Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport
armasuisse
Science and technology

Cyber-Defence Campus

Annual Report 2022

CYD
CYBER DEFENCE CAMPUS

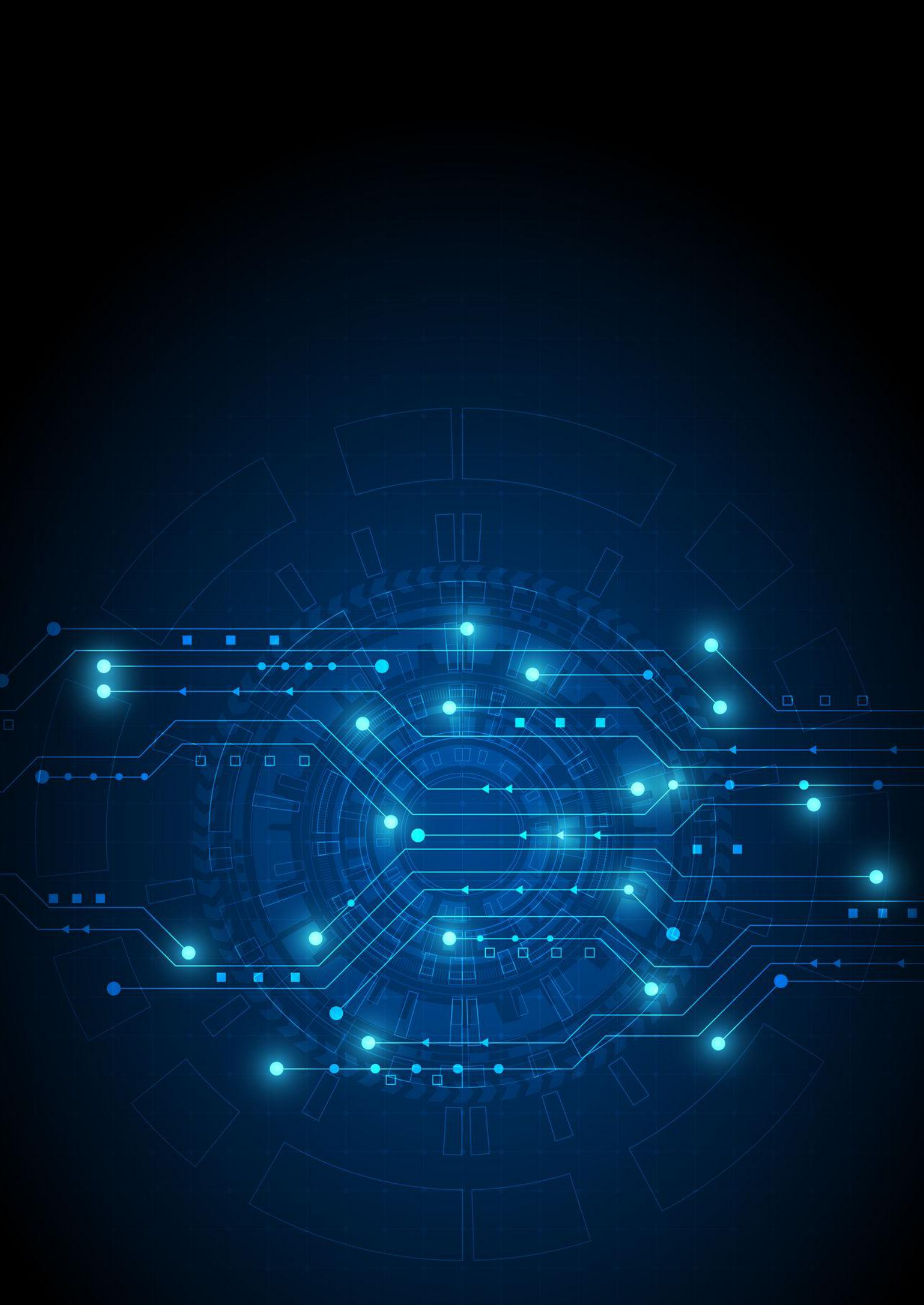


Table of Contents

MPRINT

Publisher: Cyber-Defence Campus, armasuisse, Feuerwerkerstrasse 39, CH-3602 Thun

Contact: +41 58 480 59 34, cydcampus@armasuisse.ch

Image reference: Where not stated differently: Source DDPS/DDPS, Pixabay, Adobe Stock

Foreword

The year 2022 was a special year both in terms of security policy and technology.
At the beginning of the year, Russia launched a military attack on Ukraine. The cyber incidents associated with the invasion highlight that the use of cyber means to support military action has become the norm. As a result of increasing international interconnectedness and interdependence, cyber attacks are likely to have cross-border effects and can thus also pose a threat to Swiss facilities. According to the 2022 supplementary report to the "Security Policy Report 2021", direct cyber attacks against targets in Switzerland can be expected in an escalating situation.

Two months after the invasion of Ukraine, the Swiss Armed Forces presented the General Concept Cyber. This concept shows how the Armed Forces should further develop their capabilities in the cyber domain. The Armed Forces must be able to protect themselves and actively ward off threats. The implementation of the strategy will take place gradually with the development of a cyber command in 2024 and will last until the 2030s. In December, the Federal Council decided to establish a new Federal Office for Cyber Security within the DDPS. The planned Federal Office is to provide a national reporting and point of contact for cyber attacks, disseminate information and warnings and raise awareness among the population for protection against attacks from the network and also protect the federal administration from cyber attacks.

2022 was also a groundbreaking year for developments in the field of artificial intelligence. The company OpenAI unveiled two AI-based systems, DALL-E 2 and ChatGPT, which are able to automatically generate images respectively texts of such high quality that they approximate human abilities. The impact for cyber defence, the CYD Campus and society in general is significant. As Federal Councillor Viola Amherd pointed out at the REAIM 2023 conference in The Hague, the use of artificial intelligence in defence can offer many opportunities, but at the same time risks and ethical aspects must be taken into account.
A lot happened at the CYD Campus in 2022. Looking back, we have made significant progress in the fourth year since the CYD Campus was founded. For example, the number of partner organisations working with the CYD Campus has increased to more than 60. I am particularly pleased that we were able to expand the number of study places. In 2022, 13 students from Swiss universities had the opportunity to conduct their research as CYD Fellows and another 39 students completed a university internship or a master's thesis as part of the talent development programme at the CYD Campus. We managed to effectively network and significantly strengthen the Swiss cyber community thanks to our events such as the CYD Campus Conference in Bern, the Cyber Alp Retreat in Sachseln, the conducted hackathons, the Cyber Startup Challenge and Jam Sessions. We also succeeded in intensifying international cooperation, for example by sending one of our cyber experts to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, for a three-year period.
In November, the new premises of the CYD Campus at Zollstrasse 62 in Zurich were inaugurated together with ETH Zurich and our industrial partners, offering us significantly more space for the joint implementation of projects and events with our partners. In 2022 alone, over 50 projects were conducted across locations and over 30 scientific papers were published. A highlight, for example, was the establishment of a national testbed for network security, which links the three CYD Campus locations (Thun, Lausanne and Zurich) via ETH Zurich's innovative SCION technology.
These encouraging developments contribute to our mission: improving cyber defence in Switzerland.

This annual report provides information about the public, unclassified activities of the CYD Campus in 2022. I hope you will enjoy reading it.

Thun, 31. January 2023

Dr Vincent Lenders
Director of the Cyber-Defence Campus

1 About the Cyber-Defence Campus

1.1 Strategy Embedding and Key Tasks

Due to the changing ecosystem and the increasing threat of cyber attacks in all spheres of life, the Swiss government has made cyber security a central and national security concern. The Federal Department of Defence, Civil Protection and Sport (DDPS) is increasing the allocation of resources to cyber defence and making it a strategic and operational priority. For this reason, the first Action Plan for Cyber Defence (APCD) was created in 2016. In view of the rapid further development of the cyber threat situation over the past five years, a new Cyber DDPS Strategy has been elaborated for the period 2021–2024, building on the Action Plan. Both the Action Plan and the new Strategy Cyber DDPS are aligned with the overarching National Strategy for the Protection of Switzerland against Cyber Risks (NCS).

Strategy Cyber DDPS 2021 - 2024

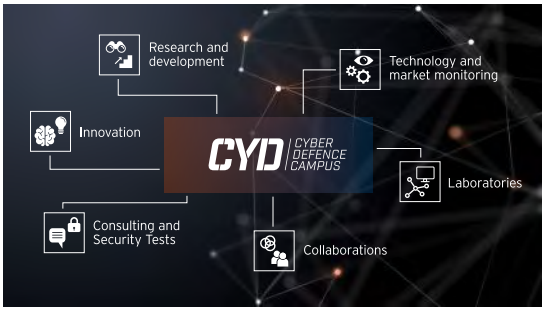
As part of the APCD and the "Cyber DDPS Strategy", the Cyber Defence (CYD) Campus has been developed and operated in the DDPS for four years. It is located at the Federal Office for Defence Procurement (armasuisse). The CYD Campus offers the DDPS an anticipation and knowledge platform for identifying and assessing technological, economic and social cyber trends. In order to be able to cooperate as closely as possible with the universities, the DDPS and industry, the CYD Campus is represented at three locations: at the main location in Thun (armasuisse Science and Technology), at the Innovation Park at the EPFL in Lausanne and, since this year, at Zollstrasse 62 in Zurich. This allows it to efficiently build up know-how and provide cyber expertise according to the needs of the Swiss Confederation. The new location in Zurich in particular allows the CYD Campus to create an ideal environment for collaboration and to provide room for new talents thanks to its larger premises.

Consequently, the CYD Campus acts as a nexus between industry, government administration and academia. In the orientation of the "Cyber DDPS Strategy", the head of the DDPS, Federal Councillor Viola Amherd, defines the fields of action and the corresponding distribution of tasks. Today, the CYD Campus has the following three key tasks:

Early identification of trends in the cyber sector: This includes comprehensive technology and market monitoring, international scouting of startups and the fostering of a collaboration network.

Research and innovation of cyber technologies: Through collaboration with academia and industry, emerging cyber risks are identified and innovative solutions are developed to effectively counter threats in the cyber space. In addition, the CYD Campus aims to ensure and enhance the security and resilience of existing cyber systems.

Training of cyber specialists: At the CYD Campus, talents at Master, PhD and postdoc level as well as university interns are trained for future challenges. In addition, CYD Campus experts define and supervise numerous student projects.



Core competencies of the Cyber-Defence Campus

The aim of this annual report is to provide insights into the realisation of the above-mentioned tasks in 2022 of the Cyber-Defence Campus. In doing so, a brief summary of some highlights of 2022 will be provided. Public activities in research projects, customer mandates and demonstrators will also be discussed. Furthermore, activities in 2022 related to the expansion of laboratory infrastructures are addressed and technology and market monitoring activities are described. The final chapters of this report provide an overview of events, publications, presentations and an outlook for 2023.

1.2 Partners

The CYD Campus is organizationally located at armasuisse Science and Technology (DDPS). About 60 other national and international organisations from academia, industry and the public sector contribute as partners.

Public Partners/Federation	Higher Education	Industrial Partners
National		
Swiss Armed Forces	Bern University of Applied Sciences (BFH)	Adnovum
Federal Department of Foreign Affairs (FDFA)	École polytechnique fédérale de Lausanne (EPFL),	Anapaya
Federal Office of Civil Aviation (FOCA)	Center for Digital Trust (C4DT)	Astrocast
Federal Intelligence Service (FIS)	Eidgenössische Technische Hochschule Zürich (ETHZ)	Brunner Elektronik AG
Federal Office of Police (fedpol)	Northwestern Switzerland University of Applied Sciences and Arts	CYSEC
National Cyber Security Center (NCSC)	Haute École du Paysage, d'Ingénierie et d'Architecture de Genève (HEPIA)	Decentriq
Federal Statistical Office (FSO)	HES-SO Valais-Wallis	FLARM Technology
Swisstopo	Lucerne University of Applied Sciences and Arts (HSLU)	IBM Research
Swissnex	School of Engineering and Management Vaud (HEIG-VD)	Kudelski Security
	Military Academy at ETH Zurich	Noser Engineering
	Eastern Switzerland University of Applied Sciences (OST)	RUAG
	Scuola universitaria professionale della Svizzera italiana (SUPSI)	Swisscom
	University of Fribourg	Tune Insight
	University of Geneva	
	University of Lausanne	
	University of Neuchâtel	
	University of St.Gallen	
	University of Zurich	
	Zurich University of Applied Sciences (ZHAW)	
	Zurich Information Security and Privacy Center (ZISC)	
International		
Federal Office for Information Security (BSI), DE	KU Leuven, BEL	Countercraft
European Defence Agency EDA	TU Kaiserslautern, DE	CybExer Technologies
KRITIS	IMDEA, ESP	ONEKEY
Luxembourg Armed Forces	University of Luxembourg	Plug and Play
NATO CCDCOE	Universidad de Murcia, ESP	Sero Systems
US Department of Defense	Universidad Rey Juan Carlos, ESP	
	University of Oxford, UK	
	University of Southern California (USC), USA	
	Northeastern University, USA	

List of all the Partners of the Cyber-Defence Campus in 2022

1.3 People

The direction of the CYD Campus consists of employees of the department Cyber Security and Data Science of armasuisse S+T.

CYD Campus Direction

Dr Vincent Lenders

Director of the CYD Campus and Head of Department

Dr Bernhard Tellenbach

Head of Cyberspace Research Programme and Cyber Security Group

Stefan Engel

Head of Business Development and Deputy Director of the CYD Campus

Dr Colin Barschel

Head of Innovation and Industry Collaborations

Dr Gérôme Bovet

Head of Research Programme and Data Science Group

Dr Alain Mermoud

Head of Technology and Market Monitoring

Giorgio Tresoldi

Head of International Relations and Scouting

Personnel Focus Cyber Security

Dr Martin Strohmeier is an expert in the security of cyber-physical systems and scientific project manager

Daniel Hulliger is a pentester, vulnerability researcher and technical project manager

Damian Pfammatter is a pentester, vulnerability researcher and scientific project manager

Llorenç Roma is a pentester and scientific project manager

Dr Daniel Moser is an expert in wireless communication security, a pentester and a scientific project manager

Dr Miguel Keer is a scientific project manager

Dr Roland Meier is an expert in network security and scientific project manager (joined in November 2022)

William Lacube is responsible for the collaboration with the NATO CCDCOE in Estonia and is a scientific project manager

Dr Carlo Matteotti is a cryptologist and supervises students and CYD Fellows as a CYD mentor

Personnel Focus Data Science

Dr Ljiljana Dolamic is an expert in Natural Language Processing and a scientific project manager

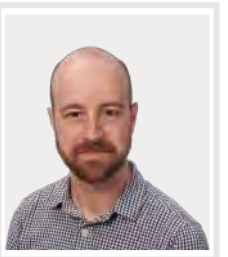
Dr Metin Feridun is a Big Data specialist and a scientific project manager (retired in October 2022)

Ivo Stragiotti is responsible for laboratory infrastructures and is a technical project manager

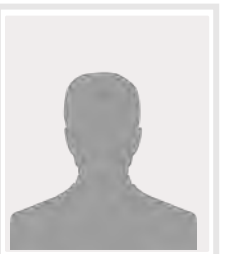
Dr Jonas Liechti is a Big Data specialist and a scientific project manager (joined in August 2022)

Dr Etienne Voutaz is a data scientist and a scientific project manager

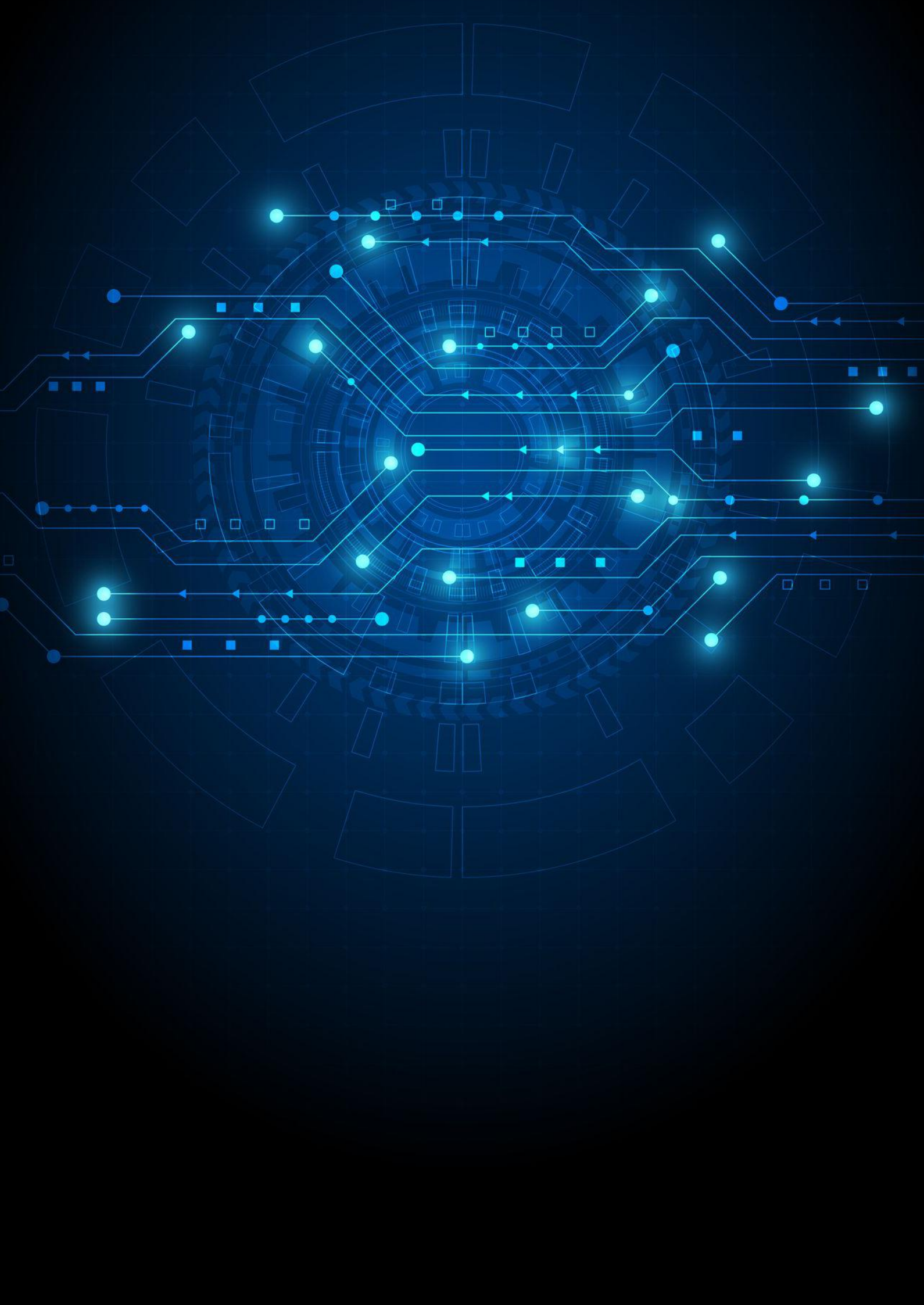
Dr Albert Blarer is a data scientist and a scientific project manager



Dr Raphael Meier is an expert in Image Processing and Machine Learning and a scientific project manager



Dr Hông-Ân Sandlin is an expert in Data Analysis and Machine Learning and a scientific project manager



Support

Monia Khelifi

Head of Administration and Event Management

Amina Bouslami

CYD Campus Lausanne Administrator (from June 2022)

Sarah Frei

Communication and Administrator CYD Campus Zurich (from April 2022)

University Interns

In order to increase students' cyber expertise and strengthen Switzerland's long-term resilience to cyber threats, the Cyber-Defence Campus offers university internships at all three locations in Thun, Lausanne and Zurich. In 2022, 27 students were able to complete an internship with the Cyber-Defence Campus. The interns come from different universities.

Perceval Faramaz, November 22 – October 23, International Affairs, Lausanne

Francesco Intoci, October 22 – March 23, Cyber Security, Lausanne

Louis Leclair, October 22 – March 23, Cyber Security, Lausanne

Alessandro Tavazzi, September 22 – February 23, Technology Monitoring, Lausanne

Eric Jedermann, September 22 – February 23, Cyber Security, Thun

Lucas Crijns, September 22 – February 23, Cyber Security, Lausanne

Etienne Salimbeni, September 22 – February 23, Data Science, Lausanne

Marc Egli, September 22 – February 23, Cyber Security, Lausanne

Nicholas Sperry Grandhomme, August 22 – Januar 23, Data Science, Lausanne

Léo Meynent, August 22 – January 23, Data Science, Lausanne

Michiel Lüchinger, August 22 – July 23, Communication and International Affairs, Thun

Valentin Mulder, May 22 – April 2023, Technology Monitoring, Lausanne

Sarah Ismail, May 22 – April 2023, Technology Monitoring, Lausanne

Johannes Willbold, March 22 – August 22, Cyber Security, Thun

Beatrice Dall'Omo, March 22 – August 22, Cyber Security, Thun

Guillaume Follonier, March 22 – August 22, Data Science, Lausanne

François Burguet, March 22 – August 22, Technology Monitoring, Lausanne

Jacques Roitel, February 22 – July 22, Technology Monitoring, Lausanne

Cyrill Vallez, February 22 – Juli 22, Data Science, Lausanne

Alexander Glavackij, February 22 – December 22, Technology Monitoring, Lausanne

Eloi Garandel, September 21 – February 22, Data Science, Lausanne

Benjamin Killian, September 21 – February 22, Cyber Security, Lausanne

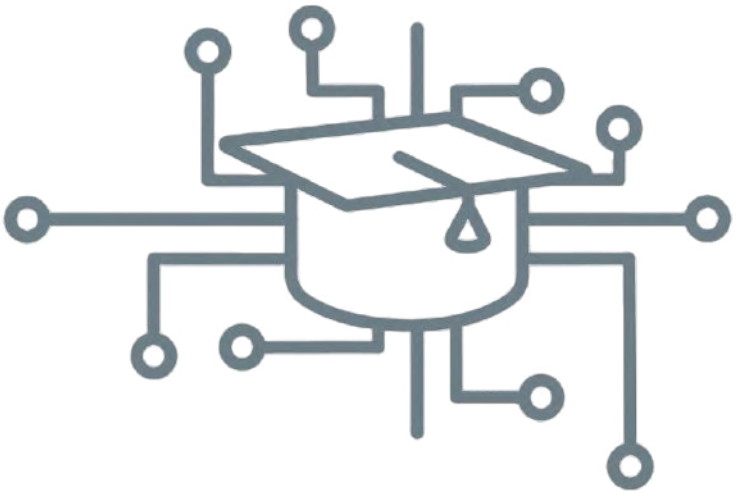
Samad Emrys Durussel, September 21 – February 22, Data Science, Lausanne

Huzar Marin, September 21 – February 22, Cyber Security, Lausanne

Marie Reignier Tayar, August 21 – January 22, Data Science, Lausanne

Michael Tsesmelis, June 21 – May 22, Technology Monitoring, Lausanne

Sarah Frei, April 21 - March 22, Communication, Thun



CYD Fellows

In 2020, the CYD Campus launched a Cyber Defence (CYD) Fellowship Programme together with the EPFL to give students the opportunity to deepen their knowledge in cyber defence topics and to strengthen Switzerland's competences in this field. This enables students to make a research contribution to Switzerland's cyber defence while they are still studying. The CYD Fellowship is a competitive talent programme that provides students with a CYD expert to supervise their research work. CYD Fellows are enrolled at a Swiss university and conduct their research on the premises of the CYD Campus at the EPFL Innovation Park in Lausanne, at Zollstrasse in Zurich or at the headquarters in Thun. CYD Fellowships are awarded several times a year to master's students, doctoral students and postdocs and provide a living allowance. In 2022, 13 fellows were active:

Jodok Vieli, Master Thesis Fellow, ETHZ, October 22 – March 23, Project title: *Systemization of DNS DoS: Attack Characterization, Mitigation, and Measurement*, CYD Mentor: Dr Bernhard Tellenbach

Dr **Lucianna Kiffer**, Postdoc Fellow, Northeastern University, September 22 – August 24, Project title: *Security and Usability of Blockchain Networks*, CYD Mentor: Dr Bernhard Tellenbach

Louis-Henri Merino, Doctoral Fellow, EPFL, June 2022 – May 24, Project title: *Coercion-Resistant Remote E-Voting Systems with Everlasting Privacy*, CYD Mentor: Dr Bernhard Tellenbach

Alessandro Stolfo, Doctoral Fellow, ETHZ, January 22 – December 25, Project title: *Privacy-Preserving Learning of Neural Language Models*, CYD Mentor: Dr Ljiljana Dolamic

Ian Boschung, CYD Master Thesis Fellow, ETHZ, January 22 – November 22, Project title: *Analysing new security guarantees made possible by the ARMv9 Confidential Compute Architecture*, CYD Mentor: Dr Bernhard Tellenbach

Adalsteinn Jonsson, Master Thesis Fellow, ETHZ, December 21 – June 22, Project title: *Binary Similarity Techniques for Malware Detection*, CYD Mentor: Dr Martin Strohmeier

Lina Gehri, Master Thesis Fellow, ETHZ, November 21 - April 22, Project title: *Analyzing and Comparing Defense Strategies in a Cyber Defense Exercise*, CYD Mentor: Dr Vincent Lenders

Jan Urech, Master Thesis Fellow, ETHZ, October 21 - April 22, Project title: *Developing an Automated Defender for Cyber Security Exercises*, CYD Mentor: Daniel Hulliger

Simran Tinani, PhD Fellow, UZH, September 21 - August 23, Project title: *Nonabelian Groups in Cryptography*, CYD Mentor: Dr Carlo Matteotti

Ksandros Apostoli, Master Thesis Fellow, EPFL, September 21 - February 22, Project title: *Privacy-Preserving Proof-of-Personhood Token*, CYD Mentor: Dr Daniel Moser

Dr **Andrei Kucharavy**, Postdoc Fellow, EPFL, December 20 - November 22, Project title: *Evolutionary dynamics for improved GAN detection*, CYD Mentorin: Dr Ljiljana Dolamic

Dina Mahmoud, PhD Fellow, EPFL, September 20 - August 24, Project title:: *ADHeS: Attacks and Defenses on FPGA-CPU Heterogeneous systems*, CYD Mentor: Dr Vincent Lenders

Dr **Dimitri Percia David**, Postdoc Fellow, UNIGE, August 20 - July 22, Project title: *Technology Forecasting and Market Monitoring for Cyber-Defence*, CYD Mentor: Dr Alain Mermoud

Students

CYD Campus employees define and supervise student projects at Bachelor, Master and PhD level. The students conduct their projects on the premises of the CYD Campus at EPFL, ETHZ and at the headquaters in Thun. During 2022, work from twelve students was supervised by the CYD Campus.

Lukas Baege, ETHZ, October 22 – April 23, Supervisor: Dr Martin Strohmeier

Pascal Schärli, ETHZ, October 22 – March 23, Supervisor: Dr Bernhard Tellenbach

Silvan Niederer, ETHZ, September 22 – January 23, Supervisor: Llorenç Roma

Pedro Miguel Sanchez Sanchez, Universidad de Murcia, September 22 – December 22, Supervisor: Dr Gérôme Bovet

Enrique Tomas Martinez Beltran, Universidad de Murcia, September 22 – December 22, Supervisor: Dr Gérôme Bovet

Yago Lizarribar, IMDEA Networks Institute, June 22 – September 22, Supervisor: Dr Gérôme Bovet

Mathis Lindner, ETHZ, February 22 – August 22, Supervisor: Dr Martin Strohmeier

Sébastien Gillard, Université de Fribourg, 21 – 23, Supervisor: Dr Alain Mermoud

Dominique Portenier, ETHZ, September 21 – February 22, Supervisor: Dr Daniel Moser

Silvio Geel, ETHZ, September 21 – February 22, Supervisor: Dr Daniel Moser

Marco di Nardo, ETHZ, September 21 – February 22, Supervisor: Dr Daniel Moser

Florian Lerch, ETHZ, September 21 – January 22, Supervisor: Dr Martin Strohmeier

Members of the Armed Forces

Constable Michael Bosshard (name changed), August 22 - October 22, Data Science, Thun

Other members of the armed forces doing their army service at Lab 42, an innovation unit of Cyber Batallion 42, used the premises of the CYD Campus in 2022.

2 Highlights

Brokenwire

CYD Campus associate Martin Strohmeier, together with research partners from Oxford University, has discovered a vulnerability called Brokenwire in the combined charging system (CCS) of electric vehicles. CCS is one of the most widely used Direct Current (DC) rapid charging technologies for electric vehicles. The attack interrupts necessary control communication between the vehicle and charger, so that the charging processes are interrupted. The attack can be conducted wirelessly from a distance using electromagnetic interference, allowing individual vehicles or entire fleets to be disrupted simultaneously. In addition, the attack can be mounted with off-the-shelf radio hardware and minimal technical knowledge.

Demonstration of Brokenwire.

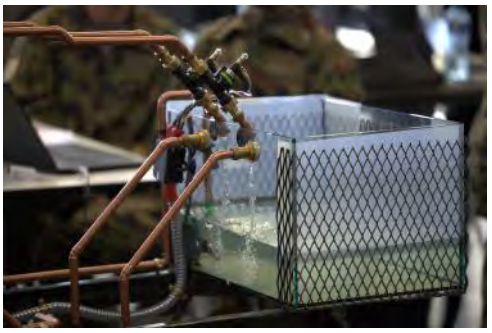
The researchers demonstrated the attack in a controlled laboratory and then against seven vehicles from different manufacturers and 18 DC high-power chargers. They also conducted a disclosure to industry and proposed various countermeasures that could be used to limit the impact. Brokenwire has immediate implications for many of the estimated 12 million battery powered electric vehicles on the road worldwide as well as profound implications for the new wave of electrification of vehicle fleets, both for private companies and key public services. In addition, Brokenwire affects electric ships, aircraft and heavy goods vehicles.

For more information: Brokenwire website & publication

ICS Hackathon in Thun

From 19 to 23 September, the CYD Campus and the Cyber Battalion 42 organised a hackathon on industrial control systems (ICS) and operational technologies (OT).

Among the more than 30 participants were researchers from the CYD Campus and the Swiss Armed Forces, employees of the NCSC and Swissgrid, soldiers from Cyber Battalion 42, students from the Lucerne University of Applied Sciences and Arts, ETH Zurich and Ruhr University Bochum, as well as experts from the private sector, such as ALSEC Cyber Security Consulting and Nozomi Networks. The participants were divided into cross-functional teams with different areas of focus in the field of industrial control systems. This allowed the groups to conduct targeted vulnerability analysis, examine different attack vectors and develop appropriate countermeasures. Additionally, this facilitated collaborative and intensive work in smaller groups.



Model of a pumped storage power plant: CYD Campus ICS laboratory in Thun.

Vulnerability tests for ICS systems are difficult to implement compared to information systems, as severe damage can be caused. However, in order to be able to carry them out and simulate attacks, as well as for educational and training purposes, appropriate laboratories are particularly suitable. Therefore, the CYD Campus provided two labs for the infrastructure of the hackathon, each simulating a different industrial control system. One is the representation of a pumped storage power plant. The second is a reconstruction of a Swiss energy substation for the development of attack and defence strategies, the so-called Krinflab. With the hackathon, the CYD Campus pursued three goals: to expand the knowledge available in the DDPS within this relevant field, to network experts from industry, universities and the public administration, and to support young talents who want to deepen their expertise in the area.

Krinflab: Reconstruction of a Swiss energy substation for the development of attack and defence strategies.

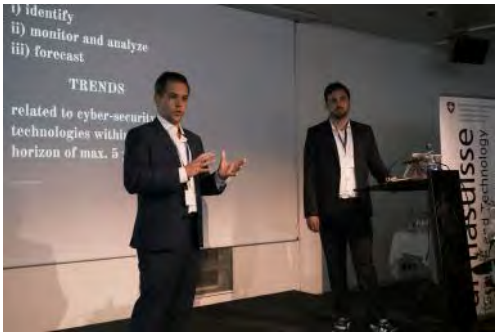
For more information: CYD Campus Hackathon News

Trends in Data Protection and Encryption Technologies 2025

Militaries and governments have long used encryption technologies to facilitate secret communications. Today, encryption technologies are equally crucial in protecting our economy and civil society. They are key enablers for the ongoing transformation of the digital economy and online society. The study launched in Switzerland by the Cyber-Defence Campus at the beginning of 2022 provides an overview of the changing landscape of encryption and data protection technologies and their global usage trends. The Swiss government mandated the CYD Campus to identify the 38 most crucial encryption and data protection technologies, intending to analyse their anticipated developments until 2025 and derive the implications for the military, civil society, and business sectors. Around fifty experts from academia, the Swiss government, and industry contributed to the study. They included numerous researchers, interns and CYD Fellows from the CYD campus. This study is a reference for organisations and individuals who have to develop coherent and efficient data protection and encryption strategies in the coming years. The technologies are divided into five categories:

1. Encryption foundations technologies are used to create other encryption applications;
2. Low-level applications: Focus on basic functionalities;
3. High-level applications: Focus on more complex functionalities;
4. Data protection technologies: Data protection without encryption;
5. Use cases: Concrete ways how technologies can be used together to create a solution that works.

The study was presented at the CYD Campus Conference 2022 and will be published in book form in summer 2023.



Alain Mermoud and Valentin Mulder present the study at the CYD Campus Conference.

Inauguration of New CYD Campus Premises in Zurich

Another highlight of the CYD Campus in 2022 was the inauguration of the new premises at Zollstrasse 62 in Zurich. The official reopening of the CYD Campus Zurich on 24 November also celebrated the launch of SCION. SCION is a novel Internet architecture developed at ETH Zurich ten years ago and made marketable in the last five years by ETH spin-off Anapaya Systems. The technology replaces the insecure internet routing protocol with a more secure and efficient protocol.

The DDPS is interested in using this technology for Swiss cyber defence and is testing this technology at the CYD Campus together with Swiss industrial partners. For this purpose, the three CYD Campus locations in Thun, Lausanne and Zurich were equipped with SCION network connections from the companies Swisscom, Sunrise and SWITCH and made available for three years as a national test infrastructure for the armed forces and security authorities.

Inauguration of new CYD Campus premises in Zurich.

Cyber-Defence Campus Conference

A central task of the CYD Campus is the networking of academia, industry and state actors in the field of cyber defence. For this purpose, the CYD Campus regularly organises events on defence and security-related cyber topics. An important annual event is the CYD Campus Conference, which attracts more than 300 participants.
The CYD Campus Conference 2022 took place on 26 October in the Kursaal in Bern. During the event, experts from public administration, academia and industry spoke on key topics in the area of securing future digital infrastructures. In addition to presentations on developments in the area of communication networks (5G+), the global financial system, the dissemination of (dis)information and cryptography, the series of talks was rounded off with an insight into the conception and implementation of realistic cyber defence training such as "Locked Shields".

Panel discussion Study Data Protection and Encryption Technologies 2025.

Cyber Startup Challenge 2022

The Cyber Startup Challenge was launched in June 2022 for the third year in a row. Within this challenge, 36 startups from various countries presented their innovative technologies in the field of network detection and security of IoT devices. After evaluation by cyber experts from the Federal Department of Defence, Civil Protection and Sport (DDPS), the three finalists ONEKEY, Narrowin and Sepio were eventually invited to the CYD Campus Conference. Each of the finalists was allowed to give a pitch at the Conference, where the startup ONEKEY was ultimately able to convince the DDPS jury.
ONEKEY has developed a technology that automatically identifies security vulnerabilities. Using the "Software Bill of Materials (SBOM)" and automatically generated "Digital Twins", ONEKEY checks operational software for critical security vulnerabilities and compliance infringements. On the one hand, the SBOM provides a detailed overview of all components of a software package. On the other hand, a "Digital Twin" is a virtual image of a system and allows its examination in the lab without the source code, the network or physical access to the devices.

For more Information: Finalists 2022 & Press Release Cyber Startup Challenge

Colin Barschel, Head of Innovation CYD Campus and Florian Lukavsky, Co-Founder and CTO of ONEKEY.

Representation of Switzerland at the NATO CCDCOE

CYD Campus associate William Blonay took up his position as Switzerland's representative at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, in February 2022 and will serve for three years. The CCDCOE is a NATO accredited cyber centre of excellence that aims to strengthen research and training cooperation in the field of cyber defence internationally. The centre achieves this by organising joint exercises and conducting research projects, technical training and conferences.

The flagships of the CCDCOE include the annual international conference on cyber conflicts (CyCon), the Tallinn Manual and «Locked Shields», one of the world's largest cyber defence exercises (more information in the next highlight), in which William Blonay also participated in the Red and Green Team in 2022.
Since joining as a «Contributing Nation» in 2019, Switzerland has benefited from the exchange of information and knowledge as well as from the various joint research and training activities of the CCDCOE. This cooperation also contributes to the implementation of the National Strategy for the Protection of Switzerland against Cyber Risks (NCS) and the Cyber DDPS Strategy 2021–2024. Against the backdrop of the changed global political situation, Switzerland is particularly keen to consolidate international cooperation, particularly in the area of defence.

Each CCDCOE member state sends one or two experts as representatives to Tallinn. These experts are active in various areas of competence such as technology, strategy, operations, support, education and training, and law. Switzerland is currently represented at the CCDCOE by two delegates: In addition to William Blonay, who belongs to the technology competence area, Lisa Schauss, a member of the Armed Forces Command Support Organisation (FUB) and part of the education and training competence area, represents Switzerland at the CCDCOE.

To learn more about William's experience at the CCDCOE, read the interview in the December 2022 issue of armafolio.

Cyber Defence Exercise «Locked Shields»

The CCDCOE organised the Locked Shields Cyber Defence exercise in April 2022, which has been held annually since 2010. One of the ways in which the CYD Campus directly participates in the organisation of the exercise is by sending experts to the Green and Red Teams. These two teams are responsible for the organisation and implementation of the exercise and are composed of experts from all participating states. The Swiss Armed Forces regularly participate with their own Blue Team or together with other countries to train their experts in cyber defence.

During the exercise, the Red Teams operate as attackers against the Blue Teams, which perform as cyber rapid reaction teams defending the national IT systems and critical infrastructures of the fictitious island state of Berylia against large-scale cyber attacks. In total, more than 2000 participants from 32 nations took part in the event. In addition to protecting numerous complex cyber-physical systems, the teams formed from member states and partners are required to make strategic and tactical decisions, report incidents and deal with challenges in the areas of forensics, law, media relations and information warfare. The aim of the exercise was to improve participants' skills and knowledge in the field of cyber defence and to promote cooperation between the different nations and organisations.

Due to the numerous attacks and the complexity of the exercise, Locked Shields is also an ideal environment to test cyber defence products. Chapter 6.1 "Innovation project results" elaborates on the cooperation between the Cyber-Defence Campus and industry in this context.

William Blonay on his first day representing Switzerland at the CCDCOE.

Part of the exercise «Locked Shields» im April 2022.

3 CYD Talent Development

Specialists in cyber security and data science are scarce in Switzerland as well as in many other countries. The promotion and training of new cyber talents is therefore a major challenge and one of the three key tasks of the CYD Campus. The CYD Campus pursues different approaches in order to enhance students' cyber expertise.

On the one hand, the CYD Campus offers university internships at all three locations in Thun, Lausanne and Zürich. In addition, student projects at Bachelor, Master and PhD level are defined and supervised by CYD Campus researchers. These students are enrolled at a university and are supervised by a CYD Campus Mentor. In addition, the CYD Campus, together with EPFL, launched the CYD Fellowship programme in 2020 to motivate students and provide them with the opportunity to strengthen their skills in the field of cyber defence.

In 2022, 27 university interns were employed and twelve student projects were supervised by CYD Campus researchers. Furthermore, 13 CYD Fellows were active. The aim is to promote a new generation of cyber-talents in this way. Thus, the CYD Campus makes a substantial contribution to combating the shortage of skilled workers in the highly specialised cyber field with the long-term goal of ensuring the necessary cyber skills for government, academia and business in Switzerland.

Since 2022, participants in the Cyber Training Course also have the opportunity to complete their internship at the Cyber-Defence Campus. The Cyber Training Course was first launched as a pilot project during the 2018 recruit school (RS) and aims to strengthen the cyber defence skills of the Swiss Armed Forces militia. The course is aimed at EFZ IT specialists, school-leavers and university students. In 2022, the first recruit of the Cyber Training Course had the opportunity to complete an internship at the CYD Campus.

To gain more insight into the activities of the CYD Fellows, the university interns and the members of the armed forces (AdA), interviews were conducted for this annual report.

Interview with Sarah Ismail, University intern in Lausanne in the field of Technology Monitoring

What is the research topic you have been working on during your time at CYD Campus?

My research focuses on data protection and encryption technologies. The goal is to predict current trends in these technologies based on public attention via Wikipedia page views. Using data from other sources such as arXiv, Google Trends and OpenAlex, this study determines, measures and analyses the time-varying public attention given to each technology.

How have the CYD Campus's knowledge and resources helped you in your research?

On the one hand, I learned new technical skills, such as programming in a programming language I had not previously mastered. On the other hand, I was able to work with highly specialised and competent people in their field. This made it easier to learn and share knowledge. Finally, the CYD Campus provides many tools to help you conduct your research in a pleasant and suitable environment.

If you could give one piece of general advice to future interns for their time at the CYD Campus, what would it be?

I would say that you should not hesitate to communicate with your colleagues and ask them questions, it reinforces collaboration, the exchange of ideas and above all it promotes creativity.

What was your motivation for doing an internship at the Cyber-Defence Campus?

Cyber security is a hot topic. As we have seen on the news, multiple data breaches have occurred in recent years. This triggered my curiosity and ignited the desire to learn more about the field of cyber security. I am also fascinated by the world of research and would like to develop my skills in this field.

Where do you see yourself in 10 years?

Ideally, in ten years' time, I would have gained solid professional experience as a business analyst, possibly in the field of cyber security, and I would also like a position with responsibility where I can work on a variety of projects.

Interview with Luca Crijns, University intern in Lausanne in the field of Cyber Security

What is the research topic you have been working on during your time at CYD Campus?

I am working on a network filter that is able to extract flows from network traffic with speeds of 100 Gbps based on configurable rules. Filtering by IP addresses and ports is very common and can be done by many hardware solutions. However, deep packet inspection and filtering based on packet payload are mostly done using software. I tested several hardware solutions combined with appropriate software to do exactly that.

How have the CYD Campus's knowledge and resources helped you in your research?

In addition to my supervisor, I have a technical supervisor who is able to help me when I have technical issues with the hardware and software. He has proven invaluable when I have issues or want to talk something through.

If you could give one piece of general advice to future interns for their time at the CYD Campus, what would it be?

For me it proved useful to send out a weekly update on the project at the end of the week. By doing this, you automatically ensure that you have made progress at the end of every week. In addition to that, remember that your supervisor is there to help and you can usually drop in for a chat if you are stuck. There's no point staring at the screen for long periods of time wondering what to do.

What was your motivation for doing an internship at the Cyber-Defence Campus?

My motivation was to learn something new. I come from a mathematics background and I previously had no experience with networking whatsoever. That's why I chose this internship to expand my knowledge and horizons. I wasn't sure if I could see myself working in a field that is closely related to mathematics.

Where do you see yourself in 10 years?

Honestly, I haven't a clue. As I like the work I do at the CYD Campus, I probably want to do something similar. It's a bit of a simple answer, but at this point I can't provide any more details.

Interview with Sergeant Michael Bosshard (Cyber Training Course, name changed)

What was the research topic you worked on during your time at CYD Campus?

During my time at CYD Campus I worked mostly on Deep Learning Methods on Graphs. Deep Learning Methods on Graphs is a relatively young field of research which is growing fast. In particular, I studied classification tasks using conventional convolutions as well as more modern methods such as EdgePooling and Variational Graph Autoencoders. The end goal was to streamline graph-level tasks that would take much more time using static methods.

How did the CYD Campus's knowledge and resources help you in your research?

The CYD Campus was able to provide me with a solid environment where on the one hand I was given enough support to pursue my research goals, and on the other hand also offered scientific challenges.

If you could give one piece of general advice to future interns for their time at the CYD Campus, what would it be?

The main piece of advice I would give is that it's worth getting to know the environment and the surroundings of the CYD Campus as there are many facilities and structures to support you during your research.

What was your motivation for doing an internship at the Cyber-Defence Campus?

My main motivation for my internship was to use my data science skills in order to make an impact in the world of cyber security and asset protection. Coming from a purely scientific background (mathematics), I found it very interesting to apply and develop my knowledge through on use cases.

Where do you see yourself in 10 years?

In 10 years' time, I hope to have developed into a more experienced data scientist and be able to draw on to a wide variety of different methods and approaches. I cannot tell if I will be working in the public or the private sector, but I am confident that the tasks I will take on will still be challenging and motivating.

Interview with Lina Gehri, Master Thesis CYD Fellow in Zurich

What was the research topic you worked on during your time at CYD Campus?

I created machine-learning models to detect Command and Control attacks. My goal was to generalise the models in such a way that they are able to detect Command and Control traffic in various and unfamiliar network environments. To train and test them, I used network traffic that was captured during the extensive cyber defence exercise Locked Shields.

How did the CYD Campus's knowledge and resources help you in your research?

The biggest advantage was that I received a lot of support from different people at the CYD Campus. If I had a question or needed some assistance, their combined experience and knowledge helped me a lot and many new ideas came up during discussions about my thesis.

If you could give one piece of general advice to future CYD fellows for their time at the CYD Campus, what would it be?

Make use of the opportunity, go to the office to talk to the people there about what you are doing, whether it's about your thesis or your latest interests.

What was your motivation for doing a fellowship at the Cyber-Defence Campus?

I had already decided to do my master thesis in collaboration with the CYD when my supervisor told me about the fellowships and encouraged me to apply. It seemed like a great opportunity to get to know and work with like-minded people, so I decided to give it a shot

Where do you see yourself in 10 years

Hopefully still learning new things and still excited about the work I do. If you want specifics, ask me again in 9 and a half years.

4 Research

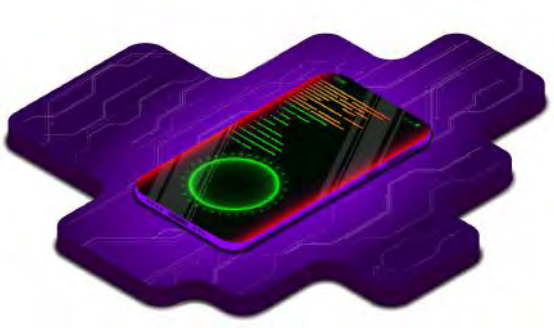
Research at the CYD Campus is a long-term investment in securing the required expert knowledge and scientific-technical skills for the tasks and activities of the Confederation in the field of cyber defence. As an integral part of technology management, it also forms the basis for a solid roadmapping of future technologies and for innovation projects of the DDPS. It therefore contributes both to the development of operational cyber defence capabilities that will be required in the future, as well as to the scientific-technical support of planning and procurement in the DDPS.

Research projects are implemented in collaboration with universities and industrial partners.

4.1 Cyber Security Projects

Secure Mobile Operating Systems

Mobile devices (smartphones) are essential for efficient work, yet their mobility and connectivity offer many opportunities for attack. The protection of confidential and classified information is therefore particularly difficult. The aim is to use a commercially available mobile device to share sensitive information and applications. This device allows information to be exchanged, whether in a call, a message or via an app, up to the level of "confidential". The main challenge is to find the best architecture for a secure mobile operating system that balances security, feasibility and user friendliness.



Two approaches are pursued to protect sensitive data: The first approach involves compartmentalisation of risks. This means that the area of attack on the system is nested to minimise the impact of an attack. To achieve this, two architectures for a secure mobile operating system were developed, along with a risk analysis. The cyber security not only includes the mobile operating system, but also the hardware, cryptographic components, and boot chain hardening (signatures). The second approach seeks to separate the execution of an application from the operating system and the manufacturer to ensure sovereignty over the application and to increase security.

Sovereign Smartphone Architecture

Smartphones are at the heart of many people's digital lives. However, they do not offer the same flexibility as PCs, on which users can install and run any software they like. The vendors of the major operating systems such as iOS and Android can dictate which apps can run, how they run and which phone resources they can access. This is not desirable, as users have to entrust their security and privacy to OS vendors and accept the functionality restrictions they impose. Given the widespread use of Android and iOS, immediately leaving these ecosystems is not a practical solution. As an alternative, the development of a new smartphone architecture is proposed that gives control back to the users while ensuring compatibility with current smartphone ecosystems. Such a design is proposed and analysed on the basis of advances in trusted execution environments for ARM and RISC-V.

Detection of Software and Device Vulnerabilities: Microsoft Windows Applications

Vulnerability research in the area of Windows-based systems and applications aims to uncover any unknown security gaps. By focusing on software that is used by stakeholders (organisations within the DDPS, but also the rest of the Federal Administration), a directly measurable benefit for the IT security of the Federal Administration is created in addition to the research activity.

Besides the development of competencies for detecting and exploiting vulnerabilities, several security gaps, some of which were critical, have been discovered in the past year and communicated to the stakeholders in the form of advisories. Affected vendors were informed about the vulnerabilities in detail and encouraged to fix them as quickly as possible by providing fully functional proof-of-concept exploits.

Detection of Software and Device Vulnerabilities: IoT Devices

Nowadays, connected devices, often referred to as the Internet of Things (IoT), are omnipresent, yet their applications are often critical with respect to security. Therefore, detecting potential vulnerabilities in such devices is crucial, but often challenging. One particular issue is that an analyst typically does not have access to the source code of the programs running on the device, which consequently exist only as machine-executable binary code. In contrast to the source code, which is easier for humans to understand, many abstractions (e.g. function names) are no longer present in binary code, thus making analysis much more difficult. Moreover, the binary code depends on the processor architecture used, which often differs more for IoT devices (e.g. ARM, MIPS) than for conventional computers (often x86). In this research project, techniques for the (semi-)automated analysis of IoT binaries are tested and their feasibility is demonstrated with corresponding proof-of-concept tools.

Detection of Software and Device Vulnerabilities: Linux Kernel

Nowadays, the Linux kernel is the basis for various operating systems, which in turn are used on a variety of devices (desktop PCs, server systems, mobile or small electronic devices, etc.). A viable approach to identifying potential security problems in the Linux kernel is to use a so-called kernel fuzzer, which is designed to detect possible abnormal behaviour in the kernel based on unanticipated input. Probably the best known of these fuzzers for the Linux kernel is syzkaller. For the current kernel version, a public instance of syzkaller lists more than 1000 such types of abnormal behaviour, but it is unclear whether they are actually exploitable, i.e. whether they are genuine vulnerabilities. This research project is working on an automated procedure to assess this exploitability. This is essential in order to be able to classify the criticality of identified instances of abnormal behaviour and to be able to address them in a prioritised manner.

Controllable Routing on the Internet

Traditional Internet technologies do not provide end-users with transparency or control over the path of data traffic to its destination. In particular, the lack of information about network devices reduces the trustworthiness of the forwarding path and prevents end-user applications that require certain router functions from reaching their full potential. Furthermore, the loss of control results in applications communicating via undesirable routes, while alternative paths with more desirable properties remain unusable. Within this project, CYD Campus researchers developed a system that allows applications to flexibly forward traffic, potentially over multiple paths, according to user-defined preference policies, with information about routers exposed and transparently attested by autonomous systems. The granularity of this information is selected individually by each autonomous system and protects against the disclosure of sensitive network details to attackers. The researchers demonstrated the feasibility of their system by deploying it on a SCION test network, demon-strating a high throughput on commercial hardware.

Secure Wide Area Networking

With the growing need for secured connections between offices, partners and cloud-based applications, private networks based on MPLS (Multiprotocol Label Switching), VPN (Virtual Private Network) or similar technologies are no longer a viable option for building secure WANs (Wide Area Networks). In this project, alternative technologies such as Anapaya/ETHZ's SCION and programmable routers are being investigated to enable secure communication and transfer information between company sites, trusted partners, and cloud providers. The aim is to develop and evaluate secure routing techniques, including explicit path routing, secure route attestation, defence against distributed denial of service (DDoS) attacks, and traffic obfuscation. These techniques will be demonstrated in a testbed developed in 2022 that connects the CYD Campus sites in Thun, Lausanne and Zurich.

Network Programmability

Recent advances in programmable network devices make it possible to run custom programs both on the control and data level. In this project, we explore how these new possibilities can improve network security. In particular, we focus on network obfuscation, a technique to hide sensitive information that is not protected by traditional security measures such as encryption.

In 2022, we focused on so-called traffic-analysis attacks. These attacks take advantage of the fact that even with encrypted traffic, information about the size and timing of packets is leaked. Published attacks show that this information is sufficient to determine details about ongoing communication. Unfortunately, existing defences are limited in terms of security and/or performance. In collaboration with researchers from ETH Zürich, we developed a system that obfuscates network traffic such that traffic-analysis attacks are no longer possible. The system runs on programmable network devices with high transmission speeds, which makes it particularly suitable for protecting wide-area networks.

Cyber Threat Intelligence Platforms

Cyber security information is typically highly sensitive and confidential, making organisations reluctant to share this data with third parties, even if aggregated analysis of common threats would offer significant benefits in terms of responsiveness and security. To address this trade-off, CYD Campus researchers are developing a platform that provides guarantees that users can only access the global insights (cyber threat models). Each institution retains full control over its datasets. On the one hand, this is made possible by the development of a distributed architecture without a centralised database and, on the other hand, by the integration of advanced cryptographic techniques based on the model of homomorphic multi-party encryption. This allows institutions to securely collaborate with critical sensitive data that is not usually shared, leading to new and improved threat posture. In 2022, two prototypes were developed and evaluated for the exchange of data from MISP (Malware Information Sharing Platform) databases and from Network Intrusion Detection Systems (NIDS) such as Suricata.

Quantum Safe Cryptography

Advancing research in the field of quantum computers poses cryptological risks. Previously used digital signature schemes and asymmetric cryptosystems (public key encryption), which are secure for conventional computers, can be broken with quantum computers. For this reason, the National Institute of Standards and Technology (NIST) has promoted the standardisation of quantum-safe public key procedures in recent years. In July 2022, the first four quantum-safe crypto algorithms were determined by NIST. These include one algorithm for encryption (CRYSTALS-Kyber) and three algorithms for digital signatures (CRYSTALS-Dilithium, FALCON and SPHINCS). At the CYD Campus, the candidates of the last evaluation round were examined, which are code-based (finalist "Classic McEliece", "BIKE" and "HQC") or based on multivariate polynomials (finalist "Rainbow" and "GemSS"). Due to the fact that it is generally recommended to combine classic algorithms with quantum-safe methods in the future, CYD Campus researchers are currently investigating how a secure multiple key exchange can be implemented when the algorithms are used in hybrid form.

Protecting against Pulse Wave Distributed Denial of Service (DDoS) Attacks

Pulse wave Distributed Denial of Service (DDoS) attacks are a new type of network attack consisting of short, high-frequency traffic pulses. Such attacks target the Achilles heel of modern DDoS defence systems: their response time. By continuously adjusting their attack vectors, pulse wave attacks succeed in rendering existing defences ineffective. In this project, CYD Campus researchers use programmable switches to develop an in-network DDoS defence that is effective against pulse wave attacks. To do this, they use Aggregate-based Congestion Control (ACC), a mechanism that has existed for two decades to handle high-bandwidth congestion events. The researchers propose ACC-Turbo, a revised version of ACC that mitigates patterns of attack by applying online clustering techniques to the network. In this way, ACC-Turbo identifies attacks in real time and limits attack traffic efficiently. The CYD Campus has fully implemented ACC-Turbo on P4 switches and is currently evaluating it for a variety of attack scenarios.

Hacking Micro Drones

Unmanned Aerial Vehicles (UAVs), also known as drones, represent a revolution in security and military applications. Due to recent advances in miniaturisation and decreasing costs, mini UAVs have also become very popular in the civilian sector. These drones are generally too small and too weak to be equipped with lethal weapons. Nevertheless, they pose a threat to the military and security agencies because they are equipped with powerful sensors and can be used for infiltration or data collection over restricted areas. The military and security agencies are therefore seeking to develop capabilities to counter the threat posed by mini UAVs. The aim of this project is to explore various techniques for jamming and taking over mini-drones in order to neutralise the threat they pose. In particular, it investigates whether it is possible to exploit the wireless control and navigation channels through advanced signal jamming, signal spoofing and signal manipulation attacks. This year, the focus has been on complex multi UAV GPS spoofing, which has been successfully demonstrated in the laboratory.

Experimental set-up in the lab in order to take over drones in a controlled environment via GPS spoofing.

Side-channel Attacks and Hardware Backdoors

Every electronic device generates electromagnetic emissions. The electromagnetic signals generated may be related to how the emitting electronic components operate internally. A malicious attacker can intercept the emitted signals and examine them to obtain information about the emitting device. The practice of eavesdropping and protecting against eavesdropping and their investigation is summarised in a framework known as TEMPEST. In the case of video monitors, the emitted signals can be used to reconstruct the content. It has already been shown how an attacker can use the signals from the connection cable between a PC and a video monitor to extract internal information from the monitor.
CYD Campus researchers demonstrated how an attacker can use QR codes to extract internal data by exploiting the signals emitted by the video monitor. They systematically evaluated and tested different attack scenarios. The results show how this attack would allow large amounts of information to be stolen from a target up to 50 metres away, from different rooms and even from different floors. The work resulted in a publication and was presented at a scientific conference, CRITIS 2022 in Munich.

Cloud Environments for Data Processing

CYD Campus researchers evaluated the ARCA Trusted Operating System (OS), the flagship product of Swiss startup CYSEC. Arca Trusted OS is a hardened Linux-based operating system combined with a secure Kubernetes orchestrator to contain intrusion and prevent compromise of data in containers on-premise, in the cloud and on the network edge.
They also assessed the security of the ARCA appliance (i.e. ARCA Trusted OS running on a bare metal server) to understand possible scenarios in the armed forces where this solution could be used. To this end, a better understanding of the solution and its security features was required. In order to achieve this goal, CYD Campus researchers provided a detailed description of the solution, including different modules, components and functions that are part of the ARCA appliance. They also reviewed the key security-related features (i.e. HW/SW components, OS hardening measures, etc.) offered to the applications running on the ARCA appliance, with a focus on whether they provide a higher level of security compared to alternatives and whether they are suitable for integration in the context of the armed forces.

Protection of Non-Secure Avionics Systems

This research project deals with the analysis of vulnerabilities in avionics hardware and the associated wireless protocols. In previous years, CYD Campus researchers analysed attacks on the ADS-B (Automatic Dependent Surveillance–Broadcast), CPDLC (Controller-Pilot Data Link Communications) and FLARM technologies both in theory and in practice with the help of the Avionics Laboratory in Thun. FLARM is a collision warning device used in light aircraft and drones that was developed in Switzerland and has received worldwide attention and dissemination.

In 2022, the researchers dedicated themselves to the practical analysis of the Traffic Collision Avoidance System (TCAS), which is used in larger aircraft. In addition, the impact of radio frequency interference of the Global Positioning System (GPS) in commercial airliners was examined, in particular after the outbreak of the Ukraine war. Both activities will be ongoing in 2023, alongside practical attacks on CPDLC and a security analysis of European U-Space technology candidates.

Cyber in Aerospace

Cyber security in Aerospace has been a key research topic since the inception of the CYD Campus. There are many fundamental commonalities in aerospace, including in the area of cyber security. For example, many legacy technologies are used that have often been in use unchanged for 20 or even 40 years. Particularly in the area of wireless communication technologies, this fact leads to fundamental security problems, as content is neither encrypted nor authenticated. But even where content is encrypted, it is often not done with open, secure standards, but with weak proprietary systems that contradict Kerkhoff's principle about secure cryptosystems. This year, as part of its work on the avionics data link ACARS (Aircraft Communication Addressing and Reporting System), the CYD Campus has identified several such procedures, which can be detected automatically amongst a stream of mixed data (encrypted, unencrypted and weakly encrypted). Further work to decrypt some of the ciphers found is ongoing.

Deep Learning for Security (Steganography)

Criminal eavesdroppers and cutting-edge secure communication systems are locked into an eternal arms race, requiring the continuous further development of existing protocols, as well as novel methodologies and modelling approaches toward analysing cyber threats to real-world side-channel attacks. A particularly important feature of high-utility cryptographic protocols is the ability to conduct cryptography under plausible deniability, as the mere act of encryption is increasingly targeted by oppressive regimes around the world and cryptographic channels, such as those relying on VPNs, are often blocked. In this project, we developed novel demonstrably secure methods for steganographic communication in texts based on research on deep multi-agent reinforcement learning in cooperative games. Further refinements of this method are planned as well as extension to other modes of communication such as audio.

Security of Electric Vehicles and Charging Infrastructures

As part of the DDPS conversion to electric vehicles, the security of the existing charging infrastructures has to be reviewed. Preliminary work has already been carried out which revealed that for certain systems using so-called Power Line Communication (PLC), the data flow can be intercepted from afar by wireless means. This may have various security and privacy implications for cars and infrastructure. During the CYD Campus Car Hackathon in Thun in October 2021, an active attack on a charging system was developed in which an a low-effort, so-called denial-of-service (DoS) attack wirelessly interrupts and terminates the charging process. The attack, dubbed Brokenwire, was reported to the National Center for cyber security and all the researchers involved are in communication with car and charging manufacturers with regards to its mitigation. The analysis of such attacks and possible countermeasures was carried out during 2022.

Examination of security vulnerabilities in electric vehicles and charging infrastructures in Thun.

4.2 Data Science Projects

Distributed IoT Sensors: Hardware and Behavioural Analysis

Internet-of-Things (IoT) devices are now ubiquitous in numerous use cases, including in a military context, making them an attractive target for cyber attacks. Unfortunately, manufacturers do not prioritise security in either hardware or software during the development process. For example, widely used IoT devices do not have a tamper-proof identifier, so they can be easily imitated. By looking at hardware variations, such as clock drift, CYD Campus researchers are training machine learning models to recognise hardware fingerprints that can uniquely identify an IoT device. These fingerprints could be used in the future as additional security in various applications. Similarly, researchers create software fingerprints that model the normal behaviour of an IoT device. The Campus trains machine-learning models to detect if a device is behaving in an unexpected way, which enables the detection of cyber attacks such as botnets or ransomware. Metrics such as process calls and resource allocations from the operating system are used for this purpose.

Distributed IoT Sensors: Modulation Classification and Collaborative IoT

The electromagnetic spectrum is a versatile resource and at the same time crucial for numerous systems, such as telecommunications, radar and positioning. Therefore, it must be protected from cyber attacks that could affect these systems. Automatic algorithms for modulation classification attempt to identify modulations. Some expert systems and approaches based on machine learning provide good results but have problems when dealing with unknown parameters, such as the channel or sampling rate, for which they have not been trained. This project explores transfer-learning methods that enable the use of low-cost Software Defined Radios. With transfer learning, the CYD Campus is able to classify modulations under previously unknown conditions that usually lead to misclassification in traditional approaches.

Artificial Intelligence Working Group with the US

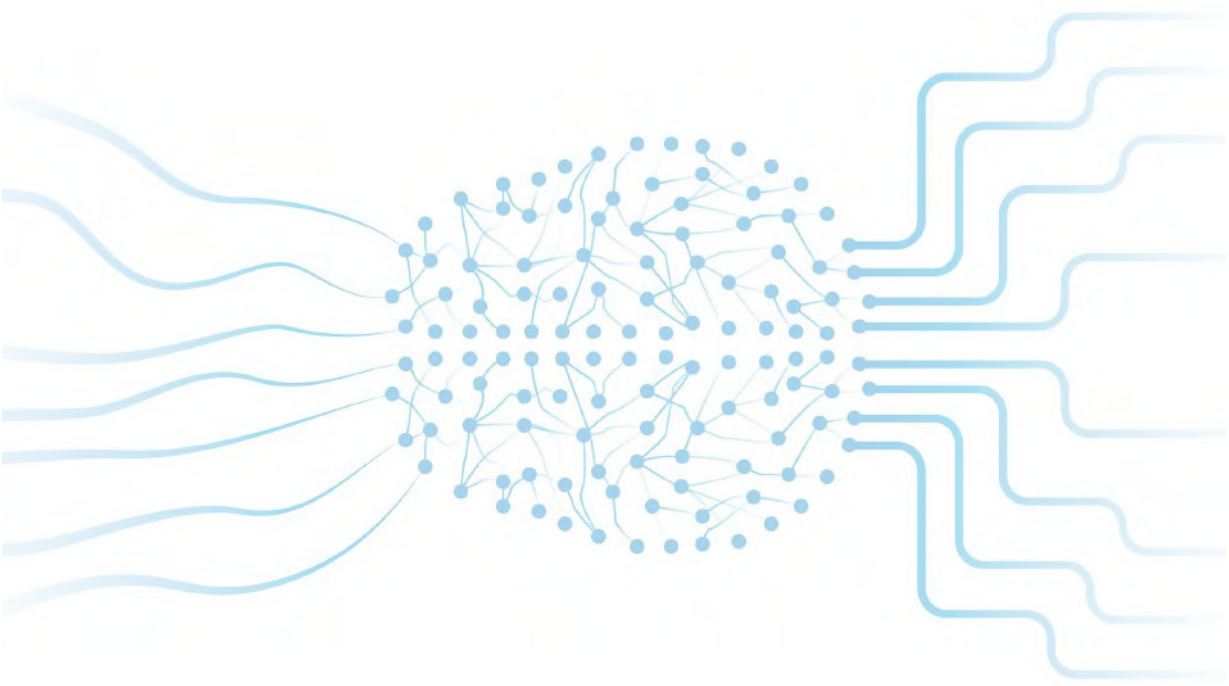
Representatives of the CYD Campus and the US Department of Defense have been regularly exchanging information on the topic of artificial intelligence for several years. In particular, joint basic knowledge in this area has been gained and relevant applications identified. For this purpose, current technical possibilities were examined, potential technology solutions developed and joint activities initiated. Identical areas of interest include the monitoring of new technologies, Internet of Things (IoT) and decentralised machine learning. In 2022, a NATO working group (IST-ET-121) was established and co-chaired with the US Army Research Lab. Within this framework, meetings were held every four weeks, enabling the international participants of the working group (CHE, USA, CAN, SWE, ESP, GER, CCDCOE) to exchange information on the application of machine learning.

Intelligence Gathering Cyberspace: Stratosphere

In order to be able to analyse data, it must first be acquired. While cyberspace is de facto a space of its own, cyber risks today can also affect air and space, such as aircraft and satellites. It is therefore important to consider cyber risks in a multidimensional environment. In this project, the intention is to collect data in a strategic location, namely the stratosphere. This is particularly interesting because it is located between satellites and the Earth. This will allow researchers from the CYD Campus to collect and locate signals. For this purpose, they are developing an elevation platform carried by a weather balloon. The payload will contain a software defined radio that can receive signals and communications and locate transmitters on Earth or in space.

Computer-assisted Data Analytics: Robustness of Deep Learning Models

Machine-learning models have become increasingly important in recent years. They are no longer used solely in specialised applications, but can be found in many applications, including smartphones to detect user activity. A crucial question can be derived from this observation: Are these models robust against attacks? It appears that the vast majority of these models can be easily overcome by an attacker. Since this could have devastating consequences in a military context, the models need be rendered robust against adversarial attacks. In this project, CYD Campus associates are investigating Deep Learning models and exploring methods to increase their robustness. To this end, they have expanded the training set with adversarial samples that could be used by attackers. The results indicate that the robustness of models trained with such adversarial samples improves compared to normal accuracy.



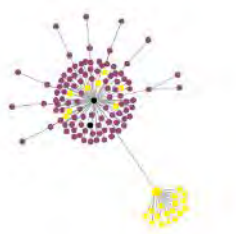
Detecting Fakes in Social Media: Efficient Identification of Misinformation and Disinformation in Social Media

In the event of a rapidly spreading pandemic, it is necessary to quickly obtain relevant information about the disease. Twitter is a popular medium to get real-time information about global events. However, the network also serves to spread misinformation. Misleading online content has led numerous people to make a number of assumptions that constitute a danger to themselves and to society in general. We have seen people denying the existence of the pandemic, believing that vaccines are more dangerous than the virus itself, and violently protesting against the measures taken by governments to contain the disease. The aim of this project is to develop a robust misinformation detection methodology for social media (especially Twitter) that is independent of the specific application domain by quickly classifying event-specific misinformation on arbitrary topics and identifying deliberate attempts to manipulate public opinion through social media.

Detecting Fakes in Social Media: Identifying Radicalization

Suspicious behaviour on social media is portrayed under a number of labels, such as fake news, disinformation, compromised accounts, identity fraud, propaganda, hate speech, or radicalisation. All listed behaviours share a common trait: they divide society. The aim of the project is to detect and predict radicalisation events for individual users on social media. The core assumption is that most people that end up radicalised do not start out that way. Radicalisation is a process developing over time. In particular, this process can be a gradual shift towards more and more extreme positions. Even though the line between being radicalised or not can be fuzzy, we apply some simplification and binarise this process. Since the main goal of the project is to predict radicalisation events, the CYD Campus researchers had to define the point in time where they assume that a shift toward a radical attitude has taken place. The lexical diversity of a user's posts is generally high during the period in which the radicalisation event occurs and lower thereafter, which is why they have adopted this information as an indicator for a change in behaviour. Identifying the most influential features in the information flow makes it possible to provide early warning signals when the intention to radicalise can be pinpointed.

Tweets Propagation Tree



from fake news

from authentic news

- the central root node displays a news report;
- the nodes marked in black show highly influential users;
- the nodes highlighted in pink show retweets;
- the yellow colored nodes show quotations from the original message or from a retweet.

Investigation of Multimodal Embeddings for the Characterisation of Information Operations

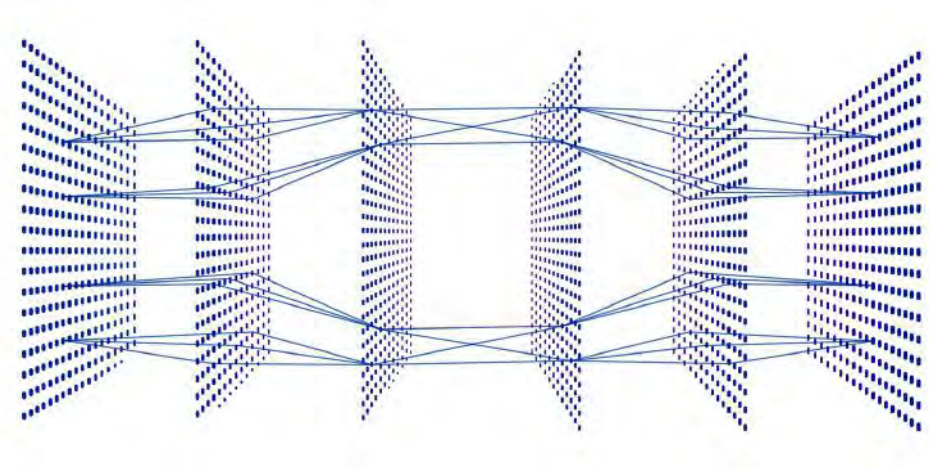
Information operations have become ubiquitous in social media, which has fuelled the demand for tools that can identify, track and analyse such content. Social media posts are often multi-modal, regularly comprised of text and imagery. Recent advances in Deep Learning allow internet-scale datasets to be used to condense high-dimensional uni- and multi-modal data to low-dimensional representations which can be used for downstream tasks. The aim is to investigate if such models can be adopted to analyse information operations on Twitter using zero- and few-shot learning. The ability of such models to characterise image types, topics and the emotionality of posts on social media is investigated.

In the area of image data emotionality, a novel zero-shot method using Contrastive Language-Image Pre-Training (CLIP) and specially constructed text modules was implemented in this framework to classify the valence of a given image (11-level Likert scale, from 1 very negative to 11 very positive with 6 as a neutral value). It was shown that the CLIP-based approach performs better in predicting valence values than widely used baseline methods (ResNet architectures). Furthermore, a method for the classification of 6 basic emotions (+1 neutral emotion) was implemented using a combination of CLIP embedded features and traditional machine-learning methods (SVM, random forests, logistic regression).

In summary, the project provides a solid theoretical and practical understanding of CLIP for zero/few-shot classification tasks in the context of information operations analysis. In addition, the project has developed an API that implements the developed algorithms and is readily available for purposes of demonstration and study of feasibility. The experiments have demonstrated the effectiveness of large pre-trained models for classification according to different features of posts in social media. Such models can play a crucial role in dynamically analysing these datasets.

Automatic Classification of Image Information: Authentication and Integrity of Videos against Manipulation

The aim of this research project is to develop a method that implements a digital signature of video data. With such a signature, it should be possible to verify the authenticity of the video data (i.e. origin and integrity of the content). Such a mechanism is particularly important in view of the increasing threat of manipulated video content (e.g. deep fake videos). For instance, officially produced video content could be provided with a digital signature, which in turn can be electronically verified by the recipient. In this sense, the electronic signature can be seen as a preventive measure against manipulated video content. In order to implement this, research is being conducted on a combination of cryptographic primitives with modern Deep Learning methods (so-called Vector-Quantized Variational Autoencoders). A first functional prototype is available for short video sequences.



Multi-modal Information Gathering and Fusion: Acquisition and Visualisation of Data Flows in the Online Advertising Sector

This research project is examining methods for client-based acquisition and visualisation of data flows to third parties in conjunction with online advertising. The goal of this project is to better understand which data flows are generated to third parties when using the Internet. It has already been shown that online advertising, in addition to being used to collect personal information, is also utilised to finance platforms for distributing disinformation and malware. A platform was therefore created in this project which can be used to raise staff awareness of these issues. The tool “webXray” was used to analyse the data and D3.js used to display the data. The visualisations comprise networks which give an impression of economic relationships between websites and third parties, as well as descriptive statistics, which provide information about the extent of the data collected.

Detection of Cyber Attacks on Electrical Systems

The energy transition is transforming the topology of electricity networks. The phasing out of nuclear power and the increasing electrification of transport means are pushing power grids to operate in new operational modes. It is thus expected that production and consumption patterns will be marked in the coming years by increasing uncertainty and greater fluctuations. This transformation impacts the cyber security of such networks. These new conditions require more flexibility and shorter reaction times from network actors, especially operators, as well as new cyber security tools. The CYD Campus is developing machine-learning methods to detect certain types of cyber attacks. In particular, we have shown, by analysing production and consumption cycles, that distortion and replay attacks are quickly and efficiently detected.

Early Warning Signals in OSINT: Anticipating Conflicts

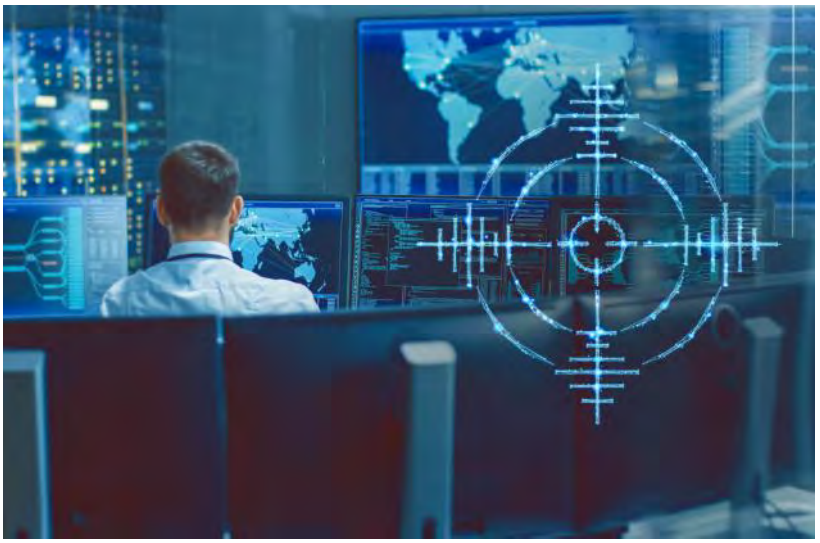
Anticipating conflicts is a key task for governments and armed forces. Knowledge of potential conflicts or instabilities can largely influence geopolitical strategy and enable enhanced preparation. Recently, several open sources have started to collect data that can be of great importance for conflict prediction. In this context, the ACLED database (The Armed Conflict Location & Event Data Project), which contains numerous daily reports of demonstrations, protests, riots and fatalities from many countries, should be mentioned. The CYD Campus employees developed statistical methods to identify and predict so-called tipping points that indicate a change of direction. Social media were also used to model and detect social instabilities using Machine Learning techniques.

Data Science Methodologies for Technology and Market Monitoring: Taxonomy Expansion & Linking

In order to track technology and market developments, one must be able to recognise technologies, distinguish them, and understand their relationships to each other. Using the technology-related concepts within the Wikipedia graph, the CYD Campus proposes a method for identifying the real-world position of a new concept within an existing taxonomy based on semantic and relevant similarities. In addition, a framework for recognising the technology-related concept in non-structured text is being built by using the approach of concept tagging, which does not involve the extraction of the surface form from the raw text. In this way, it is possible to focus on the semantic content of a document rather than its textual form, and to detect concepts that are not explicitly mentioned in the text. In addition, answering questions can be used as an underlying task to link the technologies between them as well as to link the technologies to the companies tackling them.

Data Science Methodologies for Technology and Market Monitoring: Early Technology Detection & Monitoring

The objective of the project is to perform online monitoring of technologies and technology actors in publicly accessible information sources. The monitoring concerns the early detection of mentions of new technologies, of new actors in the technology space and the facts related to new relations between technologies and technology actors. The goal of this project is to answer the following research questions: “How is novelty formalised?”, “Can we train models to detect and identify novelty?” and “Can we reduce the amount of information the user needs to consume?”. CYD Campus researchers answer these questions by transforming the given task into a question/answer task, using the pre-trained language models in a zero-shot and fine-tuned setting..



Machine Translation: Dialect Identification

The identification of language dialects is a very challenging task from the perspective of linguistics and algorithmic processing of natural language. In this project, the main focus was to develop methods for language identification of small samples of text (e.g. social media posts, short messages) focusing primarily on “noisy” text and language similarity. To tackle these specific challenges, the CYD Campus employees are developing a language/dialect classifier that is robust to noise, whereby the term “noise” means any departure from the standard or known writing. They are focusing on characters and subwords as the units upon which the classification is based. The change from word to subword tokenisation opens ample space for tokenization possibilities: any substring of a word (subword) is potentially a good token especially for dialect identification where subtle lexical differences might be hidden at the subword level. Moreover, the choice of the best subword tokenization method might depend on the language that is processed and the downstream task that is performed.

Machine Translation: Universal Adversarial Perturbations

This project aims to investigate Universal Adversarial Perturbations (UAP) that would deceive various modern Deep Learning models for the task of Natural Language Processing (NLP) and in particular for the task of text translation. Unlike image processing, attacks in the NLP and neural machine translation (NMT) systems have been little studied. Since NMT systems are used in highly sensitive applications, exploring adversarial attacks, especially UAPs, is critical to the NMT model. By developing an algorithm to generate UAPs, the project seeks to analyse the vulnerability of NMT systems and understand their behaviour by explaining the existence of UAPs. The project focuses on universal attacks on NLP and NMT systems. For example, a white-box attack scenario is considered, where researchers have access to the parameters of the model, its structure and training data. White-box attacks are more interesting than black-box attacks because they are more target-specific. A black-box attack realistically simulates the attack of a typical Internet hacker. White-box attacks refer to an attack with certain detailed knowledge about the inner functioning of the system. White-box attacks usually expose more vulnerabilities of the NMT model because they can access the model parameters. The researchers are also assessing the transferability of the proposed white-box attacks to black-box settings, which is more practical in real applications. This project enables better characterisation of the vulnerability of NMT systems and outlines the necessity to design strong defence mechanisms and more robust NMT systems for real-life applications.

Machine Translation: Families of Languages and Dialects

Machine translation has made significant progress since the introduction of neural network models, and so-called transformers are currently standard for language pairs with a large volume of parallel translation data, so-called high-resource language pairs. For low-resource language pairs or in the case of a complete lack of parallel translation data, additional effort is required. In this project, the emphasis is on solutions for dealing with a low-resource language when high-resource languages from the same family are available. To train the initial translation models, transfer learning was employed using different high-resource languages, which was fine-tuned by the researchers to suit the given low-resource language. Additionally, backward translation is used as a technique to augment the parallel translation data when only monolingual sources are available. All of these techniques have been shown to enhance the quality of translation in a low-resource setting. The CYD Campus researchers also improved unsupervised NMT by simplifying existing architectures, with virtually no loss in performance, followed by an algorithm for adaptive scheduling of the training tasks. In addition, they refined tokenization models, either using subword alignment across the source and target languages or with a novel subword construction method.

5 Customer and Portfolio Analysis

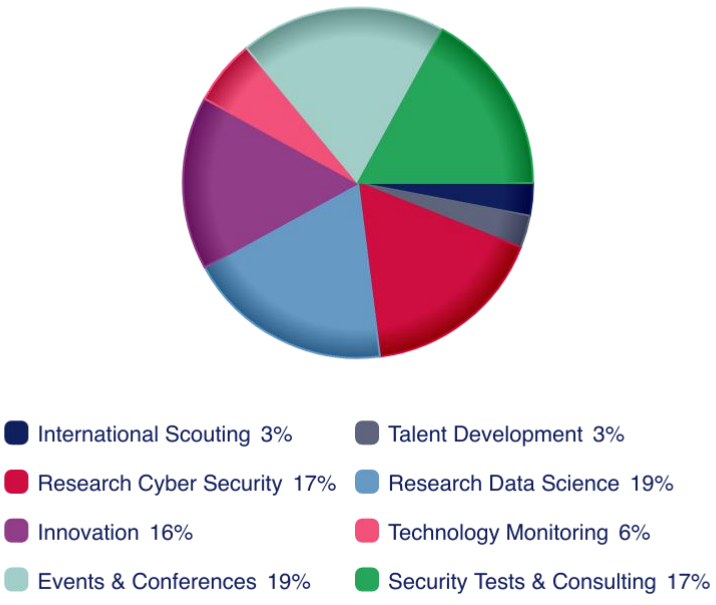
The federal government's cyber disposition is divided into three areas: Cyber security (FDF), Cyber defence (DDPS) and Cyber law enforcement (FDJP). The CYD Campus primarily provides services for the cyber defence sector. However, due to synergies especially in the technological field, the other two areas also benefit from the services of the CYD Campus. The direct services are defined in annual service agreements. In 2022, the CYD Campus provided services for Procurement, Defence and Administration.
In 2022, services were provided to the following organisations, among others:

- armasuisse
- Defence Group
  - Armed Forces Staff
  - Project Cyber Command
  - Armed Forces Command Support Organisation (FUB)
  - Joint Operations Command
  - Training and Education Command
- Federal Intelligence Service
- Federal Department of Finance: National Cyber Security Centre (NCSC)
- Federal Office for Civial Protection
- Federal Office of Police (fedpol)

The evaluation of the CYD Campus Portfolios for 2022 is presented in the figure below. The most important core services were in the areas of research, innovation, security testing and consulting, as well as in the organisation of events for the cyber community. The legend in the table provides information regarding the distribution of the assignments that were processed under the portfolios in 2022.

Note: *For classification reasons, the contractual services cannot be described in more detail in the Annual Report.*

Portfolio Evaluation of CYD Campus
2022



6 Innovation

The CYD Campus supports technological innovations for public administration units and defence with a technology readiness level (TRL) of 4 to 6. The aim of the innovation projects is to implement the research results or new needs in the form of demonstrators for the customer and to prove the applicability of the technology in practice for the customer.

6.1 Innovation Projects Results

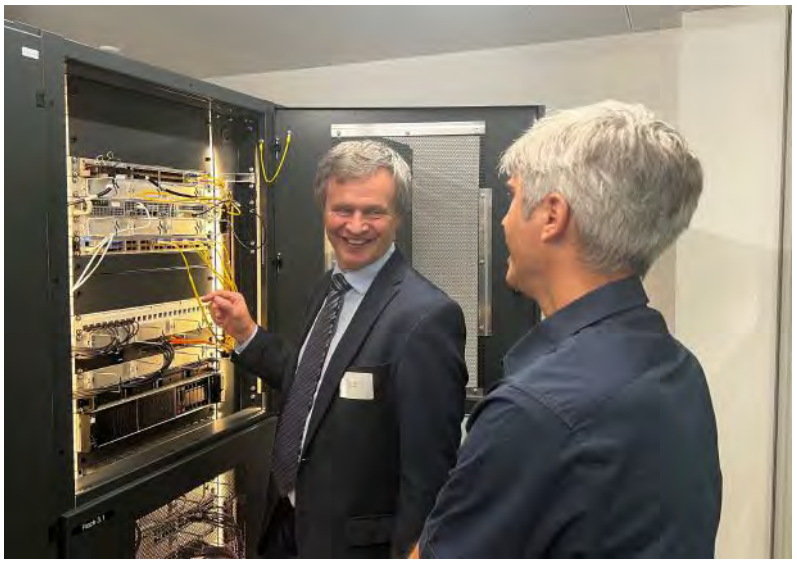
For classification reasons, we cannot present explicit results, which is why a generic overview of selected results is provided.

Secure Smartphone

The aim of the project is to enhance the security of a smartphone operating system by integrating virtualisation and the SCION technology. SCION is a cutting-edge internet architecture that offers robust security, efficient packet forwarding and scalable routing capabilities by organising networks into isolated domains. In this project, a SCION gateway was integrated into Android to route all native application traffic through the secure SCION network. Virtualisation was used to isolate security risks and provide multiple instances of the Android operating system, each with a different level of confidentiality. The project has successfully demonstrated the ability to run Linux on a virtual machine on a smartphone, using the native display for the first time.

SCION Technology

The CYD Campus has been working on setting up a SCION network connecting the three CYD Campus locations in Thun, Lausanne and Zurich.
The goal in 2022 was to set up a SCION testbed to test various state-of-the-art network attacks and defence measures: secure routing techniques, including explicit path routing, secure route confirmation, defences against distributed denial of service (DDoS) attacks and traffic obfuscation.
In November 2022, a functional link between the CYD Campus sites was established and successfully tested through independent service providers, ensuring further exploration of the SCION protocol.



Launch of the SCION testbed with Toni Eder, Secretary General DDPS and Ivo Stragiotti, CYD Campus employee.

5G

5G is the latest generation of mobile networks offering significant advances in terms of speed, capacity and connectivity compared to previous generations. Currently, 5G still relies on the previous 4G network as the backbone, but the full 5G Stand Alone (SA) architecture will be introduced for commercial use in the future. 5G SA introduces new features like network slicing, but also new security vulnerabilities that need to be addressed. The CYD Campus is examining the security implications of network slicing and is looking for ways to mitigate vulnerabilities. In the future, network slices can be used to isolate 5G instances, for example for the government.
Another security aspect of 5G is Lawful Interception (LI), where telecom operators provide intercepted network data to law enforcement agencies. The 5G SA core network aims to prevent sensitive information from being intercepted by unauthorised parties by providing an interface that is only accessible to authenticated law enforcement agencies. The CYD Campus worked on a project to develop a more privacy-preserving and scalable LI interface by combining technologies such as fully homomorphic encryption (FHE) and information theory.

Homomorphic Encryption to Strengthen Collective Cyber Resilience

Defence systems lose effectiveness if they do not have access to an up-to-date and comprehensive database. At the same time, cyber security information is highly sensitive and confidential. This creates tension between the benefits of improved threat response capabilities and the drawbacks of sharing critical information with third parties. Tune Insight's software mitigates this conflict by enabling stakeholders to share even critical and high-value cyber security information without having to share or disclose details to each other. This allows all stakeholders to gain valuable insights and build machine-learning models based on more comprehensive and relevant collective threat intelligence, which enables better defence.
The CYD Campus is developing and testing this new software solution together with Tune Insight, the University Hospital Zurich (USZ) and other critical healthcare infrastructures. The goal is to enable organisations in Switzerland to better collectively defend themselves against cyber attacks.

Cyber Toolkits for Cyber Defence Exercise «Locked Shields»

In the Locked Shields exercise, Blue Teams have to defend themselves against a variety of cyber attacks. Over 8000 attacks were carried out against each Blue Team during the course of the exercise in 2022. While most of these attacks are automated, Red Teams also carried out manual, sophisticated attacks, imitating a nation-state adversary. Locked Shields is an optimal opportunity to test different technologies and specific products to respond to a cyber attack. For this reason, the CYD Campus has partnered with innovative Swiss companies to provide the Swiss Blue Team with the most suitable and innovative tools.

Each team had to defend an infrastructure consisting of over 40 web applications running on a number of virtual machines. Just like a real network, these applications and web servers had vulnerabilities and bugs, were sometimes misconfigured, or simply not updated to the latest version. Each of these scenarios could allow an attacker to penetrate a company or organisation's network. In order to increase the level of complexity, the Red Team had injected several backdoors, such as web shells, prior to the start of the exercise, which gave them easier access. Since updating and patching all services that are exposed to the exercise internet (and thus attacks) is too time-consuming, it was decided to use the Airlock Web Application Firewall as part of the Cyber Toolkit for the Swiss Blue Team. It was deployed to protect a wide range of applications, from webmail to websites, software repositories to interfaces of services used by critical infrastructures. The use of this product is described below.
The first phase of the exercise consisted mostly of automated and known attacks (OWASP Top 10). Thanks to the well-maintained standard rule set of the Airlock Web Application Firewall (WAF), the infrastructure could be successfully protected. Although the attacks became more sophisticated during the course of the exercise, the WAF was able to keep up with more exotic cases.

One such case was an attack on the Content Delivery Network (CDN) deployed in the exercise. The CDN provider distributed malware through the CDN instead of legitimate software, resulting in defacements, cross-site attacks and attacks on legitimate users. In this case, Airlock WAF was used to rewrite the addresses of the malware resources into legitimate and secure content, thus successfully blocking the attack.

In summary, the Swiss Blue Team was able to successfully deploy the technology and respond quickly to evolving attacks, which is a good example of the effective collaboration between the CYD Campus, Swiss industry and the Swiss Armed Forces.

Content Delivery Network (CDN)	A content delivery network improves availability and scaling in the delivery of online content such as websites, videos and applications. When a large number of users request content, it is delivered faster using locally distributed content servers. CDNs also help to keep the load on the origin server low as the number of users and content delivery increases (scalability).
Web-Shell	A web shell is a type of backdoor or malware that allows attackers to remotely control a web server. Web shells are usually hidden in legitimate websites or uploaded to the server via vulnerabilities in web applications. Once the web shell is installed on the server, the attacker can use it to execute arbitrary commands, upload or download files and perform other actions on the server.
OWASP 10	The OWASP Top 10 is a standard document for raising developer awareness and web application security. It represents a broad consensus on the most important security risks for web applications.

Overview of Cyber Situation

The existing governmental "Information Sharing and Analysis Centres" (ISAC) procure, analyse and exchange information in order to protect Switzerland's critical infrastructures. This is essential as a protection against the growing number of cyber threats and must be constantly developed to keep pace with new ones. ISAC gathers information from partners such as fedpol, Govcert, critical infrastructure operators and private institutions to create an overview of past and current threats. A proof of concept (PoC) was used to test the feasibility of a central platform that integrates different tools and allows cross-referencing of events. Three open-source tools were investigated for the PoC: MISP, TheHive/Cortex and OpenCTI. The PoC was built with a microservice architecture and relied mainly on Docker. The platform was continuously tested by partners to understand the requirements for the final product. The proposed solution recommends replacing TheHive and Cortex Evolution with a custom platform developed in-house that uses a central database for data storage and is based on a Kubernetes cluster or a single high-performance server.

Cyber Training- Simulation Cyber Incident Response

Managing a cyber incident requires cooperation and communication between the cyber response team, management, employees and often the public. The speed with which a cyber incident can unfold, combined with the uncertainty involved, makes handling such a crisis particularly challenging. Besides strong scenario-based playbooks, in order to improve the handling of such situations, it is important to train and test the response. This is mostly done with table-top exercises. However, in the light of increasing digitalisation it makes sense to use computer-based tools, especially given that most of the communication will happen online or through online-based channels such as emails, websites and social media. The Cyber-Defence Campus, together with the Joint Operations Command and the Armed Forces Command Support Organisation, tested a crisis simulation platform from the company Conducttr to effectively prepare for future cyber crises. Several tests were successfully carried out with the participation of civilian experts, military and militia units. allowing the Swiss Army to increase the knowledge and possible use cases for this technology.

6.2 Cyber Startup Challenges

2022: Network Detection and IoT Device Security

The Cyber Startup Challenge 2022 was organised by the Cyber-Defence Campus to explore the startup landscape in the area of Internet of Things (IoT) device security. 36 startups from around the world participated and presented innovative technologies in the field of network detection and IoT device security. The jury nominated the three finalists: ONEKEY, Narrowin and Sepio. ONEKEY provides automated security analysis of IoT devices and operational technologies that reduces the time required to identify and remediate vulnerabilities. Narrowin's Lightweight Network Explorer enables real-time monitoring and analysis of network structures, reducing complexity and effort. Sepio's Asset Risk Management platform detects, assesses and mitigates known and unknown risks using a novel algorithm and a threat intelligence database.
The German startup ONEKEY won the Cyber Startup Challenge 2022 and convinced the jury with its innovative technology for automated security and compliance analysis of IoT devices and operational technologies (OT). ONEKEY's solution uses "Software Bill of Materials (SBOM)" and "Digital Twins" to detect and isolate security vulnerabilities and compliance breaches. This technology can be integrated into software development and procurement processes and is used by leading international companies.

2021: Strengthen your Information Sharing and Analysis Centre (ISAC)

In 2022, collaboration continued with the Swiss startup Decentriq, the winner of the Cyber Startup Challenge 2021. The Challenge focused on the topic "Boost your Information Sharing and Analysis Center (ISAC)". Decentriq offers a software-as-a-service (SaaS) platform that enables secure and private data collaboration. The startup provides "Data Clean Rooms" that allow financial institutions to share incident data and gain anonymous insights without compromising privacy. Decentriq uses "Confidential Computing" technology to ensure that no one, including the platform operator, has direct access to the data. The platform thus offers a solution to the trade-off between sharing sensitive data and protecting it. Within the use case of the innovation project, several banks share phishing emails in order to analyse them and gain insights to improve their cyber security and better protect their customers. A successful proof of concept was implemented with three large Swiss banks in 2022.

7 Security Analyses, Penetration Testing and Security Consulting

In 2022, CYD Campus employees examined the security of a dozen military systems that are being processed as part of armament and ICT procurements within the DDPS. The tests were conducted as security analyses, penetration testing or security consulting. The clients were in most cases the procurement units of armasuisse.

The focus was on the following areas:

- Windows platforms
- Linux platforms
- Web applications
- Middleware
- Computer networks
- VPN technologies and crypto solutions
- Command and control information systems
- Drones
- Vehicles
- Wireless communication systems (voice and data)
- Aviation and satellite communication systems

The analyses and audits led to security measures that were subsequently implemented in the procurement projects or are borne as remaining risk by the decision-makers as part of the information security and data protection concept (ISDS).

Note: *For classification reasons, the security analyses, penetration testing and security consulting services cannot be described in more detail in the Annual Report.*

Security Advisories 2022

The CYD Campus regularly finds vulnerabilities in manufacturers' software and devices. These vulnerabilities are disclosed according to a so-called Responsible Disclosure procedure. According to this procedure, the manufacturers are informed first and only after a reasonable period of time to fix the vulnerabilities are the people affected notified or informed about the vulnerabilities.

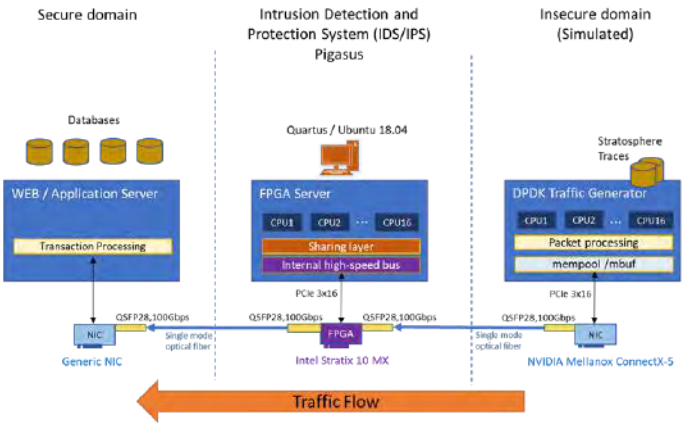
Vulnerabilities are scored according to the Common Vulnerability Scoring System (CVSS). CVSS is an industry standard for assessing the severity of potential or actual security vulnerabilities in computer systems. In the CVSS, the security vulnerabilities are evaluated according to various criteria, so-called metrics, and compared with each other so that a priority list for countermeasures can be created.

Hardware / Software	Date	CVSS	CVE
Combined Charging System (CCS)	February 22	6.5	CVE-2022-0878
CVRF-CSAF-Converter	March 22	5.7	CVE-2022-27193
CSAF Provider	May 22	6.2	CVE-2022-43996
e***	September 22	10	
Plantronics Hub	September 22	7.8	
Elvexys StreamX	December 22	6.5	CVE-2022-4778
Elvexys StreamX	December 22	7.5	CVE-2022-4779
Elvexys ISOS	December 22	4.5	CVE-2022-4780

8 Demonstrators

Demonstrator: Architecture of the 100 Gbps Intrusion Prevention System

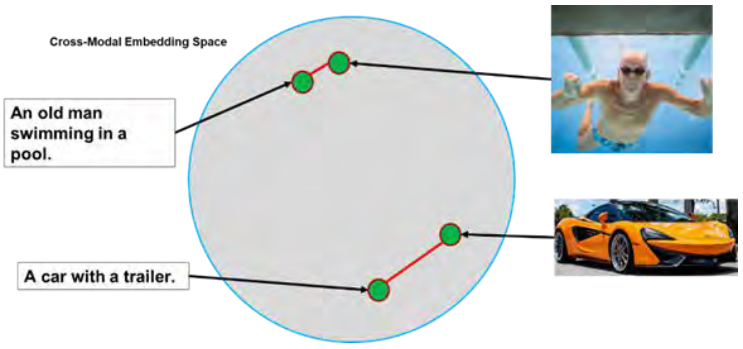
Intrusion Detection and Prevention Systems (IDS/IPS) such as SNORT require a lot of processing power when analysing high-throughput traffic. Analysing a traffic stream of 100 Gbps typically requires multiple servers. This demonstrator shows how to implement a 100 Gbps intrusion prevention system using only a single server. The idea is to offload CPU-intensive tasks to an FPGA and to use the acceleration performance of modern FPGAs. The demonstrator includes an Intel Stratix 10 MX FPGA which is combined with a Intel Xeon CPU with 16-cores to handle up to 100 Gbps.



Architecture of a 100 Gbps «Intrusion Prevention System» with only one server.

Demonstrator: Automatic Evaluation of Image Data in Disinformation Campaigns

In this demonstrator, the technical potential of a recently published Deep Learning method, the so-called "Contrastive Language-Image Pre-training" (CLIP), is shown. The method is based on an anonymised dataset published by Twitter for research purposes. The special feature of CLIP lies in its ability to measure similarities between text and image content (see Figure 1). This capability opens up a variety of potentially very interesting applications: semantic searching of images (analogous to Google Image Search but on a local server), classification of images without a training process, and exploration of large sets of images for trending content. The purpose of this demonstrator is to show these potential applications of CLIP and illustrate them in an intelligence context.



Ability of Contrastive Language-Image Pre-training (CLIP) to map both image data and text data into a vector space. Within this vector space, similarities between image and text content can then be measured, allowing for a variety of interesting applications.

Demonstrator: Mixed Reality for Training Simulation

Mixed reality (MR) describes the blending of the real, physical world with a virtual reality, i.e. with a computer-generated, interactive environment. In order to use this mixed reality for training purposes, a demonstrator has been developed.

The goal of the demonstrator is to bring innovation to training simulation, to test the conservative claims of the industry, to demonstrate the potential of mixed reality in simulation training, and to assess and evaluate the limitations of the technology. Driving a tank is simulated.

Use of the demonstrator for tests with people.

The potentials of mixed reality include:

- Increased physical and operational situational awareness
- Cost reduction in training and education
- Improved training and mission preparation
- Flexibility and (partial) mobility in training, education and mission preparations
- Better support (maintenance, logistics, medical forces, etc.)
- More effective sensor-message-guidance-impact network
- Conservation of material and the environment
- Execution of scenarios that are impossible or difficult to realise in the real world (emergency scenarios in vehicles, execution of large exercises, operations in urban areas, etc.)

Mixed reality demonstrator for training simulation.

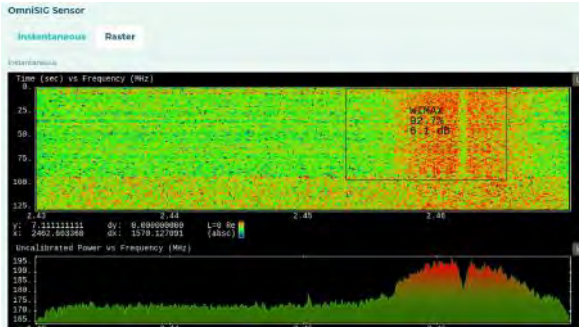
There are certain risks associated with using the technology, including:

- Virtual reality (VR) or simulator sickness
- Data and information overload
- Strong dependence of MR during operation
- Strong dependence on ICT services
- Security (integrity of the systems, availability of the services, confidentiality of the data)
- Possible strong impact on doctrine, especially on training
- Alignment of education, training, and deployment
- Lack of interoperability and frameworks
- Low market maturity
- Low MR readiness level for military uses

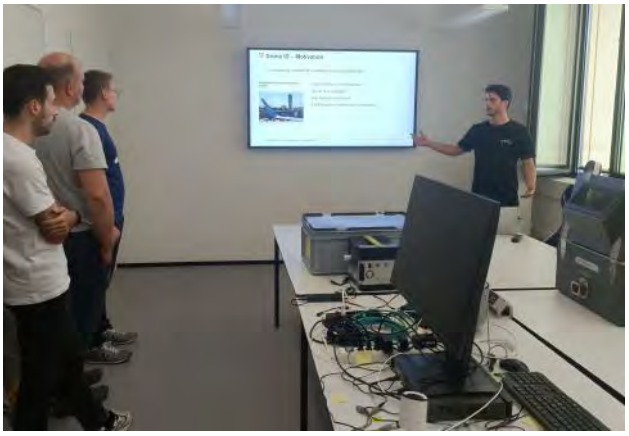
The first results with the demonstrator show that although there is great potential, bundling the different components and overcoming the risks is challenging. The demonstrator was developed in a first step as a virtual demonstrator (virtual reality VR). The transition from VR to MR in 2022 has proven to be particularly demanding. The different dynamics between real and virtual images still need to be mastered.

Demonstrator: Signal Classification

Cyber warfare and electromagnetic warfare have usually been considered as separate fields. Today, we see a convergence of both fields towards an integrated understanding and use of technologies. This is also evident in the context of modern hybrid warfare operations. Against this background, it is becoming increasingly important to be able to classify signals in the electromagnetic spectrum with limited computing power and with increasing flexibility. Today, there are several research approaches that use Deep Learning techniques to classify spectrum data. The work started in 2021 has been extended to demonstrate broader functionality when working with different types of waveforms.



Demonstrator uses machine learning models to classify the electromagnetic spectrum in real time.



Presentation of the demonstrator to students of the Lucerne University of Applied Sciences and Arts.

Demonstrator: Drone Hijacking with GPS

The demonstrator drone hijacking shows a method where a radio transmitter is used in the vicinity of a drone to fake an authentic GPS signal. Drones that rely on GPS signals to determine their location can be affected. It has already been demonstrated how a drone reports the fake location back to the pilot. The demonstrator now focuses on how a drone can be hijacked using this approach. The basic idea is to constantly fake nearby locations and simulate real movement so that the drone keeps moving and the faking transmitter has full control over the movement of the GPS drone. This technique could consequently be used by a legitimate actor to hijack drones from malicious attackers and thus protect themselves from drone attacks.

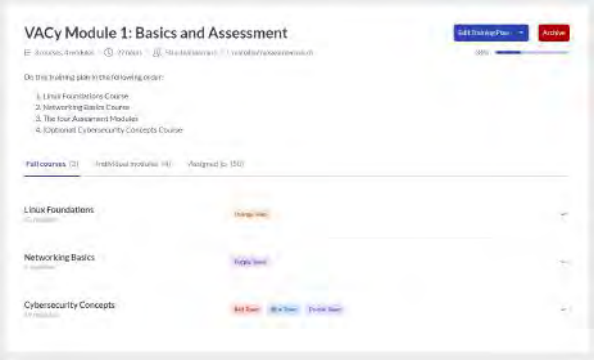
Demonstrator: Augmenting Reality for Security

Augmented reality (AR) allows a person to interact with their real environment which is augmented with virtual information and objects. This demonstrator considers the applicability of AR as a tool for users to defend themselves against cyber security attacks such as phishing. AR goggles can simulate a cyber security expert "looking over the user's shoulder" to assist in defending against attacks. This approach enables a much better defence against phishing and spear phishing compared to traditional methods.

Evaluating augmented reality for better defence against phishing using the demonstrator.

Demonstrator: Gamified Cyber Training

It is well known that there is a systematic shortage of qualified workers in the cyber security domain; one possible remedy to this problem is to attract more people to be trained in this field. To effectively reach young people, it is necessary to offer something appealing. In this context, gamification in cyber education can make an important contribution. Gamification refers to applying game-typical elements in a non-gaming context. To test different scenarios and hypotheses, CYD Campus associates considered the products of several startups and tested two of them with a group of young people. With the experience gained in this first experiment, it was possible to move on to a more extensive test. The 50 young people who are part of the first pilot of the Pre-Service Cyber Training (completion December 2022) were able to use the innovative software of one of the selected startups.



Software environment of the demonstrator for the pre-service cyber training of the Armed Forces.

Demonstrator: Visualisation of Critical Infrastructure Attacks

When performing capture-the-flag or live-fire exercises, it is often difficult for cyber security experts and decision-makers to understand the impact of cyber actions on physical infrastructure. This is because, unlike attacks on cyber-physical systems such as power generation plants or military (weapons) systems, it is comparatively less straightforward to detect when a website fails to load, malicious emails arrive or ransomware enters a computer. To identify the best cyber training tools for the Swiss Armed Forces, a demonstrator was built to illustrate these effects. It consists of a 2.4 x 1.2 metre terrain model, which is modular and easy to move, with a mixed civilian-military airport as well as critical infrastructure, energy production and military systems. This layout was expanded in 2022. A physical representation of a pumped storage power plant was added, using real programmable logic controllers (PLCs) and sensors and actuators. This can be used for demonstration, but also for research and training in operational technology (OT).

Visualisation of cyber attacks on a military airfield.

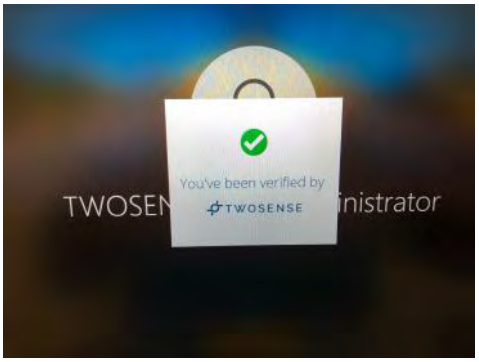
Demonstrator: Offline Translation

The exchange of information in different languages has become a necessity. Machine translation tools have also become an integral part of our everyday professional lives. However, these online translation tools also carry with them significant privacy risks, especially when dealing with sensitive information. It is therefore imperative that automatic translation can be used without exposing the information to the outside world. For this reason, the offline translation demonstrator provides bidirectional offline automatic translation of text between English and six other languages, namely Arabic, German, French, Italian, Russian and Chinese. To avoid errors caused by incorrect language usage, a language recognition tool is also integrated. It can be used via GUI and REST API.

Example of translation from Chinese into English with an offline system.

Demonstrator: Continuous Authentication

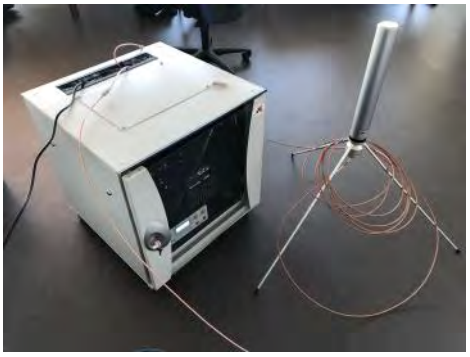
Password queries or one-time biometric checks such as fingerprint or iris sensors grant users access after successful authentication and do not regularly check for malicious behaviour or a change of user. These methods allow, for example, so-called midday attacks, where an attacker uses a workstation where a legitimate user is still logged in. Similarly, password data can be stolen through leaks, shoulder surfing or phishing attacks, giving an attacker free rein to the target system. This is in contrast to Continuous Authentication (CA), which is a method where a user is observed over an extended period of time and authentication is continuously granted or revoked if appropriate. CA thus authenticates the user's behaviour even when he/she is logged in, typically with biometric features such as gaze tracking or environmental monitoring such as wireless proximity sensing. The demonstrator automates identity security by biometrically authenticating users so that they no longer have to authenticate themselves manually. The demonstrator allows up to ten users to log in on two managed computers using the automated authentication software to demonstrate the continuous authentication capability.



Behaviour-based verification of the user by the demonstrator.

Demonstrator: Aircraft Communication Spoofing

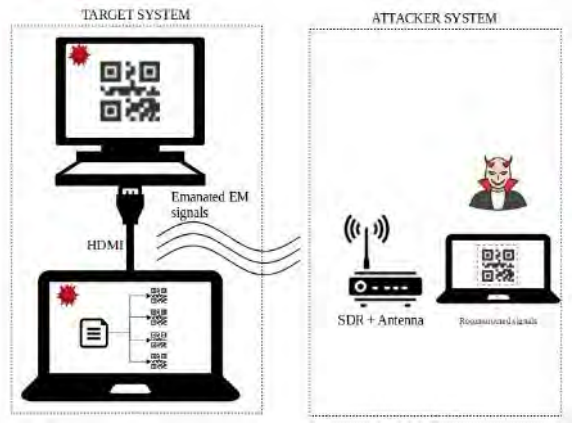
In the 2010s, researchers and hackers demonstrated numerous vulnerabilities in wireless technologies used by aircraft and air traffic controllers. To date, such spoofing has been demonstrated using low-level tools such as software-defined radios exclusively on computers with simulated hardware and software.
This demonstrator uses a realistic representation of avionics systems (hardware and software) as they are actually installed in aircrafts. Full access to these systems for the purpose of penetration testing allows CYD Campus researchers to demonstrate wireless radio frequency (RF) attacks on GPS, Automatic Dependent Surveillance - Broadcast (ADS-B), and Traffic Alert and Collision Avoidance System (TCAS) systems.



Demonstration of spoofing in the Cyber Avionics Lab.

Demonstrator: TEMPEST Data Outflow

Every electronic device generates electromagnetic emissions. These electromagnetic signals are related to how the emitting electronic components operate internally. A malicious attacker can intercept the emitted signals and investigate them to ob-tain information about the emitting device. The practice of eavesdropping and protecting against eavesdropping and their examination is summarized in a framework known as TEMPEST.
In the case of video monitors, the emitted signals can be used to reconstruct the content. It has already been shown how an attacker can use the signals from the connecting cable bet-ween a PC and a video monitor to extract internal information from the monitor. In this demonstration, the CYD Campus illu-strates how a QR code can be used to exfiltrate internal data through these emitted signals from the video monitor. Since many companies rely on computer networks as a communi-cation system to transfer different types of information between servers and workstations, it is expected that such networks will be an interesting target for malicious attackers, as some of this information may contain commercial secrets and may be highly confidential.



Exploiting the emission of HDMI video cables to exfiltrate sensitive data from an compromised computer.

Demonstrator: Anti-GPS Jamming

GPS jamming, where GPS signals can no longer be received, is a growing problem and threat to both civilian and military users. Whereas military users can rely on specific signals that are resistant to jamming, even the defence sector is increasingly dependent on non-hardened consumer hardware. Together with the Swiss Drone and Robotics Centre (SDRZ) and the sensor department of armasuisse S+T, the CYD Campus has tested a novel device that is resistant to GPS jamming due to an advanced zero-steering algorithm and a special signal filtering technology. The novelty of this device is that it can be easily retrofitted and consumes little power. The effectiveness of the device was tested and demonstrated in an approved GPS jamming test on a drone in open airspace.

GPS jamming test on a drone.

Demonstrator: Car Hacking

The CYD Campus Renault Zoe electric car is used as a laboratory for cyber security research as it is equipped with various sensors, communication devices and software systems that can be accessed and manipulated. Researchers demonstrate the car's communication networks (e.g. the CAN bus), sensors and software for vulnerabilities and potential cyber attacks.
The car also offers our researchers access to analyse the security of charging systems and their impact on the electric grid, which is highly relevant with the broader move to electric mobility in Switzerland and the DDPS. Until now, collaborators have used it to demonstrate the vulnerability of the Brokenwire electric charging system and test adversarial attacks against the camera systems and traffic sign recognition models.

Demonstration of the exploitation of security vulnerabilities of electric vehicles to eavesdrop on communications.

9 Technology Monitoring

The CYD Campus is an anticipation platform for national and international cyber developments and trends. Cyber threats and technologies are evolving rapidly, and keeping track of these trends is challenging. We are attempting to detect technical developments and understand their opportunities and risks at an early stage. To identify the most recent developments in the market, we rely on quantitative and qualitative technology and market monitoring methods developed in a Technology Monitoring (TM) Portfolio. On the one hand, emerging cyber technologies and clusters are discovered using a Technology Market Monitoring (TMM) platform through quantitative analysis of publicly available data. On the other hand, promising startups are identified through qualitative scouting, an international technology monitoring programme. The mission of the TM Portfolio is to i) identify, ii) analyse and iii) forecast trends related to cyber security technologies within a time frame of a maximum of five years.

Quantitative and Scientific Approach

At CYD Campus we make use of recent advances in big data and artificial intelligence to develop a more quantitative approach based on open data and scientific methods. A TMM platform is being continuously developed and improved in collaboration with various partners from industry and academia. The platform constantly scans dozens of open and closed data sources, which provide CYD Campus' technology analysts with aggregated insights that they combine with their experience from research and scouting activities. Predictive methods can be used to forecast trends, giving stakeholders an edge in knowledge. Actionable intelligence is provided to various types of decision-makers, including stakeholders in:

- Defence
- Cyber security
- Security policy
- Market research
- Strategic management

The TM Portfolio activities contribute to cyber strategies at different levels:

i. Confederation: National strategy for the protection of Switzerland against cyber risks (NCS)
ii. DDPS: Strategy Cyber DDPS
iii. Swiss Armed Forces: General concept cyber
iv. CYD Campus: Business architecture

An essential activity of the TM Portfolio in 2022 was the study "Trends in Data Protection and Encryption Technologies". This is also the main contribution to Measure 1 (Technology Monitoring) of the NCS. The study provides an overview of the changing landscape of encryption and data protection technologies with the aim of analysing the likely developments up to 2025 and deriving the implications for the military, civil society and business sectors. The CYD Campus, which brings together an interdisciplinary and international research community, was also instrumental in establishing the Swiss Technology Observatory in 2022.

Website Technology Observatory

10 International Scouting und Cooperation

In 2022, the startup scouting of the CYD Campus focused on Switzerland, the USA, Israel, Germany and France with a few companies located in other countries. The focus of the scouting is on the search for new technologies in the areas of cyber security and artificial intelligence with the aim of discovering the most important trends and actors at an early stage. Consultations were held with more than 80 startups and companies. The outcomes of these conversations were disseminated in a structured form to potentially interested parties within the public administration. In order to gain access to the most interesting startups and also to detect early-stage companies, the CYD Campus relies on a large network ranging from venture capitalists to accelerators, and from embassies to business development organisations. Particularly important partners are the Swisscom Outpost in Silicon Valley and the Swissnex Network (Boston, Bangalore, Tel Aviv). Another important tool for scouting is participation in world-leading conferences such as the RSA Conference in San Francisco, Black Hat, Defcon, Usenix Security, Cybertech and Cyberweek in Tel Aviv and the European Cyber Week in Rennes. These events offer the opportunity to meet a large number of companies and partners in a short period of time.

2022: 100 STARTUPS
80 technical presentations
30 of which referred to relevant agencies within the federal government
8 proof of concepts implemented
15 active scouting-partners
1 Cyber Startup Challenge

The start-ups identified during the scouting activities led to several proof of concepts, which are described in more detail in the chapter "Demonstrators". In addition, the information gained was used to support the procurement process and to better understand the cyber market.

Venture capitalist	An investor who invests in high-growth companies. Venture capitalists help prepare the company for growth. Similar to the CYD Campus, they look for innovative startups.
Accelerator programme	This is a programme that supports startups by providing access to resources, mentoring and networking. Participants in an accelerator programme often work on their business ideas and receive feedback. Startups who participate in these programmes can be promising for the CYD Campus.

International Cooperation

Cooperation with international partners is crucial in cyberspace. Since threats and malicious actors are not bound by national borders, Switzerland is dependent on close cooperation. In this context, on the one hand, the CYD Campus conducts research projects with scholars from world-leading universities such as the University of Oxford, the University of Southern California and the Ruhr University Bochum. On the other hand, the CYD Campus also cooperates with other governments and international organisations. For example, the CYD Campus represents Switzerland in the CapTechs Cyber and Information of the European Defence Agency. Depending on the needs, discussions on specific projects are deepened and CYD Campus researchers examine whether a contribution by armasuisse is beneficial. These committees also serve as a platform for informal exchange among experts. Thus, the CYD Campus is leading Swiss efforts for possible participation in a future PESCO project in the field of the Cyber-Ranges Federation (CRF). The aim of CRF is to improve the performance of European Cyber Ranges (CR) by merging existing national Cyber Ranges into a larger cluster.

NATO is also an important cooperation partner. The CYD Campus contributes significantly to the activities of the CCDCOE in Tallinn, both through the involvement of the researcher William Blonay on-site and through research contributions to the work programme of the centre. In addition, the Campus selectively participates in interesting NATO STO working groups. These projects are supported by the armasuisse office in Brussels.

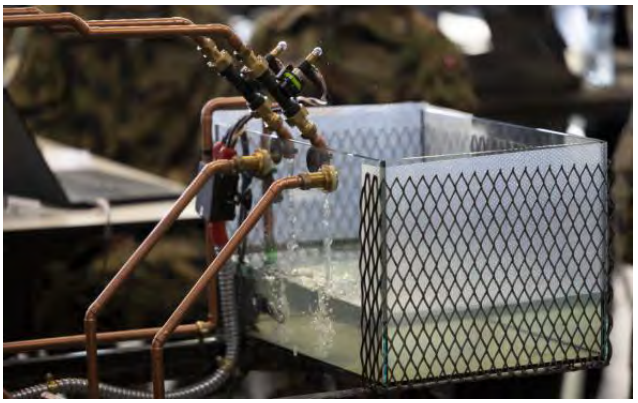
Bilateral exchange with partner organisations of the DDPS in selected partner nations is also of great importance. Depending on the respective partner country, the aim is to find researchers with matching interests in order to exchange expertise, methodologies and data or, in certain cases, to conduct joint research projects. For these projects, cooperation is carried out together with the armasuisse office in Washington, the Swiss embassies and the defence attachés worldwide.

CapTechs European Defence Agency	These are working groups where members collaborate on research and development of military capabilities.
Permanent Structured Cooperation (PESCO) Project	Designates a cooperation project of the European Defence Agency (EDA) within the framework of European defence cooperation. The aim is to improve military capabilities and promote closer cooperation between member states. Norway, Canada, the United Kingdom and the USA are also involved in selected PESCO projects.
NATO Science and Technology Organization (STO)	The organisation focuses on the promotion of scientific and technical cooperation in the field of defence. The STO encourages the development of technologies and concepts that are relevant to NATO's military tasks

11 Laboratory Infrastructures

ICS Lab Pumped Storage Power Plant

In 2022, a new ICS laboratory was commissioned at the CYD Campus in Thun. ICS is short for industrial control systems, which consist of hardware and software used to control, monitor and operate plants, machines and processes in industrial environments. They are frequently found in critical infrastructures. Since industrial control systems are expensive and have a long production cycle, suitable laboratories are needed to carry out vulnerability tests. The ICS laboratory is a representation of a pumped storage power plant. The industrial control system controls functions such as measuring the water level or operating valves and pumps. As part of the ICS Hackathon in September 2022, this lab was used to conduct targeted vulnerability analyses, investigate different attack vectors and develop effective countermeasures. This lab is used for talent development and further cyber defence research of ICS systems.



Model of a pumped storage power plant: CYD Campus ICS lab in Thun.

Advanced Cyber Avionics Lab

The Cyber Avionics lab, which was built up by the CYD Campus over two years, was presented to the international cyber community on 8 August 2022 at the 15th Cyber Security Experimentation and Test (CSET) Workshop. The testing of cyber attacks on aviation communication systems requires the utmost care in order to not disrupt air traffic. In Switzerland, airspace is occupied day and night, which is why it is almost impossible to conduct practical tests in the real world. However, in lab tests, cyber attacks can be investigated without interfering with air traffic.
In the Cyber Avionics Lab, the same certified systems are integrated and connected as in currently deployed aircraft. Therefore, statements can be made on how a real aircraft would react to corresponding cyber attacks. The tests focus on communication systems in civil airspace.

Cyber Avionics Lab to investigate cyber attacks in airspace.

5G Lab

The CYD 5G Lab operates a 5G Standalone (5G SA) core network deploying the open source software Open5GS. It is currently used for two ongoing research projects. Most of this lab is virtualised and runs in our data centre: The core network is virtualised, while the Radio Access Network (RAN) is emulated and partially virtualised. Both LXC containers and QEMU virtual machines are used for virtualisation. As this lab is growing, two real antennas (gNB) will join the lab and the core network will be moved to Kubernetes to have a Service Base Architecture (SBA) that more closely resembles a real 5G network.

SATCOM (Starlink)

To complement the existing non-permanent experimental platforms with small satellite antennas, a satcom lab is currently being established. At the centre of this lab is a 2.5-metre diameter satellite dish mounted on a motorised platform. It allows CYD Campus staff to align the dish with the satellites via a configuration platform and, in the case of non-geostationary satellites, to follow their orbit. The dish's receiver is designed to receive a variety of frequencies, allowing researchers to use multiple frequency bands simultaneously. In 2022, the basis for a consolidated lab was created by adding a purpose-built container to the roof of the Georg-Herzog-Haus in Thun. In addition, a Starlink dish has been installed to examine this novel and highly relevant constellation in practice.

SATCOM Cyber Security Lab.

SCION (Thun-Lausanne-Zurich)

The three CYD campus sites in Zurich, Lausanne and Thun were equipped with SCION network connections in November 2022 and will be available to the armed forces and security authorities as a national test infrastructure for three years. SCION enables secure and controllable routing. In addition, programmable switches at the sites offer the possibility to implement new obfuscation methods for data traffic in the network and to examine their efficiency. During this period, the resistance of the SCION technology to various forms of cyber attacks, such as DDoS attacks or route hijacking, will also being tested. In addition, the implementation of the technology for the needs of Swiss cyber defence is to be expanded and tested on the basis of concrete use cases. Security tests will be conducted by employees of the CYD Campus as well as associated partner organisations from industry, universities and the army.

SCION network topology enables efficient routing based on different criteria (Source: anapaya.net)

Internet of Things (IoT) Laboratory

The IoT cluster consists of about 50 single-board computers, most of which are Raspberry Pis of various models. This cluster serves different scenarios. First, some experiments are conducted whose aim is to identify malware that infects the devices, as well as to mitigate the attack. In addition, CYD Campus researchers are experimenting with the hardware fingerprints of these Rapsberry Pis in order to use them as unique identifiers. Furthermore, this cluster is also used to test a distributed machine learning framework simulating a real environment of edge computing.

IoT Lab in Thun.

Data Science Lab for Machine Learning Operations

The Data Science Lab (DSL) enables the CYD Campus researchers to implement digital projects according to modern standards of scientific activities and software development. For this purpose, the DSL maintains applications for versioning (based on Git) of instructions (code) and can provide computer and storage capacity as required. In order to ensure optimum use of the available resources, various mechanisms have been implemented in the DSL which are typically used in cloud infrastructures. The DSL thus has access to storage capacities which can be made available in a flexible manner for individual projects and can be adapted to changing requirements at any time. General computing power is assigned to the projects in the DSL on a dynamic basis. This enables the development and usage of numerous implementations, from web applications to the processing and analysis of data. For highly specialised analyses, such as those which require the application of deep learning algorithms, a network of graphic processors can be addressed indirectly via a central management application. This architecture, also known as a cluster, enables efficient and fair usage of limited resources. Using this configuration, the DSL offers the option of defining projects completely, from the automated connection of resources to the analysis and provision of results in a declarative form as a list of instructions (code). The entire development can thus be versioned in a project in the DSL, the versions tested automatically and made available as required. This practice combines automatic resource management, also known as “Infrastructure as Code (IaC)” with modern standards from the area of software development (DevOps) or machine learning (MLOps).

Data Science Lab in Thun.

12 Events

Conferences

28 November–2 Dezember 22 MILCOM, Washington D.C., USA
At MILCOM, scientists gather around the topics of military communications and data analysis. Gérôme Bovet, head of the Data Science group, was the organiser of a panel within the framework of the NATO working group IST-ET-121 and was invited by the US Army Research Lab to hold a presentation.

15–17 November 22 Rennes European Cyber Security Week
More than 4000 public and private actors and 84 partners in the field of cyber security met in Rennes to identify and anticipate future technological developments. The CYD Campus participated in order to connect with relevant stakeholders.

10–11 November 22 10th OpenSky Symposium, Delft, Holland
Martin Strohmeier gave a presentation on the danger of open aviation datasets and presented the latest research results.

26 October 22 CYD Campus Conference
The CYD Campus Conference 2022 was held on 26 October at the Kursaal in Bern. During the event, experts from public administration, academia and industry gave presentations on key topics in the area of securing future digital infrastructures. The CYD Campus welcomed more than 300 participants to this conference.

14–16 September 22 CRITIS, München, Deutschland
CRITIS brings together researchers, academics, critical infrastructure operators, industry, defence and government organisations working in the field of security of complex infrastructure systems. At CRITIS 2022, Llorenç Romá presented a research paper showing how information from critical infrastructure can be secretly and systematically exfiltrated.

26–29 Juni 22 Cyber Week Tel Aviv, Israel
Giorgio Tresoldi presented research findings on cyber security in civil aviation at a panel discussion organised by the Israeli National Cyber Directorate.

6–20 Juni 22 RSA Conference, USA
In addition to attending the conference and having the opportunity to meet numerous startups, the CYD Campus organised a networking event at the Swiss Consulate together with Swissnex and the Swisscom Outpost in Silicon Valley.

30 Mai–2 Juni 22 CyCon, Tallinn, Estland
At the 14th International Conference on Cyber Conflicts (CyCon), CYD Campus researcher Martin Strohmeier participated in the panel discussion "Cyber Security Threats in the Transport Industry" and shared his research on security and privacy issues of satellite communications in aviation.

6–7 April 22 Swiss Cyber Security Days, Freiburg
Martin Strohmeier, CYD Campus researcher, gave a presentation on the security of electric cars and charging infrastructures during the conference.

27–28 März 22 Applied Machine Learning Days, Lausanne
- Workshop on visual disinformation by Raphael Meier, CYD Campus researcher
- Organisation of an Artificial Intelligence & Cyber Security Track by Martin Strohmeier, together with C4DT
- Presentation by Vincent Lenders on the role of artificial intelligence in cyber defence

Coffee Break at the CYD Campus Conference 2022.

Challenges & Hackathons

3–7 Oktober 22 Hackathon ElectroSense
This year's hackathon focused on the LoRa protocol. Three teams worked on localising LoRa transmitters, fingerprinting and developing an OSINT LoRa platform. During different events in 2022, the participants had the opportunity to prepare their activities so they could immediately start analysing data at the hackathon.

19–23 September 22 ICS Hackathon
The CYD Campus, together with Cyber Battalion 42, organised a hackathon around Industrial Control Systems (ICS) and Operational Technologies (OT). The 30 participants conducted vulnerability tests, investigated various attack vectors and developed suitable countermeasures. Further information can be found in the chapter Highlights.

5–7 September 22 Satcom Hackathon
The CYD Campus organised a hackathon on satellites and satellite communication. The 10 participants came from university collaborations and other federal agencies. The aim was to examine and understand ground stations, CubeSats and communication between satellites and to find possible attack vectors.

Data Science Challenges

16 November 22	Kubernetes
31 September 22	Early warning signals
12 September 22	Detection of sarcasm
15 August 22	Detection of anomalies in IoT device behavior
20 June 22	Multimodal image and text queries
28 March 22	Detection of disruptive events

Security Challenges

5 December 22	Hack the Box
3 October 22	Scavenger Hunt
29 August 22	WebApp/Linux Hacking
13 June 22	Android Application Hacking
4 April 22	Static Reverse Engineering

New opening of Zurich office

24 November 22
In 2022, the CYD Campus celebrated the reopening of its premises at Zollstrasse 62 in Zurich together with selected research partners. At the same time, the three CYD Campus locations (Thun, Lausanne, Zurich) were connected with SCION network connections. The technology replaces the insecure internet routing protocol with a more secure and efficient protocol.

Lunch seminars

During these information events, lectures on specific CYD topics are organised by selected speakers for customers of the Defence and Federal Administration.

28 November 22	Post-Quantum Cryptography Speaker: Jean-Charles Faugère, CTO CryptoNext Security AG
29 August 22	Secure and Private Computing, Speaker: Prof. Dr Katerina Mitrokotsa, University of St. Gallen

Research reports

The annual reports are used to inform about ongoing research projects on behalf of the clients and interested parties. The reports took place in hybrid form, with around 80 guests being welcomed in each case. Some of the participants were from the Armed Forces Staff, AFCSO, GS DDPS, FIS.

2 September 22	Research report 3b Data Science
6 July 22	Research report 3a Cyberspace

Retreats

4–8 July 22 Cyber Alp Retreat in Sachseln
Researchers from the CYD Campus and selected research partners met in Sachseln (Obwalden) and gave presentations on key topics such as the Internet of Things, traffic safety, disinformation in social media, and technology and market monitoring. The event brought together 120 participants from the DDPS, industry and academia to exchange views on current and future challenges and drivers in cyberspace over a period of several days.

Lunch seminar on Post-Quantum Cryptography.

Cyber Alp Retreat 2022 in Sachseln.

Cyber Security Jam Session in Zurich.

Visits

20 December 22	Austria Working visit, Zurich
20 December 22	Visit Kdt LVb Pz / Art
28 November 22	Visit of National Armaments Director with representatives from Norway
23– 24 November 22	Visit Royal Institute of Technology (KTH) Sweden, Thun/Zurich
22 November 22	Visit of Federal Intelligence Service, Thun
22 November 22	Visit Swiss Federal Audit Office, Thun
10 November 22	Visit of the Security Policy Committee of the Council of States, Thun
11 November 22	Besuch Advanced Course in Engineering (ACE), Thun
8 November 22	8 November 22 Visit of Cyber Technical Course, Zurich
8 November 22	Visit of the "Fachstab" Cyber, Zurich
2 November 22	Visit to the Working Group on Information Security (AIS), Thun
31 October 22	Visit Cyber Training Course 22, Thun
22 September 22	Visit Air Force
7 September 22	Visit Lucerne University of Applied Sciences and Arts, Zurich
24 May 22	Visit of management of Swisstopo, Thun
23 May 22	Visit delegation GPS, Sweden, Thun
16 May 22	Visit Cyber Course 22, Thun

Technology and Market Monitoring Events

31 May 22 Startup Jam Session in Zurich

The CYD Campus hosted its first Cyber Security Startup Jam Session in Zurich, bringing together experts from armasuisse S+T, Swisscom, the ETH Entrepreneur Club as well as several student venture capital funds with entrepreneurs, students and cyber security experts. The aim of the initiative is to foster collaboration with the startup ecosystem in Switzerland and to drive the development of innovative technology solutions.

Student Exchange

On Tuesdays every two weeks, CYD students and interns report on the results of their research projects. In this context, all employees of the respective locations meet online to discuss the research work and findings.

Recruitment Platform Students

7 Oktober 22 EPFL Forum:

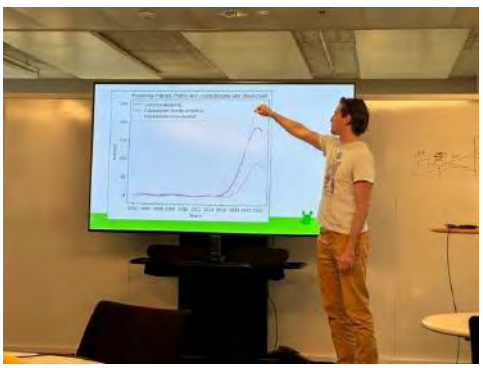
At this year's EPFL Forum, the CYD Campus was present to connect with students and give them insights into the activities of the CYD Campus, as well as to tell them about the various opportunities the CYD Campus offers to gain practical experience.

CYD Fellowship Workshop for applicants:

29 June 22

25 January 22

Visit Fachstab Cyber at the CYD Campus in Zurich. Fa



Student exchange in Lausanne.

13 Presentations

15 November 22	*Guest Lecture, Wireless Security (ETH): Wireless Security in Critical Transport Infrastructures*, Zurich, Dr Martin Strohmeier
2 November 22	*Seminar Applied Cryptography Group (ETH): Modern Jets, retro ciphers reloaded – The undead ciphers of ACARS*, Zurich, Dr Martin Strohmeier
26 October 22	*Securing the Future of (Dis-)Information*, CYD Campus Conference, Bern, Dr Raphael Meier
25 October 22	*How to: Cyber Security in Aviation, SWISS Airlines Management Colloquium*, Dr Martin Strohmeier
25 October 22	*Secure satellite communications and cyber security in space*, Hot Seat: Security Academy VBS, Dr Martin Strohmeier
16 September 22	*Plenary Talk*, CRITIS, Munich, Dr Bernhard Tellenbach
15 September 22	*High Data Throughput Exfiltration through Video Cable Emanation*, CRITIS, München, Llorenç Roma
23 August 22	*Does the Swiss army need a blockchain?* AFCSO, Bern, Dr Vincent Lenders
16 August 22	*AI and Fake News, Communication Cdo Op*, Dr Raphael Meier
1 July 22	*Presentation CYD Campus*, SIX Cyber Security Hub, Dr Vincent Lenders
22 June 22	*Keynote*, Swisscom Business Days, Crissier, Dr Vincent Lenders
17 June 22	*La 17ème journée franco-suisse sur la veille et l'intelligence économique*, Dr Alain Mermoud
2 June 22	*Cyber security in satellite communication*, CyCon, Tallinn, Dr Martin Strohmeier
31 May 22	*Presentation CYD Campus State Secretariat for Migration*, Dr Gérôme Bovet
20 May 22	*Guest Lecture, ADiT @ AFCSO*, Dr Raphael Meier
18 May 22	*GRPM Convention de sécurité*, Payerne, Dr Vincent Lenders
12 May 22	*Presentation CYD Campus*, Cyber security Seminar University of St. Gallen, Dr Vincent Lenders
10 May 22	GS-VBS Security Academy, Bern, Dr Vincent Lenders
6 May 22	*Cyber security in Aviation*, Swiss Aviation Safety and Operation Conference, Dr Martin Strohmeier
6 April 22	*Cyber Protection of Electrical Vehicles*, SCSD Fribourg, Dr Martin Strohmeier
25 March 22	*Trends in Aviation Cyber security*, Aviation Cyber Forum CAA London, Dr Martin Strohmeier
22 March 22	*Collaboration CYD Campus-EPFL*, KNOVA EPFL, Dr Vincent Lenders
18 March 22	*Guest lecture on disinformation*, University of St Gallen, Dr Hông-Ân Sandlin
16 March 22	*Presentation CYD Campus*, FITANIA, Dr Vincent Lenders
16 March 22	*Presentation CYD Campus*, armasuisse Command and Control + Reconnaissance Systems, Dr Vincent Lenders
2 March 22	*A View from the Cockpit: Exploring Pilot Reactions to Cyber attacks*, Deutsche Flugsicherung GmbH, Dr Martin Strohmeier
21 February 22	*CYD Campus*, Security Policy Committee SIK-S, Dr Vincent Lenders

Presentation by Raphael Meier on disinformation at the CYD Campus Conference in Bern.

Martin Strohmeier holds a presentation on cyber security in satellite communication at CyCon.

Presentation by Vincent Lenders about the CYD Campus.

14 Scientific Papers

14.1 Publications

December

DFAulted: Analyzing and Exploiting CPU Software Faults Caused by FPGA-Driven Undervolting Attacks
Dina G. Mahmoud, David Dervishi, Samah Hussein, Vincent Lenders and Mirjana Stojilović, IEEE Access Journal.

Early Guessing for Dialect Identification
Vani Kanjirangat, Tanja Samardzic, Fabio Rinaldi, and Ljiljana Dolamic, Conference on Empirical Methods in Natural Language Processing 2022, Abu Dhabi.

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. arXiv preprint arXiv:2212.07425.

November

A Methodology for Evaluating the Robustness of Anomaly Detectors to Adversarial Attacks in Industrial Scenarios
Ángel Luis Perales Gómez, Lorenzo Fernández Maimó , Félix J. García Clemente, Javier Alejandro Maroto Morales, Alberto Huertas Celdrán & Gérôme Bovet, IEEE Access Journal.

Measuring 5G Electric Fields Strength With Software Defined Radios
Franco Minucci, Dieter Verbruggen, Hazem Sallouah, Vladimir Volski, Guy Vandenbosch, Gérôme Bovet & Sofie Pollin, IEEE Open Journal of the Communications Society.

End-to-End Wireless Disruption of CCS EV Charging
Köhler, Sebastian, Richard Baker, Martin Strohmeier & Ivan Martinovic. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, pp. 3515-3517.

Beyond S-curves: Recurrent Neural Networks for Technology Forecasting
Alexander Glavackij, Dimitri Percia David, Alain Mermoud, Angelika Romanou & Karl Aberer. arXiv preprint arXiv:2211.15334.

October

Privacy-preserving and Syscall-based Intrusion Detection System for IoT Spectrum Sensors Affected by Data Falsification Attacks
Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Chao Feng, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, IEEE Internet of Things Journal.

RITUAL: a Platform Quantifying the Trustworthiness of Supervised Machine Learning
Alberto Huertas Celdrán, Jan Bauer, Melike Demirci, Joel Leupp, Muriel Figueredo Franco, Pedro M. Sánchez Sánchez, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, 18th International Conference on Network and Service Management (CNSM), Thessaloniki, Greece.

SpecForce: A Framework to Secure IoT Spectrum Sensors in the Internet of Battlefield Things Series Military Communications and Networks
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet & Gregorio Martínez Pérez, IEEE Communications Magazine.

TechRank
Anita Mezzetti, Loïc Maréchal, Dimitri Percia David, William Lacube, Sébastien Gillard, Michael Tsesmelis, Thomas Maillart & Alain Mermoud, A. arXiv preprint arXiv:2210.07824.

September

RITUAL: A Platform Quantifying the Trustworthiness of Supervised Machine Learning

Alberto Huertas Celdran, Jan Bauer, Melike Demirci, Joel Leupp, Muriel Figueredo Franco, Pedro M. Sanchez Sanchez, Gérôme Bovet, Gregorio Martinez Perez, Burkhard Stiller, International Conference on Network and Service Management (CNSM 2022).

High Data Throughput Exfiltration through Video Cable Emanations,

Llorenç Romá, Daniel Moser and Vincent Lenders, International Conference on Critical Information Infrastructures Security (CRITIS), München, Deutschland.

A Secure Framework for Distributed Privacy-Preserving Threat Intelligence Sharing

J. R. Trocoso-Pastoriza, A. Mermoud, R. Bouyé, F. Marino, J.-P. Bossuat, V. Lenders and J.-P. Hubaux, arXiv.

OpenSky Report 2022: Evaluating Aviation Emissions Using Crowdsourced Open Flight Data

J. Sun, L. Basora, X. Olive, M. Strohmeier, M. Schäfer, I. Martinovic and V. Lenders, DASC 2022.

Studying the Robustness of Anti-Adversarial Federated Learning Models Detecting Cyberattacks in IoT Spectrum Sensors

Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Timo Schenk, Adrian Lars Benjamin Iten, Gérôme Bovet, Gregorio Martínez Pérez, Burkhard Stiller, IEEE Transactions on Dependable and Secure Computing.

Building collaborative cybersecurity for critical infrastructure protection

Jollès, Eric; Gillard, Sébastien; Percia David, Dimitri; Strohmeier, Martin & Mermoud, Alain. In Critical Information Infrastructures Security: 17th International Conference, CRITIS 2022, Springer. München, Germany.

Identifying Emerging Technologies and Leading Companies using Network Dynamics of Patent Clusters: a Cybersecurity Case Study

Michael Tsesmelis, Ljiljana Dolamic, Marcus Matthias Keupp, Dimitri Percia David & Alain Mermoud. arXiv preprint arXiv:2209.10224.

August

SAFEAMC: Adversarial Training for Robust Modulation Classification Models

Javier Maroto, Gérôme Bovet, Pascal Frossard, EUSIPCO 2022, Belgrade, Serbia.

Aggregate-based Congestion Control for Pulse-Wave DDoS Defense

Albert Gran Alcoz, Martin Strohmeier, Vincent Lenders & Laurent Vanbever, ACM SIGCOMM, Amsterdam, Netherlands.

Building an Avionics Laboratory for Cybersecurity Testing

Martin Strohmeier, Giorgio Tresoldi, Leeloo Granger & Vincent Lenders, 15th ACM Workshop on Cyber Security Experimentation and Test (CSET).

An Experimental Study of GPS Spoofing and Takeover Attacks on UAVs

Harshad Sathaye, Martin Strohmeier, Vincent Lenders & Aanjhan Ranganathan, 31st USENIX Security Symposium (USENIX Security), Boston, MA, USA.

July

Intelligent and behavioral-based detection of malware in IoT spectrum sensors

Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Miguel Azorín Castillo, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, International Journal of Information Security.

Communicating via Markov Decision Processes

Samuel Sokota, Christian A. Schroeder De Witt, Maximilian Igl, Luisa M. Zintgraf, Philip Torr, Martin Strohmeier, Zico Kolter, Shimon Whiteso, Jakob Foerster, Proceedings of the 39th International Conference on Machine Learning (ICML).

June

Needle In A Haystack, Fast: Benchmarking Image Perceptual Similarity Metrics At Scale

Cyril Vallez, Andrei Kucharavy & Ljiljana Dolamic, arXiv:2206.00282v1.

Investigating Graph Embedding Methods for Cross-Platform Binary Code Similarity Detection

Victor Cochard, Damian Pfammatter, Chi Thang Duong & Mathias Humbert, IEEE European Symposium on Security and Privacy (Euro S&P).

Efficient Collective Action for Tackling Time-Critical Cybersecurity Threats

Sébastien Gillard, Dimitri Percia David, Alain Mermoud & Thomas Maillart, 21st Workshop on the Economics of Information Security (WEIS), Tulsa, USA.

On the Security of the FLARM Collision Warning System

Boya Wang, Giorgio Tresoldi, Martin Strohmeier & Vincent Lenders, 17th ACM ASIA Conference on Computer and Communications Security (ASIACCS), Nagasaki, Japan.

Security and Privacy Issues of Satellite Communication in the Aviation Domain

Georg Baselt, Martin Strohmeier, James Pavur, Vincent Lenders & Ivan Martinovic, 14th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia.

An ML and Behavior Fingerprinting-based Framework for Cyberattack Detection in IoT Crowdsensing

Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, VII Jornadas Nacionales de Investigación en Ciberseguridad, Bilbao, Spain.

May

Early Warning Signals in Open Source Intelligence: Two Use Cases of the 2019 Iraqi and 2020 Indian Farmers' Protests

Étienne Voutaz & Albert Blarer, Computing and Informatics.

Block-sparse Adversarial Attack to fool Transformer-based Text Classifiers

Sahar Sadrizadeh, Ljiljana Dolamic & Pascal Frossard, International Conference on Acoustics Speech and Signal Processing (ICASSP).

Intelligent Fingerprinting to Detect Data Leakage Attacks on Spectrum Sensors
Alberto Huertas Celdran, Pedro M. Sanchez Sanchez, Gérôme Bovet, Gregorio Martinez Perez & Burkhard Stiller, IEEE International Conference on Communications.

Evolutionary Optimization of Residual Neural Network Architectures for Modulation Classification
Erma Perenda, Sreeraj Rajendran, Gérôme Bovet & Sofie Pollin, Mariya Zheleva, IEEE Transactions on Cognitive Communications and Networking.

April

Policy-based and Behavioral Framework to Detect Ransomware Affecting Resource-constrained Sensors
Alberto Huertas Celdran, Pedro M. Sanchez Sanchez, Eder J. Scheid, Timucin Besken, Gérôme Bovet, Gregorio Martinez Perez & Burkhard Stiller, IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary.

ditto: WAN Traffic Obfuscation at Line Rate
Roland Meier, Vincent Lenders & Laurent Vanbever, 29th Network and Distributed System Security Symposium (NDSS), San Diego, California, USA.

March

FPGA-to-CPU Undervolting Attacks
Dina G. Mahmoud, Samah Hussein, Vincent Lenders & Mirjana Stojilovic, Design Automation and Test in Europe Conference, Antwerp, Belgium.

Creation of a Dataset Modeling the Behavior of Malware Affecting the Confidentiality of Data Managed by IoT Devices
Alberto Huertas Celdran, Pedro M. Sanchez Sanchez, Fabio Sisi, Gérôme Bovet, Gregorio Martinez Perez, Burkhard Stiller, Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities.

February

Understanding Realistic Attacks on Airborne Collision Avoidance Systems
Matthew Smith, Martin Strohmeier, Vincent Lenders & Ivan Martinovic, Journal of Transportation Security (JTRS).

Federated learning for malware detection in IoT devices
Valerian Rey, Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán & Gérôme Bovet, Computer Networks.

January

Electrical-Level Attacks on CPUs, FPGAs, and GPUs: Survey and Implications in the Heterogeneous Era
Dina G. Mahmoud, Vincent Lenders & Mirjana Stojilovic, ACM Computing Surveys (CSUR), Volume 55, Issue 3.

Cybersecurity Technologies: An Overview of Trends and Activities in Switzerland and Abroad
Michael Tsesmelis, Dimitri Percia David, Thomas Maillart, Ljiljana Dolamic, and Giorgio Tresoldi, William Lacube, Colin Barschel, Quentin Ladetto and Claudia Schärer, Vincent Lenders, Kilian Cuche & Alain Mermoud. Available at SSRN: https://ssrn.com/abstract=4013762 or http://dx.doi.org/10.2139/ssrn.4013762.

14.2 Student Works

CYD Fellows

Postdoc

Dr **Lucianna Kiffer**	*Security and Usability of Blockchain Networks*	ETH Zurich
Dr **Andrei Kucharavy**	*Evolutionary Dynamics for Improved GAN Detection*	EPFL
Dr **Dimitri Percia David**	*Technology Forecasting and Market Monitoring for Cyber-Defence*	University of Geneva

PhD

Louis-Henri Merino	Coercion-Resistant Remote E-Voting Systems with Everlasting Privacy	ETH Zurich
Alessandro Stolfo	Privacy-Preserving Learning of Neural Language Models	ETH Zurich
Simran Tinani	Nonabelian Groups in Cryptography	University of Zurich
Dina Mahmoud	ADHeS: Attacks and Defenses on FPGA-CPU Heterogeneous Systems	EPFL

Master

Jodok Vieli	*Systemization of DNS DoS: Attack Characterization, Mitigation, and Measurement*	ETH Zurich
Ian Boschung	*Analysing new security guarantees made possible by the ARMv9 Confidential Compute Architecture*	ETH Zurich
Jonsson Adalsteinn	*PE Malware Detection with Deep Neural Model*	ETH Zurich
Lina Gehri	*Analyzing and Comparing Defense Strategies in a Cyber Defense Exercise*	ETH Zurich
Jan Urech	*Developing an Automaten Defender for Cyber Security Exercises*	ETH Zurich
Ksandros Apostoli	*Privacy-Preserving Proof-of-Personhood Token*	EPFL

Students and

Pedro Miguel Sanchez Sanchez	Identical IoT device identification via hardware fingerprinting	PhD, University of Murcia
Enrique Tomás Martínez Beltrán	Training AI models in a privacy-preserving and decentralized fashion	PhD, University of Murcia
Yago Lizarribar	Localization of Non-Cooperative Transmitters with Low-Cost Crowdsourced Spectrum Sensing Networks	PhD IMDEA Networks Institute
Florian Lerch	Adversarial Attacks on Sensors and ML Systems	Master Thesis ETH Zurich
Beatrice Dall'Omo	Evaluation of Practical Attacks on Drone Monitoring Device	Master Thesis EURECOM
Guillaume Follonier	Improved OCR of Image With Text Memes	Master Thesis EPFL
François Burguet	The new risk and return of venture capital: Empirical study on Crunchbase data	Master Thesis EPFL
Marco di Nardo	Symbolic Modelling of libc Functions and Application to Concolic Execution	Semester Thesis ETH Zurich
Alexander Glavacki	Towards a General Model for Technology Forecasting: An RNN Model for Scientometrics Using ArXiv Data	Project work
Eloi Garandel	Detection and Prediction of the emergence and trend of cybersecurity technologies hosted on GitHub,	Project work
Eric Jollès	Building Collaborative Cybersecurity for Critical Infrastructure Protection: Empirical Evidence of Collective Intelligence Information-Sharing Dynamics on ThreatFox	Project work

Jacques Roitel	Towards a Technology Convergence Index for Information Technologies: A Keyword Extraction Approach Applied to ArXiv	Project work
Johannes Willbold	SKYFALL: Exploring Novel and Neglected Attacks on Modern VSAT Systems through Service Networks	Project work
Samad Emrys Darussel	Analysis of Lag in Security Research: An exploration of ArXiv Open Data	Project work
Sarah Ismail	Forecasting Trends Using Wikipedia Pageview Statistics: The Case of Data Protection and Encryption Technologies	Project work
Cyril Vallez	Needle in a Haystack, Fast: Benchmarking Image Perceptual Similarity Metrics At Scale	Project work
Eric Jedermann	Spot on! User Location Privacy Attacks on LEO Satellite Communication	Project work
Huzar Marin	Evaluation methods for network intrusion detection and response system	Project work
Alessandro Tavazzi	Measuring Technological Convergence in Encryption Technologies with Proximity Indices: A Text Mining and Bibliometric Analysis using OpenAlex	Project work

15 Communication

@Cyber-Defence Campus

@cydcampus

Web Communications

- 11.11.2022, DDPS tests SCION network for Swiss cyber defence
- 26.10.2022, Meet the finalists of the Cyber Startup Challenge 2022
- 30.09.2022, CYD Campus hackathon on industrial control systems
- 29.09.2022, Machine learning for more security in electricity grids
- 01.09.2022, Strengthening collective cyber resilience
- 02.08.2022, New Cyber Avionics Lab
- 23.06.2022, First Startup Jam Session at the Cyber-Defence Campus
- 20.06.2022, Call for the Cyber Startup Challenge 2022
- 07.02.2022, The Cyber-Defence Campus publishes its Annual Report 2021

Press Releases

- 26.10.2022, «Cyber Startup Challenge 2022»: Startup ONEKEY convinces the DDPS

armasuisse Print

- December issue, Representation from the Cyber-Defence Campus at the Cooperative Cyber Defence Centre of Excellence in Estonia strengthens cooperation between Switzerland and NATO (in German)
- Issue 2022, Research brochure armasuisse Science and Technology (in German)

Videos

- 22.06.2022, EPFL/Cyber Defence Campus collaboration
- Digitalisation, Innovation & Security in the DDPS, Focus armasuisse

16 Outlook 2023

For the coming year, the CYD Campus will continue to expand its cooperation with universities and the industry, especially in the areas of digitalisation, artificial intelligence and innovation. In these three areas, the DDPS, but also the entire federal government, is facing technological challenges. Finally, the following development steps and planned activities of the CYD Campus, which are to be implemented in 2023 in accordance with the Cyber DDPS strategy, are worth highlighting:

The additional security policy report which was published in 2022 explains why the international cooperation has become even more pressing for Switzerland as a result of the war in Ukraine. The CYD Campus will also make a significant contribution in 2023 to intensified international cooperation in the area of cyber defence and further develop the relationship with NATO, among other things.

A new CYD Fellowship for Proof of Concepts aims to promote the innovative capacity of young cyber talents in Switzerland from 2023 and better integrate them in the innovation processes of the DDPS. It also serves to develop entrepreneurial thinking and action.

As every year, we are planning to hold a conference and cyber events. The 2023 CYD Campus Conference will be held on 26 October 2023 in the Kursaal in Bern. We are looking forward to welcoming more than 300 cyber experts as well as interested parties to this event. Hackathons on the security of cars and critical infrastructures are also planned.

As a measure of national strategy to protect Switzerland from cyber risks (NCS2), development of an automated technology radar (TMM 2.0) is to be accelerated. This instrument uses existing databases, websites and directories to recognise trends and technologies early on and to estimate their significance for Switzerland. The tool will also be used to support the scouting and monitoring activities of the CYD Campus, as well as to better monitor Switzerland's Security-relevant Technology and Industry Base (STIB).

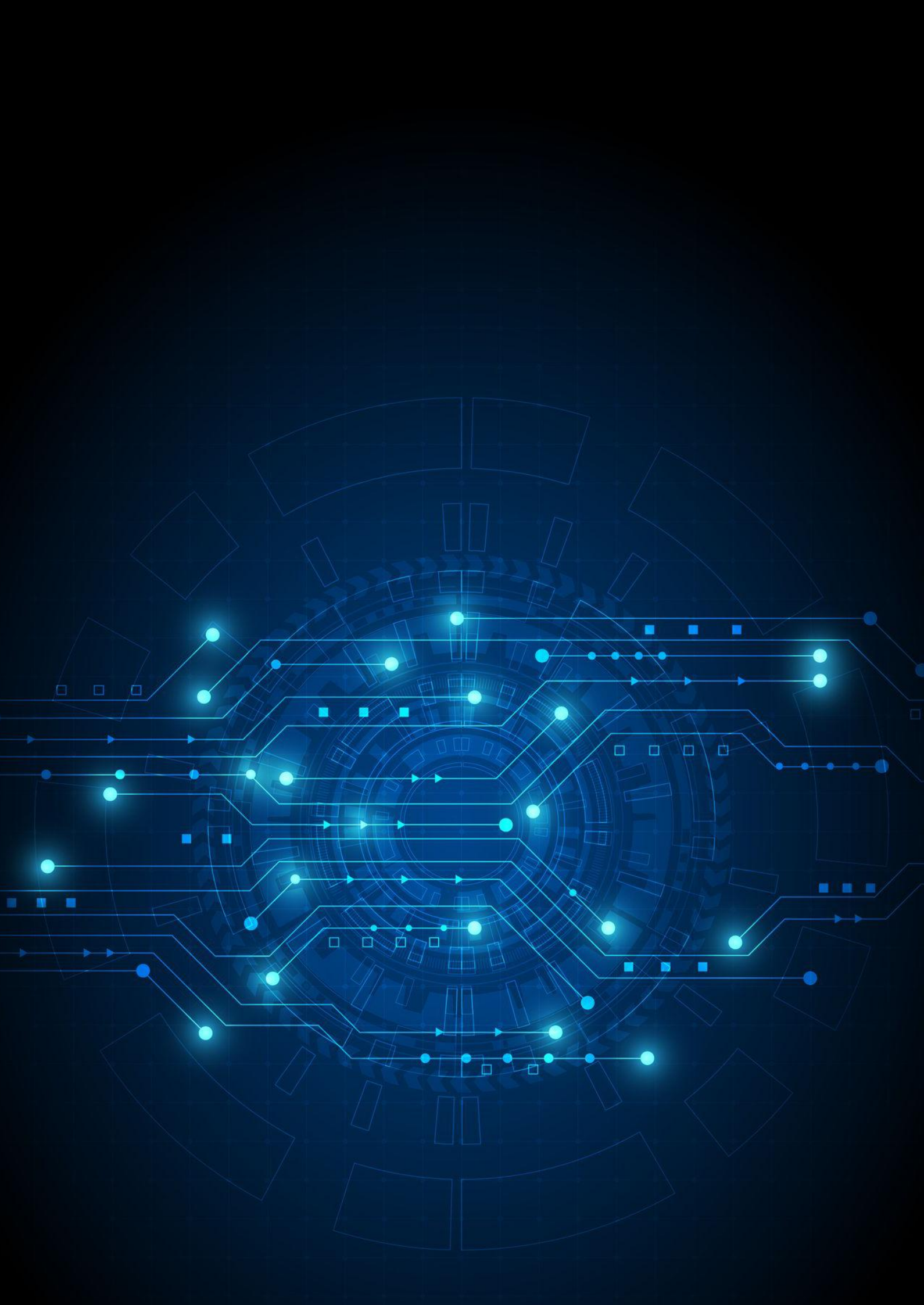
The Space Campus will create a new platform for the space community, which will promote the research projects and talents in this area as well as business opportunities. The CYD Campus will host the Space Campus in Lausanne and strengthen Swiss innovation in space.

In 2023, we aim to further intensify the cooperation with the Cyber Battalion 42. The Battalion commenced service at the start of 2022 and consists of members of the Armed Forces who possess important expertise in the IT and cyber security area based on their civilian activities. It will become an important component of the Cyber Command, which is under development and which will emerge from the current Armed Forces Command Support Organisation (AFCSO). By involving these experts in specific projects, both the CYD Campus as well as the Cyber Bat 42 will benefit from valuable synergies.

Once again in 2023, we want to generate a significant added value for both the Swiss and the international cyber defence landscape, with key projects in focal issues such as the robustness of artificial intelligence and the security of 5G and/or IoT security.

In early 2023, a new website will be released which will offer the cyber defence community more content and current news, such as information on our research projects and events. This will enable us to be more agile in interacting and communicating with the cyber community in the face of the ever-changing technology and threat environment.

In addition, we will continuously check how we want to expand our offer for the upcoming cyber command and the new Federal Office for Cyber Security, for example in the areas of innovation and cyber training.



Contact us

Cyber-Defence Campus

Feuerwerkerstrasse 39

CH-3602 Thun

Zollstrasse 62

CH-8005 Zürich

EPFL Innovation Park, Bâtiment I

CH-1015 Lausanne

cydcampus@armasuisse.ch

+41 58 480 59 34