use the communication channels of the Cyber-Defence Campus more actively in order to share key findings and publications and to strengthen the cyber community through exchange with subject matter experts. Expert opinions and technological recommendations should be made accessible to a wider audience in order to increase cyber resilience in Switzerland.

Research on Emerging and Disruptive Technologies: The Cyber-Defence Campus will deal with emerging and disruptive technologies such as 5G/6G, artificial intelligence, future network technologies, space and quantum technologies, to examine their potential for Swiss Cyber Defence and the Swiss Armed Forces.

Cooperation with the Armed Forces: In 2024, the Cyber-Defence Campus plans to further develop its cooperation with the Armed Forces Cyber Command and the Cyber Battalion 42. The goal is to support skill development in the newly founded Armed Forces Cyber Command as part of the overall cyber concept and to create synergies together with Battalion 42, launched in 2022, and with members of the Armed Forces.


Dr. Vincent Lenders is already looking forward to the coming year at the CYD Campus

**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, Pixabay, 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