Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Science and technology

Cyber-Defence Campus

Annual Report 2021

Contents

IMPRINT

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

As in the previous year, 2021 was strongly influenced by the COVID-19 pandemic. Besides the negative effects such as the overburdening of the healthcare system and increased government spending, the pandemic has also led to a rapid acceleration of digitalization. As a result, the importance and complexity of cyber threats have risen considerably, with increasing critical implications for the security of our society.

Every day, our employees and partners of the Cyber Defence (CYD) Campus make an important contribution to Switzerland's cyber security by engaging in research, innovation, knowledge transfer or talent training. Since its foundation three years ago, several strategic objectives of the Cyberdefence Action Plan, the Cyber DDPS Strategy and the National Strategy for the Protection of Switzerland against Cyber Risks (NCS) have been implemented at the CYD Campus. In 2021, significant progress and results have been achieved particularly in the following areas.

Systematic scouting of new technologies and startups has been extended to six additional countries. To complement the already established technology and market monitoring in Switzerland, the United States and Singapore, cyber developments and trends in the United Kingdom, Germany, Austria, France, Israel and Estonia are now being actively monitored with an international partner network. Recent developments from these regions are now analyzed at an early stage and examined within the framework of studies and proof-of-concepts with the relevant federal agencies. Last year alone, a dozen proof-of-concepts were realized with stakeholders. For instance, an innovative software of a startup was implemented on the first pilot project of the Army's pre-service cyber training by the CYD Campus.

Research cooperation with universities such as ETH Zurich, EPF Lausanne, ZHAW or the University of Lausanne was further developed and extended in line with the needs of the Swiss defense to new fields of technology such as post-quantum cryptography, the combating of disinformation or the protection of critical infrastructures. Moreover, the Swiss cyberdefense community was cultivated and further expanded through our events such as the lunch seminars, the hackathons, the conferences or this year's Cyber Startup Challenge. Furthermore, I am very pleased that this year ten students from Swiss universities were able to conduct their research as a CYD Fellow and another 35 students completed a university internship or a master's thesis at the CYD Campus as part of the talent development program.

This annual report provides information about the public, unclassified activities of the CYD Campus in 2021.

I hope you will enjoy reading it.

Thun, December 31, 2021

Dr. Vincent Lenders
Head of the Cyber-Defence Campus

1 About Cyber-Defence Campus

1.1 Strategy Embedding and Key Tasks

Due to the changing ecosystem and the increasing threat of cyberattacks in all spheres of life, the Swiss government has made cybersecurity 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 Cyberdefence (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 within the DDPS for three years. It is part of the Federal Office for Defence Procurement (armasuisse). The CYD Campus provides the DDPS with an anticipation and knowledge platform for identifying and assessing technological, economic and societal cyber trends. In order to be able to cooperate to the greatest extent possible with the universities, the DDPS and industry, the CYD Campus is located at three sites: At its main site in Thun (armasuisse Science and Technology), at EPF Lausanne and at ETH Zurich. This allows it to efficiently build know-how and provide cyber expertise, according to the needs of the Swiss Confederation. The CYD Campus therefore acts as a nexus between the private sector, the public sector and the academic community.

In the orientation of the "Cyber DDPS Strategy", the Head of DDPS, Federal Councillor Viola Amherd, defines the fields of action and the corresponding distribution of tasks. The CYD Campus has the following three key tasks today:

Core competencies of the Cyber-Defence Campus

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.

The aim of this annual report is to provide insights into the realization of the above-mentioned tasks in 2021 of the Cyber-Defence Campus. In doing so, a brief summary of some highlights of 2021 will be provided. Public activities in research projects, customer mandates and demonstrators will also be discussed. Furthermore, activities in 2021 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 2022.

1.2 Partners

The CYD Campus is organizationally located at armasuisse Science and Technology (DDPS). About 50 other national and international organizations from academia, industry and the public sector contribute as partners.

Public Partners/Federation

- Swiss Army
- Federal intelligence service NDB
- Federal Office of Police fedpol
- Federal Statistical Office FSO
- Swisstopo
- National Cyber Security Center NCSC
- Federal Office of Civil Aviation FOCA
- NATO CCDCoE
- US Air Force Research Lab
- US Army Research Lab
- Luxembourg Army
- European Defence Agency EDA
- Federal Office for Information Security (BSI), DE
- Swissnex

Higher Education

- EPF Lausanne
- Center for Digital Trust (C4DT)
- ETH Zurich
- Zurich Information Security and
- Privacy Center (ZISC)
- Military Academy at the ETH Zurich
- University of Fribourg
- University of Zurich
- University of Lausanne
- University of Neuchâtel
- University of Oxford, UK
- KU Leuven, BEL
- IMDEA, ESP
- University of Murcia, ESP
- University Rey Juan Carlos, ESP
- TU Kaiserslautern, DE
- ZHAW
- FHNW
- IDSIA
- Northeastern University, USA
- HEIG-VD
- University of Geneva
- HEVS
- HEPIA

Industrial Partners

- Kudelski Security
- IBM Research
- Noser Engineering
- Ad Novum
- Astrocast
- Swisscom
- CounterCraft
- Tune Insight
- Cysec
- Plug and Play
- Anapaya
- RUAG
- Decentriq

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
Head of the CYD Campus
and Head of department

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

Dr. Gérôme Bovet
Head of Research Program
and Data Science Group

Dr. Colin Barschel
Head of Innovation and
Industry Collaborations

Giorgio Tresoldi
Head of international Relations
and Scouting

Dr. Alain Mermoud
Head of Technology and
Market Monitoring

Monia Khelifi
Assistance Management

Personnel Focus Cybersecurity

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 pentester, vulnerability researcher and scientific project manager

Llorenç Roma is a pentester and scientific project manager (joined April 2021)

Dr. **Daniel Moser** is an expert in critical infrastructure security and wireless communications as well as a scientific project manager

Dr. **Miguel Keer** is a a scientific project manager

Dr. **Luca Gambazzi** is security auditor and scientific project manager (resigned August 21)

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

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

Personnel Focus Data Science

Dr. **Gérôme Bovet** is the Head of the Data Science group and Research Program Manager

Dr. **Etienne Voutaz** is Data Scientist and scientific project manager

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

Dr. **Albert Blarer** is Data Scientist and scientific project manager

Dr. **Metin Feridun** is a Big Data specialist and scientific project manager

Dr. **Mathias Humbert** is an expert in Machine Learning and Privacy as well as a scientific project manager (resigned November 21)

Dr. **Raphael Meier** is an expert for Image Processing and Machine Learning as well as a scientific project manager (joined May 21)

Thomas Sigrist is responsible for computing infrastructures and technical project manager (resigned December 21)

Ivo Stragiotti is responsible for laboratory infrastructures and technical project manager (joined July 21)

University Interns

In order to increase students' cyber expertise and strengthen Switzerland's long-term resilience against cyber threats, the Cyber-Defence Campus offers university internships at all three locations in Thun, Lausanne and Zurich. In 2021, 24 students were able to complete an internship with the Cyber-Defence Campus. The interns come from different universities such as EPF Lausanne, ETH Zurich or the University of St. Gallen.

Huzar Marin, September 21 - February 22, Cybersecurity, Lausanne

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

Benjamin Kilian, September 21 - February 22, Cybersecurity, Lausanne

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

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

Michael Tsesmelis, June 21 - May 22, Technology and Market Monitoring, Lausanne

Mathilde Raynal, May 21 - Oktober 21, Data Science, Lausanne

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

William Lacube, March 21 - Dezember 21, Technology and Market Monitoring, Lausanne

Valentyna Pavliv, March 21 - August 21, Data Science, Lausanne

Eric Jolles, March 21 - December 21, Technology and Market Monitoring, Lausanne

Victor Cochard, March 21 - August 21, Data Science, Lausanne

Caroline Violot, February 21 - July 21, Data Science, Lausanne

Anton Santiago Moreno, February 21 - July 21, Technology and Market Monitoring, Lausanne

Valérian Rey, October 20 - March 21, Data Science, Lausanne

Marc Kaufmann, October 20 - June 21, Data Science, Zürich

Stéphanie Lebrun, October 20 - March 21, Data Science, Lausanne

Etienne Bonvin, October 20 - March 21, Data Science, Lausanne

Adrien Prost, October 20 - March 21, Data Science, Lausanne

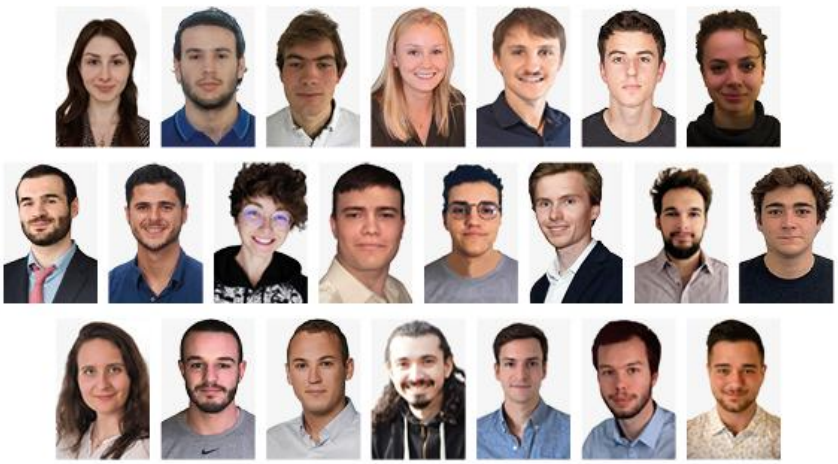
Benno Schneeberger, September 20 - February 21, Cyber Security, Lausanne

Ejub Talovic, September 20 - February 21, Technology and Market Monitoring, Lausanne

Edoardo Debenedetti, August 20 - January 21, Data Science, Lausanne

Robin Leurent, August 20 - January 21, Data Science, Lausanne

Llorenç Roma, April 20 - March 21, Cybersecurity, Thun



CYD Fellows

In 2020, the CYD Campus launched a Cyber Defence (CYD) Fellowship Program together with EPF Lausanne to give students the opportunity to deepen their knowledge in cyber defence topics and to strengthen Swiss competences in the field of cyber defence. This enables students to make a research contribution to Switzerland's cyber defense while they are still studying. The CYD Fellowships are a competitive talent program that provides students with a CYD Campus expert for the supervision of their research work. CYD Fellows are enrolled at a Swiss university and conduct their research in the CYD Campus premises at EPF Lausanne, ETH Zurich and at the headquarters in Thun. CYD Fellowships are awarded several times a year to master students, PhD students and postdocs and provide a living allowance. In 2021, ten fellows were active:

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

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

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

Louis Merlin, Master Thesis Fellow, EPFL, March - August 21, Project title: *Recovering type information from compiled binaries to aid in instrumentation*, CYD Mentor: Damian Pfammatter

Anita Mezzetti, Master Thesis Fellow, EPFL, February - July 21, Project title: *Modelling portfolios of cyber-related emerging technologies: a complex-system approach*, CYD Mentor: Dr. Alain Mermoud

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

Zuowen Wang, Master Thesis Fellow, ETHZ, September 20 - February 21, Project title: *Understanding and enhancing adversarial robustness for machine learning models*, CYD Mentor: Dr. Gérôme Bovet

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 2021, work from eleven students was supervised by the CYD Campus.

Pedro Miguel Sanchez, University of Murcia, September 21 - December 21, Supervisor: Dr. Gérôme Bovet

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

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

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

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

Philippe Panhaleux, ETHZ, March 21 - August 21, Supervisor: Dr. Martin Strohmeier

Julian Huwyler, ETHZ, March 21 - August 21, Supervisor: Dr. Martin Strohmeier

Leeloo Granger, ETHZ, March 21 - August 21, Supervisor: Dr. Martin Strohmeier

Jannik Brun, ETHZ, March 21 - August 21, Supervisor: Dr. Martin Strohmeier

Michael Karpf, ETHZ, March 21 - August 21, Supervisor: Dr. Martin Strohmeier

Georg Baselt, ETHZ, February 21 - July 21, Supervisor: Dr. Martin Strohmeier

2 Highlights

Car Hackathon

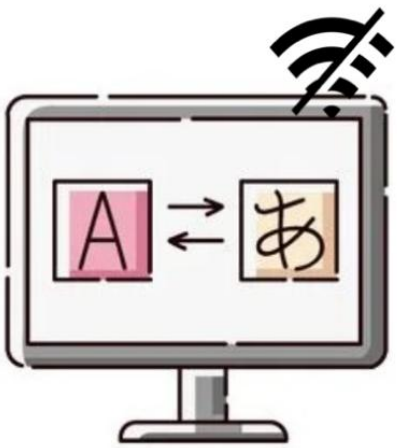
Cars are becoming increasingly intelligent. While the new functions bring more comfort and safety, they also create numerous cyber security vulnerabilities. These are not only in potentially critical systems such as brakes, engine, etc., but also in components that are accessible from the outside, such as the wireless interfaces of the multimedia system. The hazardous situation is exacerbated by the introduction of electric cars, as all systems are usually connected to a single bus system. The charging infrastructure of these vehicles raises further reliability and safety issues (charging station failure, charging station-car data exchange, etc.). The increasing number of sensors such as radar, lidar, cameras and their dependence on artificial intelligence to analyze the large amount of data they generate also create new vulnerabilities.

In order to quickly increase the relevant expertise at the CYD Campus and in the federal administration, a hackathon was held in Thun during five days in October 2021. A total of 20 participants from ETH Zurich, the University of Oxford, fedpol, the Swiss Armed Forces and armasuisse, with the support of experts from the Japanese company White Motion, uncovered potential security problems of seven different vehicles (different manufacturers, military / civilian, electric / non-electric) and took the first steps in this research area. The composition of the participants allowed an interdisciplinary exchange as well as an intensive and fruitful work. In addition, it was possible to put together several demonstrators that will be used in the CYD Campus. In addition, data was collected that will flow into the joint CYD Campus research with the universities in the coming years.

Training with experts and vulnerability check during the Car Hackathon in Thun

Offline Translation Service in the Armed Forces

Nowadays, numerous automatic translation programs are available online. They offer the possibility to translate between a variety of languages, with the quality of the translation varying, depending on the tool itself and the underlying languages. However, online translation services have led to numerous security issues, as content containing personal or confidential data could be leaked. As part of an innovation project, a proof-of-concept of an internal, offline machine translation tool capable of providing comprehensible bidirectional translations between English and six other languages was realized. Using German, French, Italian, Russian, Arabic, and Chinese as source and target languages, the feasibility of this tool was demonstrated for use in military systems, regardless of the underlying language complexity or writing system.



Dr Mathias Humbert becomes Professor for Cybersecurity at the University of Lausanne

Dr. Mathias Humbert, a research associate at CYD Campus, has been promoted to professor at the University of Lausanne in November 2021. During his two years at CYD Campus, Mathias Humbert has supervised numerous student projects, thus gaining important experience for this new challenge. As a professor at the University of Lausanne, he will further promote the long-term collaboration between CYD Campus and his department in the field of cybersecurity and data protection. For the CYD Campus, it is a key strategic goal to develop cyber talent with a view to Switzerland's security.

Security Vulnerabilities found in VPN Software

As part of the Vulnerability Research Program, VPN software solutions from various manufacturers were tested for vulnerabilities. Among other things, a CYD Campus researcher discovered a critical vulnerability in the VPN client of the American company F5. The previously unknown vulnerability could be exploited by unauthorized users to gain administrator rights on those Windows client systems on which the VPN software was installed. The VPN software is used by numerous Swiss companies to allow employees remote access to their own company network. Due to the Covid-19 pandemic and the associated home office obligation, the use of VPN clients became a common practice. Thanks to CYD Campus' early notice to the manufacturer in February 2021, the security gap was closed. On June 1, 2021, the corresponding security update was released. This highlight illustrates the relevance and effectiveness of the CYD Campus' vulnerability research for Switzerland's security.

CYD Campus Conference and CRITIS

On September 28, 2021, the CYD Campus conference took place at the EPFL SwissTech Convention Center in Lausanne and was simultaneously broadcasted online due to the ongoing pandemic. The conference welcomed 130 participants on-site and another 80 participants followed the event online. Experts from academia, government and industry gave presentations on key topics related to the security of critical information infrastructures. The event provided a platform for exchange on current and future challenges and drivers in cyberspace. In the afternoon, following the pitches of the three finalists of the Cyber Startup Challenge, the Zurich-based company Decentriq was selected as the winning startup. The conference was held in collaboration with the 16th International Conference on Critical Information Infrastructure Security (CRITIS 2021), which was held at the same site on September 27-29.

Conference program – CRITIS 2021

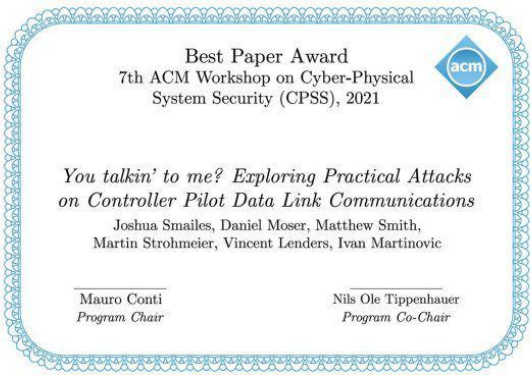
Participants of the CYD Campus conference & CRITIS 2021 in Lausanne

CYD Campus Awards

Best Paper Award at the Cyber-Physical System Security Workshop

Three CYD Campus researchers, along with researchers from the University of Oxford, received the Best Paper Award at the 7th ACM Cyber-Physical System Security (CPSS) Workshop. In their research, the scientists demonstrated that an attacker can pretend to be a legitimate air traffic controller by capturing the link between air traffic controllers and the aircraft crew, and then give false instructions to the target aircraft. The vulnerability is said to pose a significant safety risk to aircraft. They also developed three countermeasures to address these airspace safety risks. These range from plausibility checks and alerting to the use of message signatures or encryption.

To the publication


Best Paper Award
7th ACM Workshop on Cyber-Physical System Security (CPSS), 2021

You talkin' to me? Exploring Practical Attacks on Controller Pilot Data Link Communications

Joshua Smailes, Daniel Moser, Matthew Smith, Martin Strohmeier, Vincent Lenders, Ivan Martinovic

Mauro Conti, *Program Chair*

Nils Ole Tippenhauer, *Program Co-Chair*

Best Paper Award received from ACM

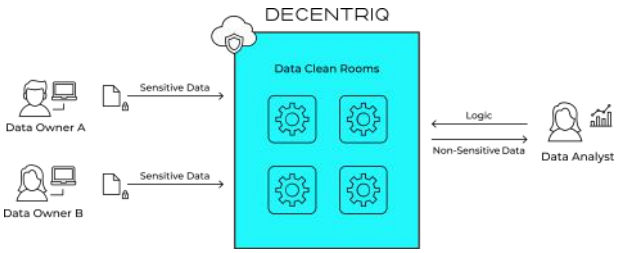
Stéphanie Lebrun presenting her work at CRITIS 2021, which was honored with the Young CRITIS Award

Young CRITIS Awards

As part of CRITIS 2021, the Young CRITS Award was granted to encourage and support young scientists conducting research in the field of critical infrastructure protection. CRITIS 2021 honored the best work of three young scientists. Santiago Anton Moreno and Stéphanie Lebrun, both CYD Campus university interns, were placed second and third, and received a total of 1500 Swiss francs for their work. Santiago Anton Moreno developed models on how to assess the cybersecurity market and technologies to facilitate investment decisions to ensure the security of critical infrastructure. Stéphanie Lebrun's work focused on the security of GNSS infrastructures.

Cyber Startup Challenge

The Cyber Startup Challenge 2021 aimed to discover the startup technology landscape around the topic of "Strengthen Your Information Sharing and Analysis Center (ISAC)" and searched for innovative solutions in the field of cyber threat intelligence with a focus on critical infrastructure protection. 38 startups from Europe, the US and Asia participated in the challenge. The jury, consisting of cyber experts from the DDPS and armasuisse S+T, selected the three finalists Decentriq, Constella Intelligence and Pandora Intelligence, who held a pitch at the CYD Campus conference on September 28, 2021. The Zurich-based startup Decentriq finally convinced the jury with its innovative Software-as-a-Service (SaaS) platform offering "Data Clean Rooms" for enterprises.The technology allows both internal and external critical infrastructure stakeholders to securely share cyber data and gain aggregated and anonymous insights. This enhances their cybersecurity without compromising data confidentiality. Decentriq will now work with the CYD Campus to integrate a proof-of-concept of its technology in a real-world DDPS environment in 2022.



Solution approach from DECENTRIQ, winner of the Cyber Startup Challenge 2021

3 CYD Talent Development

Specialists in cybersecurity 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. In order to enhance the cyber expertise of students, the CYD Campus pursues different approaches.

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

In 2021, 24 university interns were employed and eleven student projects were supervised by CYD Campus scientists. In addition, ten CYD Fellows were active.

The aim is to foster this way a new generation of cyber talents. Thus, the CYD Campus makes a substantial contribution to combating the shortage of skilled workers in the highly specialized cyber field with the long-term aim of ensuring the necessary cyber competencies for government, science and industry in Switzerland.

Some CYD Fellows in Lausanne

University intern during her cyber training at CYD Campus Lausanne

4 Research

The CYD Campus research is an a long-term investment in securing the required expert knowledge and scientific-technical competencies for the tasks and activities of the Confederation in the field of cyberdefence. As an integral part of the 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 future required operational cyberdefence capabilities and 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 Projects in Cybersecurity

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 goal 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 the user experience. Two approaches are pursued to protect the sensitive data: The first approach consists of the compartmentalization of risks. This means that the area of attack on the system is nested to minimize the impact of an attack. To achieve this, two architectures for a secure mobile operating system were developed, along with a risk analysis. The cybersecurity encompasses not only 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 increase security.

Artificial Intelligence for Cyberdefence: Blue Team Automation

The high complexity and speed of attacks makes it increasingly challenging to protect critical facilities and processes. As a response, the Fast-Blue project is developing the cognitive model of a cybersecurity team. The project aims to build an automated methodology capable of correlating and analyzing streams of cyber-related data and enabling deep threat investigations and preventive measures. This model is driven by automated workflows and an examination workbench to propose and recommend response and protection measures. The Blue Team must explore the environment, harden systems, detect and respond to Red Team activity. That fully automated cyber defence system would no longer require human assistance to identify and counter attacks within a complex infrastructure. The work conducted in 2021 focused on detection mechanisms and correlation of operating system incidents. The correlation through the use of graphs allows these incidents to be traced back to their origin and thus identified as potential attacks. The correlation has been extended to Windows and is also able to detect cross-movements between Linux and Windows. The detections are based on predefined attack scenarios, however, the goal is that the system will be able to detect attacks autonomously in the future.

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 (organizations 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 used processor architecture, 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

The Linux kernel is nowadays 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 misbehavior 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 misbehaviors, but it is unclear whether they are actually exploitable, i.e. whether they are real vulnerabilities. This research project is working on an automated procedure to assess this exploitability. This is central to classify the criticality of identified misbehaviors and to be able to address them in a prioritized manner.

Cyber Threat Intelligence Platforms

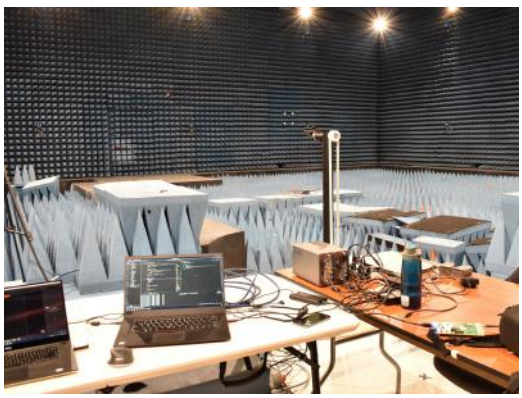
As cybersecurity information tends to be highly sensitive and confidential, organizations are reluctant to share this data with third parties, even when aggregated analysis of common threats would offer significant benefits for incident response and adaptation. In response to this trade-off, CYD Campus researchers are developing a platform that provides technological guarantees to ensure that authorized users can only access global insights (cyber threat models) based on data from the entire network. Each institution thus maintains full control over its datasets. This is made possible on the one hand by developing a Malware Information Sharing Platform (MISP)-compatible distributed architecture without a centralized database, and on the other hand by integrating advanced cryptographic techniques based on the homomorphic multiparty encryption model. As a result, institutions can securely collaborate on essential sensitive data that is not usually shared, leading to new and improved threat analysis and prediction.

Quantum Secure Cryptography

The advancing research on quantum computers poses cryptological challenges. Previously used digital signature schemes (DSS), as well as asymmetric cryptosystems (Public Key Encryption - PKE) and Key Encapsulation Mechanisms (KEM), which are secure regarding existing "standard computers", can be broken with quantum computers. Therefore, the National Institute of Standards and Technology (NIST) has begun to select and standardize quantum-safe successors to classical public-key methods. In July 2020, the third round of evaluation was initiated. In this process, seven finalists were selected from the candidates in the previous rounds, along with eight alternative candidates. In this research project, the candidates of the last evaluation round that are code-based (Finalist "Classic McEliece" and Alternate Candidates "BIKE" and "HQC") or based on multivariate polynomials (Finalist "Rainbow" and Alternate Candidate "GemSS") are examined. In addition, possibilities to extend and adapt the proposed methods are developed and investigated.

Hacking Micro Drones

Unmanned Aerial Vehicles (UAVs), also known as drones, represent a revolution in security and military applications. Due to recent advances in miniaturization and decreasing costs, mini UAVs have also become very popular in the civil 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 goal of this project is to explore various techniques for jamming and taking over mini-drones in order to neutralize the menace they present. Particularly, it is investigated 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 the possibility of gaining control of mini-UAVs through the GPS channel. GPS takeover could be successfully demonstrated in the laboratory.



Laboratory test setup to take over drones in a controlled manner via GPS spoofing

Secure Wide Area Networking

With the growing need for secured connections between offices, partners and cloud-based applications, private networks that are 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 and trusted communications and transfer information between organization sites, trusted partners, and cloud providers. The goal 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 connecting the CYD Campus sites in Thun, Lausanne and Zurich.

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-profile, so-called denial-of-service (DoS) attack wirelessly interrupts and terminates the charging process. The analysis of such attacks and possible countermeasures will be carried out during the further course of this project.

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

Cyber in Aerospace

Cybersecurity 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 cybersecurity. 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 now be detected automatically in a further research project.

Protection of Non-Secure Avionics Systems

This research project deals with the analysis of vulnerabilities in avionics hardware and the associated wireless protocols. In 2021 a practical attack on FLARM was demonstrated among other things which could be performed with little resource effort. FLARM is a collision warning device used in light aircraft and drones that was developed in Switzerland and has received worldwide attention and dissemination. The FLARM's display shows surrounding aircraft according to the priority of the most dangerous approach, thus supporting airspace surveillance. In addition, analyses of commercial avionics systems were performed with the help of the Avionics Lab. On the theoretical side, the Controller Pilot Data Link Communication (CPDLC) protocol was studied, identifying vulnerabilities and opportunities for improvement. CPDLC is a method by which air traffic controllers can communicate with pilots through a data link system.

4.2 Projects in Data Science

Distributed IoT Sensors: Hardware and Behavioral Analysis

Internet-of-Things (IoT) devices are nowadays omnipresent in numerous use cases, including military settings, which makes them an interesting target for cyber attacks. Unfortunately, manufacturers do not prioritize security in either the hardware or software during the development process. For example, the popular Raspberry Pi devices do not have a tamper-resistant identifier, making them easy to imitate. By looking at hardware variations, such as clock drift, Machine Learning models are trained to recognize hardware fingerprints that can uniquely identify an IoT device. These fingerprints could be used in the future as additional security in various applications. Similarly, software fingerprints are created to model the regular behavior of an IoT device. Machine Learning models are trained to detect if a device is behaving in an unexpected way, thus allowing the detection of cyberattacks such as botnets or ransomwares. For this purpose, metrics such as process calls and resource allocations from the operating system are used.

Distributed IoT Sensors: Modulation Classification and Collaborative IoT

The electromagnetic spectrum is a common resource and is also critical to many systems, such as telecommunications, radar, and positioning. For this reason, it must be protected from cyberattacks that could affect these systems. Automatic algorithms for modulation classification attempt to identify modulations. While some expert systems and approaches based on Machine Learning provide good results, they have problems when dealing with unknown parameters, such as the channel or sampling rate, for which they have not been trained. In this project, transfer learning methods are being explored to allow the deployment of low-cost Software Defined Radios. With transfer learning, the CYD Campus is capable of classifying modulations under previously unknown conditions that typically lead to misclassification in traditional approaches.

Artificial Intelligence Working Group with the US

In 2021, representatives of the CYD Campus and the US Department of Defense held several exchanges on the topic of Artificial Intelligence. In particular, joint fundamental knowledge was gained in this field and corresponding applications were identified. This involved examining current technological possibilities, developing potential technology solutions, and initiating joint activities. There are identical areas of interest in the monitoring of new technologies, the Internet of Things (IoT), and decentralized Machine Learning.
The working group was formed in 2020 under an agreement on research, development, testing and evaluation. This agreement was signed between the US Department of Defense (DoD) and the Swiss Federal Department of Defense, Civil Protection and Sport (DDPS) in April 2019.

Intelligence Gathering Cyberspace: Stratosphere

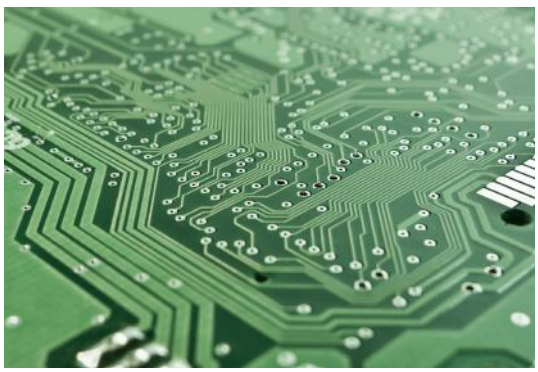
In order to be able to analyze data, it must first be acquired. While cyberspace is de facto a source of data, it has so far been considered only as a virtual environment of information and communication technologies. However, cyber risks today can also impact air and space, such as aircraft and satellites. It is therefore important to consider cyberspace as a multidimensional environment. In this project, the intention is to collect data in a strategic location, namely the stratosphere. This is particularly interesting since it is located between satellites and the Earth. This means that the CYD Campus researchers are capable of collecting data from uplinks and downlinks. For this purpose, they are developing an elevation platform carried by a weather balloon. The payload will contain a Software Defined Radio that can intercept signals and communications and locate transmitters on Earth or in space.

Data Protection with Wearable Devices: Identifying Personality Characteristics

Connected watches now account for a large share of the watch market. They offer various functions such as counting steps and heartbeats and are equipped with sensors to detect movements. While these watches are considered useful by many owners, they are unaware of the potential privacy issues. The data generated by the watches is made available to third-party apps, which can further use it for different purposes. In this project, the ability to identify the personality traits of FitBit owners by evaluating their openness, sense of duty, extraversion, adaptability, and neuroticism is investigated. By training Machine Learning models with the collected data from these watches, it was possible to outperform the current baseline as well as demonstrate that personality can indeed be determined. In addition, the data also allows categorization of possessors by gender and religion, which could lead to discrimination issues.

Computer-assisted Data Analysis: Robustness of Deep-Learning Models

Machine Learning models have become increasingly important in recent years. They are no longer used solely in specialized 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. Within this project, CYD Campus employees deal with Deep Learning models and investigate methods to increase their robustness. To do this, the training set is augmented 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 the normal accuracy.

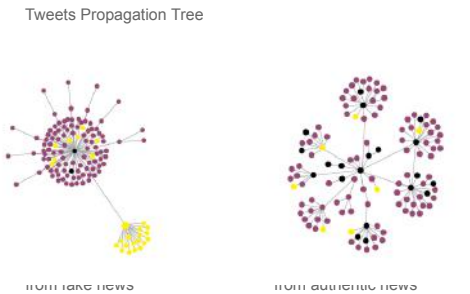


Data Protection for Wearable Devices: COVID Contact Tracing

In response to the COVID-19 outbreak, many countries implemented contact tracing apps. These apps have been used as a way to identify individuals who may have been in contact with infected individuals. In order to do this, the respective app on the smartphone regularly sends a signal via Bluetooth. In this project, CYD Campus employees are examining the data privacy of several contact tracing apps in order to find out for instance whether it is possible to identify individual users. Therefore, several data collection campaigns were organized in the major Swiss train stations. By analyzing the identifiers sent by the phones, it was possible to highlight the risks of the contact tracing apps.

Detecting Fakes in Social Media: Identifying Radicalization

Suspicious behavior on social media is portrayed under a number of labels, such as fake news, disinformation, compromised accounts, identity fraud, propaganda, hate speech, or radicalization. All listed behaviors share a common trait: they divide society. Taking the use case of radicalization, this project identifies moments in a user's social media timeline that indicate a change in their attitude toward extremist views. Based on such a moment, data-trained language models are used to model the influences the user was exposed to that may have led to this change in behavior. Identifying the most influential features in the information flow makes it possible to provide early warning signals when the intention to radicalize can be pinpointed.

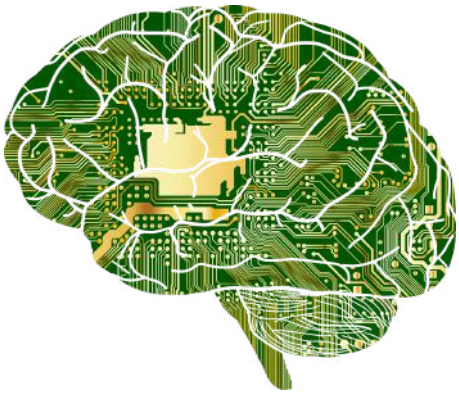


- the central root node displays a news report;
- the nodes marked in black show highly influential users;
- the nodes highlighted in pink show retweets;
- the yellow colored nodes show quotations from the original message or from a retweet.

Detecting Fakes in Social Media: COVID Misinformation

In the event of a rapidly spreading pandemic, it is necessary to quickly obtain relevant knowledge about the disease. Twitter is a popular medium for getting real-time information about global events. However, the network also serves to spread misinformation. The formation of filter bubbles, lack of control, and lack of verification or review of information are central problems of social media. In the age of infodemics, it is critical to capture people's reactions to public health measures and understand their concerns. This project focuses on identifying posts on social media that are related to a particular misconception (relatedness identification) using classic machine learning models such as logistic regression or support vector machine (SVM), as well as semantic text similarity. The posts related to a misconception are then classified with respect to the misinformation they contain. Furthermore, using the misassumption as a discussion topic and the user comments, it is possible to find out whether the author is for or against the topic (stance detection).

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. Rather than focusing only on language or dialect classification, this research project attempts to identify language before the entire utterance or text is given as input. In other words, the focus is on making a reliable statement about classification at an earlier stage. The goal of the project is to find criteria for truncating the input data that will determine and facilitate dialect prediction depending on the input sample and model. Ideally, the overall prediction accuracy of the suggested approach should exceed or at least reach the original performance. In this project, the CYD Campus tackle the challenging task of dialect classification, focusing on two languages: Swiss German and Indo-Aryan. Experimental analysis shows that in most cases there is an earlier point in time where prediction can be performed. This is possible using the input truncation criteria, which are based on calibrated probabilities and label consistencies.

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 analyze the vulnerability of NMT systems and understand their behavior 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 refers 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.

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 amount of parallel translation data, so-called high-resource language pairs. For language pairs with weak resources 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 improve the quality of translation in low-resource settings.

Data Science Methodologies for Technology and Market Monitoring

In order to track technology and market developments, one must be able to recognize technologies, distinguish them, and understand their relationships to each other. Using the technology-related concepts within the Wikipedia graph, a method for identifying the real-world position of a new concept within an existing taxonomy based on semantic and relevant similarities is proposed by the CYD Campus. Moreover, a framework for recognizing the technology-related concept in non-structured text is 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.

Early Warning Signals in OSINT: Anticipation of Conflicts

The anticipation of conflict is a key task for governments and armed forces. Knowledge of potential conflicts or instabilities can largely influence the 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. Statistical methods allow CYD Campus employees to identify and predict so-called tipping points that indicate a change of direction. Changes of direction can be a coup or other major political change. By analyzing data from India and Iraq, it was possible to model the dynamics of instability in these countries and thus identify the corresponding early warning signals.

Causal Analysis

In statistics, correlations are often used as a means to show a relationship between two variables. However, correlations do not indicate whether or not there is a causal relationship between the two variables. The purpose of causal analysis is to find the root cause of a problem rather than just examining the symptoms. This technique helps to uncover the facts that lead to a particular situation. In recent years, many advanced approaches and methods for causal inference have been developed, especially in statistics. The goal of this research project is to provide an overview of modern methods for interpreting, identifying, and estimating causal effects of observational data. For example, causality could be applied to conflict monitoring and prediction, where such methods could provide insight into the reason for a change in geopolitical stability.

5 Customers and Distribution of Cost and Effort

The federal government's cyber disposition is divided into three areas: Cyber security (FDF), Cyber defense (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 2021, the CYD Campus provided services for Procurement, Defense and Administration.

More specifically, contracts were awarded to the following organizations:

- armasuisse – Command and Control and Reconnaissance Systems
- Armed Forces Staff
- Armed Forces Command Support Organisation
  - Cybersecurity organizations
  - Defence Joint Operations Command
- Federal Intelligence Service
- Federal Department of Finance National Cyber Security Center NCSC
- Federal Office of Police fedpol

Contract Services	Distribution 2021
Security analyses, pentesting, security consulting	29 %
Security analyses & pentesting	16 %
Security concepts & consulting	13 %
Vulnerability Research	2 %
Vulnerability Research	2 %
Consulting, Technology Transformations	21 %
Consulting Support Data Science	3 %
Technology Transformation	18 %
Demonstrators	29 %
Designing Technology Demonstrators	5 %
Designing Innovation Demonstrators	24 %
Preparation & Collaboration in Studies	19 %
Creation of Capability Studies	2 %
Creation of Baseline Studies	2 %
Collaboration Baseline Studies	11 %
Creation of Technology Studies	4 %

Table 1: CYD Campus distribution of contracts 2021

The total performance of the CYD Campus divided by area is illustrated in Figure 1. The primary core services were in the areas of research, innovation and procurement support. A more detailed listing in Table 1 shows the distribution of contracts that were processed in 2021.

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

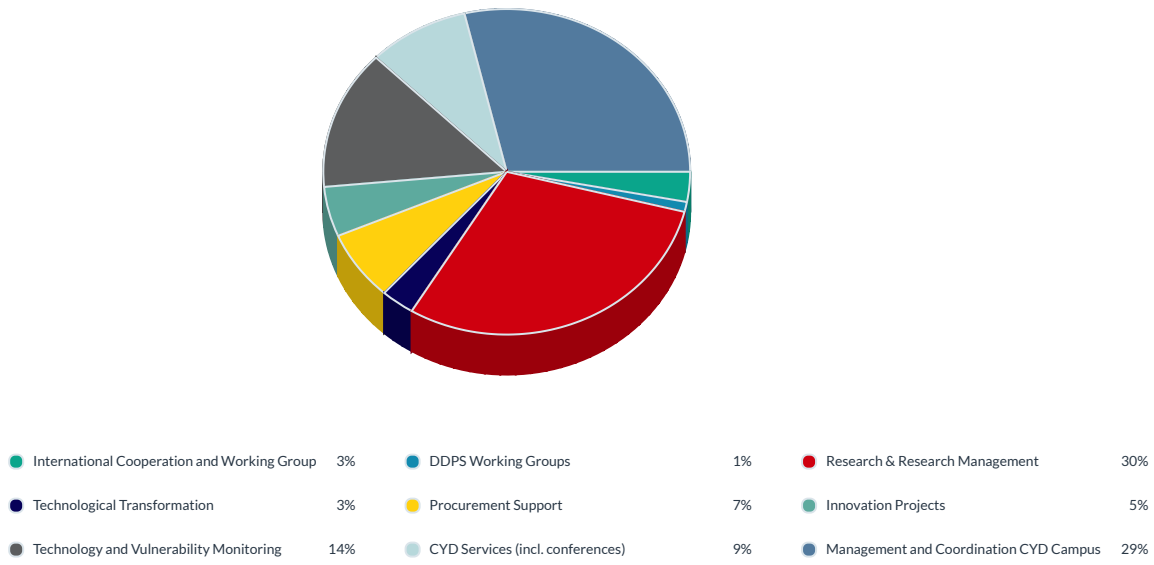


Figure 1: Services 2021 CYD Campus

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 or client and to prove the applicability of the technology in practice for the customer.

In 2021, innovation reports were carried out for the following organizations:

- Armed Forces Command Support Organisation
- Federal Office of Police fedpol
- Federal Intelligence Service – MELANI

The majority of the Innovation Reports were conducted in a one-day workshop on site in Thun. Due to the COVID-19 restrictions, the complete presence of all participants had to be waived. Rather, the events were conducted hybrid with the support of videoconferencing and in compliance with information security.

6.1 Innovation Projects Results

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

Application of Artificial Intelligence to Contemporary Challenges

Network intrusion detection systems (NIDS) are critical components of modern secure networks that help detect indications of cyberattacks on a network. Such attacks are becoming increasingly complex and are targeting the growing number of connected devices, including Internet of Things (IoT) devices. While today's IoT systems already generate a majority of Internet traffic, the IT security of the devices remains weak, leading to a high number of successful attacks. New Machine Learning (ML) technologies are expected to improve the adoption of innovative network attack detection systems. In this innovation project, the performance of new ML models for NIDS was investigated on various IoT network datasets, and new techniques for network feature extractors were verified in use.

Introduction of Methods to Protect Privacy

This project investigated how privacy-preserving protocols such as private set intersection (PSI) or private membership test (PMT) can be used to prevent unauthorized logins by remotely logged-in employees. Different cryptographic primitives such as homomorphic encryption (HE), oblivious pseudorandom functions (OPRF) and garbled Bloom filters (GBF) were used. The results show that the computations of the OPRF PSI protocol require less than 200 ms for 4,000 workers, while the data transfer cost is less than 1 MB. Using the OPRF approach for PMT, computations take 14 ms and the protocol requires parties to transmit less than 20kB.

Knowledge Transfer in the Field of Data Science

The transfer of knowledge from the academic world to the CYD Campus customers is carried out on different levels. With courses in the field of data science, employees teach the basics of statistics and mathematics to various organizations of the DDPS. The transferred learning content is adapted to the respective specialist domains of the customers and customized to current analyses.

Exploratory Work

In addition to scientific expertise, technical innovations are also transferred to the CYD Campus customers. An example of this technological knowledge transfer is the provision of expertise in the management and maintenance of data in so-called data lake architectures.

Supervision of the Implementation of Data Structures and Processing of Large Data Volumes, Big Data and Data Lakes

Big Data has driven the development of a wide range of technologies in recent years. Examples of Big Data technologies include new storage technologies for large amounts of data and different data formats (e.g., structured and unstructured data formats), the processing of data streams in real time, and computing in distributed systems. The CYD Campus advises and supports customers from the DDPS in the development of systems using data lake architectures that prominently employ Big Data technologies.

A significant part of the CYD Campus Know-How stems from the establishment of the Data Science Lab, a platform that is specifically developed and operated for the storage and processing of Big Data.

Introduction of a Novel Platform for Cyber Threat Landscape Monitoring including Data Exchange

The understanding of and protection against cyber threats is becoming increasingly complex as offensive tactics, techniques, and -procedures are rapidly evolving. The goal of the Cyber Threat Landscape Monitoring (CBL-) project is to develop a proof-of-concept for a Threat Intelligence Platform (TIP). The developed platform leverages existing open source elements such as MISP, OpenCTI, and TheHive, with each tool having a specific function.
The platform has been extensively tested and improved with specific functions such as document analysis (parsing). In addition, the architecture and the developed setup were documented. Several possible approaches to solve the problem, such as other available tools, future availability and flexibility were also considered. Furthermore, the study described an ideal final architecture. The objective of the study is to present the best possible productive design, taking into account costs, risks and long-term operation.

Introduction of an Offline Machine Translation Platform for Tactical Operational Missions

In this project, it has been demonstrated that in the case of general texts, it is possible to train models that provide a comprehensive translation regardless of the source or target language. However, it has been shown that the data used for training can have a significant impact on the quality of the translation. Varied data obtained from different sources allows the learned language and translation model to be highly reliable against language variations. In addition, models trained for general translation can be optimized on internal datasets to cover more specific use cases. These data corpora used for internal training can also be from classified sources.

Design of an Architecture for Secure Mobile Operating Systems

There is a lack of a comprehensive security architecture for a mobile operating system in open-source or commercial projects. In fact, the security architecture should capture risks in compartments to protect confidential data and communications from an attack or unauthorized access. In addition, users should be able to run unsecure applications on a device alongside secure applications while simultaneously working with confidential information. With the aim of building such a security architecture, two architectures have been developed. The underlying system is based on a hypervisor concept for running multiple kernel and Android instances. The drivers are also virtualized, whereby the kernels do not have direct access to the hardware.

Automated Exchange of Security Vulnerabilities

The CYD Campus is collaborating with the German Federal Office for Information Security (BSI) in the area of cybersecurity for the first time in 2021. The collaboration involves providing open-source software applications that enable security recommendations to be created and managed in a format that can be used by machines. This facilitates the exchange of information on security vulnerabilities, which improves cybersecurity.

6.2 Cyber Startup Challenges

2020: Cyber Threat Intelligence

Startups often have innovative and disruptive ideas and can offer technologies that can provide a technological advantage against attackers. For this reason, CYD Campus launched the Cyber Startup Challenge in 2020.

The startup CounterCraft was able to convince the jury in 2020 of its novel solution in the field of cyber threat intelligence. The company implemented a customized proof-of-concept in 2021.

The deception scenario describes a small industrial control network with a small number of active Programmable Logic Controllers (PLC). This could be a small remote facility, such as a power substation or a water pumping station. The network is managed via a human-machine interface (HMI), with control data stored in a networked database. The system is managed from a control center.

The proof-of-concept has been tested with the Army's operational units in 2021 from both the attacker's and defender's perspectives. It was possible to compare the generated tactics, techniques, and procedures (TTP) with the response of the platform.

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

The Cyber Startup Challenge 2021 aimed to discover the startup technology landscape under the theme "Strengthen your Information Sharing and Analysis Center (ISAC)" and seeked innovative solutions in the field of cyber threat intelligence with a focus on critical infrastructure protection.

A total of 38 startups from Europe, the US and Asia answered the call. The jury, formed by cyber experts from the DDPS and armasuisse S + T, selected the three finalists Decentriq, Constella Intelligence and Pandora Intelligence, which delivered a pitch at the CYD Campus Conference on September 28, 2021. Zurich-based startup Decentriq impressed the jury with its innovative Software-as-a-Service (SaaS) platform offering "Data Clean Rooms" for enterprises. "Data Clean Rooms" are secure, protected environments in which personal data is cleaned and processed so it can be used for a variety of data analysis purposes. The platform enables internal and external stakeholders of critical infrastructures to securely share cyber data and gain aggregated and anonymous insights. In this way, cybersecurity is enhanced without compromising data privacy.

Decentriq will work with CYD Campus in 2022 to integrate a proof-of-concept of its technology into a real-world DDPS environment.

7 Security Analysis, Pentesting and Security Consulting

In 2021, CYD Campus employees examined the security of a dozen military systems that are being processed as part of part of armament and ICT procurements within the DDPS. The tests were conducted as security analyses, pentestings 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
- Middlewares
- Computer Networks
- VPN Technologies and Crypto Solutions
- Command and Control Information Systems
- Drones
- Vehicles
- Wireless Communication Systems (Language and Data)
- Aviation and Satellite Communication Systems

The analyses and audits have 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, pentesting and security consulting services cannot be described in more detail in the Annual Report.*

8 Demonstrators

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.

Deployment of the Demonstrator for Tests with People

The potentials of the 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 realize in the real world (emergency scenarios in vehicles, execution of large exercises, operations in urban areas, etc.)

Mixed Reality Demonstrator for Training Simulation

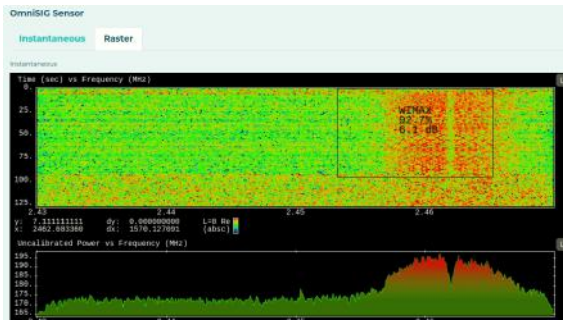
There are certain risks associated with using the technology, including:

- 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 while there is great potential, bundling the various components and overcoming the risks is challenging.

Demonstrator Signal Classification

Cyber warfare and electromagnetic warfare have mostly been considered separate domains. Today, we see a convergence of both areas 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. A promising US startup has been identified by CYD employees that can classify signals using magnitude and phase signal data through deep learning methods. The software offers a simple user interface and advanced features, and is based on state-of-the-art and constantly evolving technology. It can also be run with low-cost, off-the-shelf computer hardware. The sensors that perform the inference require limited computing power and can run on a small embedded platform with a graphical processing unit. This demonstrator shows the importance and potential of this technology, which is just beginning.



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

Demonstrator GPS Drone Spoofing

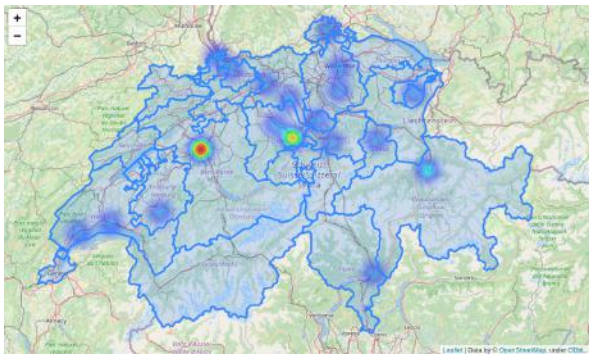
GPS spoofing is an attack that uses a radio transmitter near the target to fake a legitimate GPS signal. Since drones rely on GPS signals to determine their location, they are also affected by such attacks. It could already be shown how a drone reports the fake location back to the pilot. The research now focuses on how a drone can be hijacked using this attack. The idea is to constantly fake nearby locations and simulate real movement so that the drone is moving and the attacker has full control over the drone's movement. GPS spoofing could thus be used by an attacker to hijack commercial drones from private individuals in order to carry out undetected malicious actions, such as crashing the drone against a specific target or stealing the drone in order to obtain personal data.

Demonstrator Augmenting Reality for Security

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

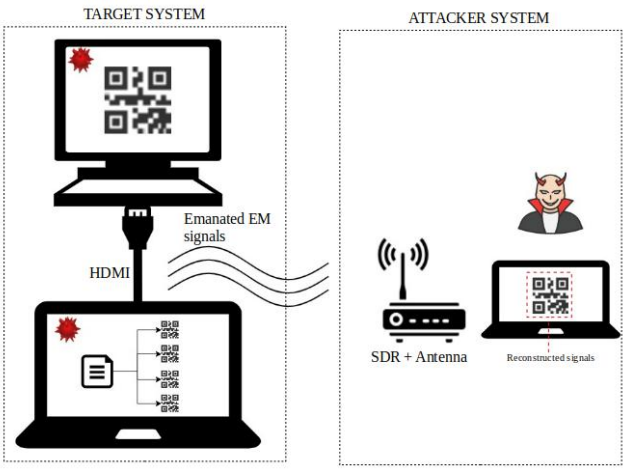
Evaluation of Augmented Reality for Better Defence Against Phishing

Demonstrator Social Media-Situation Map



Heatmap of the Number of Tweets that Reference Localities in Relation to the COVID19 Pandemic

Communication in the 21st century is shaped by three technologies: the Internet, mobile devices and social media. It is therefore not surprising that this infrastructure is used by certain actors, such as foreign intelligence services, for the targeted dissemination of misinformation. Therefore, a demonstrator for the automated analysis of content from Twitter accounts is under development. This involves downloading all posts written by the target account via the official Twitter API. Subsequently, an analysis of text, image and video data contained therein can be performed. By using regular expressions, date and time information associated with the named locations can be extracted from the tweets. This allows content to be placed in a temporal and locational context, allowing the generation of a situational picture. The textual content of the tweets is then further analyzed for word frequencies and the frequencies of named localities. This provides a first impression of dominant narratives of a Twitter account and its relation to events defined in terms of location and time. Furthermore, image data is analyzed using modern Deep Learning Methods (Convolutional Neural Networks), which allows image-with-text memes to be distinguished from other image data. Image-with-text memes are an effective tool for propagating ideas and controlling online narratives, making them attractive as a tool for disinformation campaigns.



Exploiting the Emission of HDMI Video Cables to Exfiltrate Sensitive Data from an Infected Computer

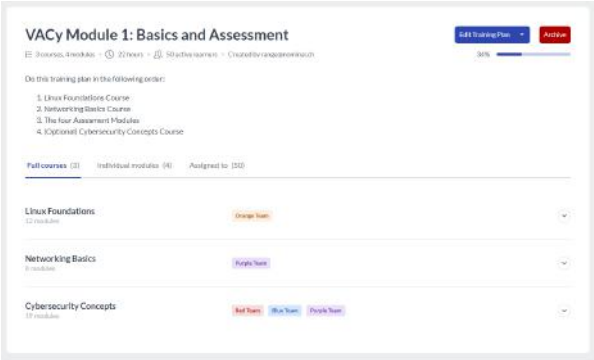
Demonstrator TEMPEST Data Outflow

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 obtain 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 between a PC and a video monitor to extract internal information from the monitor. In this demonstration, the CYD Campus illustrates 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 communication system to transfer different types of inforformation 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.

Demonstrator Gamified Cyber Training

It is well known that there is a systematic lack of qualified workers in the cybersecurity 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 them something appealing. In this context, gamification in cyber education can make an important contribution. Gamification refers to applying game-typical elements in a game-unrelated 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 (starting in November 2021) were able to use the innovative software of one of the selected startups.



Software Environmentc of the Army's Pre-Service Cyber Training

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

Demonstrator Car Hacking

During the Car Hackathon in Thun, which was described in the chapter Highlights, the participants developed several demonstrations of attacks that can be carried out against cars. In one case, connecting an interface to the CAN bus (communication interface) of an electric car could trigger unintended behavior such as flashing lights, opening and closing windows, or influence the power steering. In view of the strong trend towards electromobility, it has also been demonstrated that the charging process of electric vehicles can be disturbed and interrupted remotely.

Demonstrator Visualization of Critical Infrastructure Attacks

When performing capture-the-flag or live-fire exercises, it is often difficult for cybersecurity experts and decision-makers to understand the impact of cyber actions on the physical infrastructure. This is because, unlike attacks on cyber-physical systems such as power generation facilities or military (weapons) systems, it is comparatively easy 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 Army, a demonstrator was developed to illustrate these effects. It consists of a 2.4 x 1.2 meter terrain model that is modular and easy to move, showing a mixed civil-military airport as well as critical infrastructure, energy production and military systems. This installation was successfully tested in a live-fire cyber exercise by the Swiss Army in 2021. Next year, it will be further developed by connecting it to real Programmable Logic Controllers (PLCs) and integrating it into a realistic Supervisory Control and Data Acquisition (SCADA) environment that can be used for research and exercises.

Visualization of Cyber Attacks on a Military Airfield

Demonstrator Hybrid Cyber Range

Cyber Ranges are infrastructures that consist of several computers and networks and can be used for research or exercises. Usually, most of the infrastructure is virtualized, i.e., there are no real workstations, but they run on servers in a data center. However, real networks consist not only of servers and workstations, but also include physical components that are used to monitor and control technical processes. Components have been tested that have enabled CYD Campus employees to integrate real industrial monitoring (SCADA) systems into a Cyber Range. These were successfully employed in exercises and other trials.

Industrial control system with a visualization display (top) and a mobile cyber section (bottom)

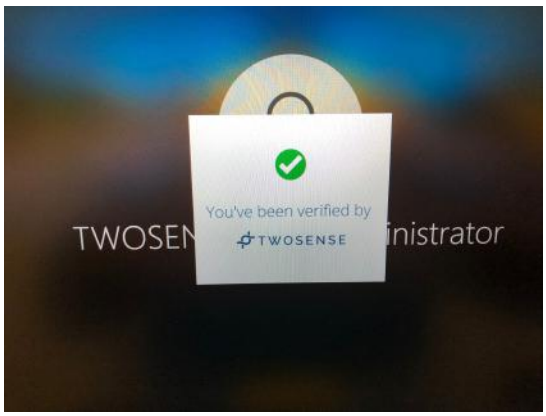
Demonstrator Offline Translation

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.

Sample translation from Chinese to English with an offline system

Demonstrator Continuous Authentication

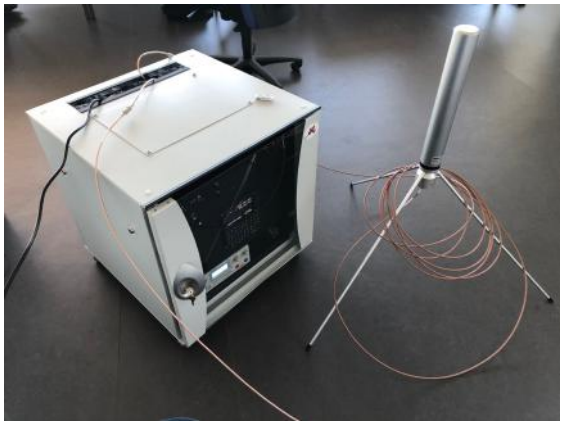
Password queries or one-time biometric checks such as fingerprint or iris sensors grant users access after successful authentication and do not regularly check for malicious behavior or a change of user. These methods allow, for example, so-called midday attacks, where an attacker uses a workstation where a legitimate user is still logged in. Similarly, password data can be stolen through leaks, shoulder surfing or phishing attacks, giving an attacker a free hand on the target system. This stands in contrast to Continuous Authentication (CA). It 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 behavior 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.



Behavior-based verification of the user by the demonstrator.

Demonstrator Aircraft Communication Spoofing

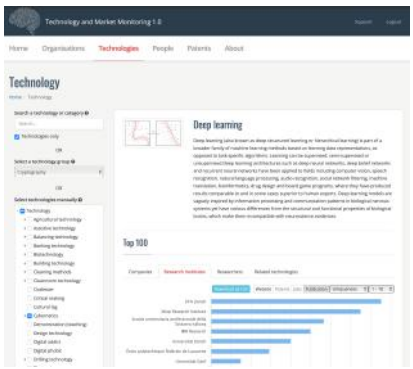
In the 2010s, researchers and hackers demonstrated numerous vulnerabilities in wireless technologies used by aircraft and air traffic controllers. To date, such spoofing has been demonstrated using low-level tools such as software-defined radios exclusively on computers with simulated hardware and software.
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 Technology and Market Monitoring

Based on open source data, the demonstrator offers users a list of relevant companies in Switzerland that correspond to the technology cluster they are looking for. In addition, information about vacancies, number of patents and number of publications is available in the demonstrator, and companies can be found with their information such as products, services and technologies offered. This makes companies visible both as potential (sub)suppliers and as possible offset partners in procurement.



Excerpt TMM Tool on Deep Learning Technologies

9 Technology and Market Monitoring

The CYD Campus provides an anticipation platform for cybersecurity technology developments and trends. With this activity, the DDPS seeks to detect technical developments and understand their opportunities and risks at an early stage. To detect the latest trends in the market, the CYD Campus employs both quantitative and qualitative technology and market monitoring (TMM) methods. On the one hand, emerging cyber technologies and clusters are discovered using the TMM platform using quantitative analysis of publicly available data. On the other hand, promising startups are identified through a qualitative scouting, an international technology monitoring program.

Cybersecurity Technologies

In order to discover relevant cybersecurity technologies on the market, it is essential to have access to data sources with up-to-date and reliable information about the technologies available on the market. For this purpose, the CYD Campus uses its own Technology and Market Monitoring (TMM) platform as well as other sources.
This year, CYD Campus researchers produced a report providing an overview of trends and activities in Switzerland and abroad in the field of cybersecurity technologies. The findings were presented at the CYD Campus EPFL site in Lausanne on December 2, 2021.

Depiction of the Swiss cybersecurity ecosystem

In the context of TMM, a study was conducted in collaboration with the Military Academy (MILAC) at ETH Zurich. The aim was to model the public, private and academic ecosystems related to the cyber domain in Switzerland. Several network maps and a geographic representation of the key players were developed. A part of this project was published on the NCSC website by providing a list of academic trainings available in Switzerland in the field of cybersecurity.
Link to Swiss Cyber Map:

Scouting

Through its qualitative scouting, the CYD Campus identifies interesting startups and partners in Switzerland and abroad that meet the requirements of the DDPS. The program is primarily aimed at emerging companies, but sometimes also at established companies that can offer innovative products. A network with various partners such as Swissnex, Swisscom, PlugandPlay, various startup accelerators and venture capital firms, as well as with Embassies and other institutional actors has already been established to systematically scan key markets for new trends in cyber technologies. From a geographical perspective, the focus is on regions with high-performing startups.

Among them are:

- Switzerland: Trust Valley, Crypto Valley and Inno-space Zurich.
- United States: Metropolitan areas around Silicon Valley, Washington DC, Boston, New York, Seattle, and Austin.
- Israel: Armed Forces unit generates 8200 top cybersecurity talents.
- United Kingdom: Renowned universities and a large defence budget contribute to the startup scene.
- France: Cyberpol in Rennes promotes work in cyber security.
- Germany: Support from organizations such as the Institute for Cyber Defence at the Bundeswehr University Munich.
- Estonia: Location of NATO's CCDCOE as well as a state with a high level of digitization.
- Singapore: The state has one of the highest per capita defence expenditures in the world.

General Approach

During the scouting process, the resources of each company, the particular issue it is attempting to solve, and the company's proposed solution are analyzed. In addition, it is investigated for which stakeholders (armasuisse, other Federal authorities within and outside the DDPS) the company and its solution could be of interest. The respective agency of the Federal Administration can also make a specific request and the CYD Campus with the help of its network will try to find the most innovative and suitable companies to address a particular challenge. If required, a more profound evaluation or a proof-of-concept will be initiated.

2021: 300 STARTUPS
60 technical presentations
20 were referred to relevant units within the Federal Administration
8 proof-of-concepts implemented
12 active scouting-partners

Activities in 2021

United Kingdom

In April 2021, the CYD Campus scouted cybersecurity companies in the UK. The Swiss Business Hub (SBH) in London was heavily involved in identifying interesting companies and, with the help of local experts and the entire embassy team, created a longlist of around 100 UK startups and companies. The scouting team met with a wide range of companies in the UK that fell broadly into the following categories: supply chain security, data analytics, network detection response, industrial control systems, infrastructure, and threat intelligence.

Germany and Austria

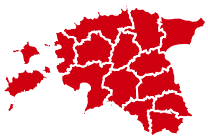
A similar process to the UK was conducted for Germany and Austria in late 2021, which also identified companies of interest.

France

In addition, the CYD Campus participated in the Forum International de la Cybersecurité in Lille, France, as well as in the European Cyber Week in Rennes, during which several important new contacts were established.

Estonia

A Scouting trip was made to Tallinn, Estonia, to gain first insights into its cyber security ecosystem. There are a some interesting companies, especially in the field of cyber education. The local ecosystem to support startups with knowledge, funding and human capital is well developed, however the absolute number of disruptive and mature startups is low.



United States

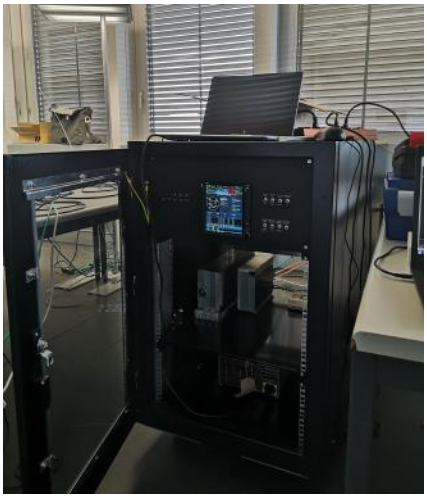
In 2019 and 2020, the cybersecurity panorama of the United States was explored thoroughly for interesting technologies. Given the rapid developments and the large market, a trip to the United States was conducted in August 2021, which allowed meeting several additional companies and sharing information with key partners.

10 Laboratory Infrastructures

The laboratory infrastructures of the CYD Campus are set up for collective knowledge building. In addition to the existing Cybersecurity lab, work has been done in 2021 to further develop the laboratory infrastructures. These are discussed in more detail in the following sections.

Advanced Cyber Avionics Lab

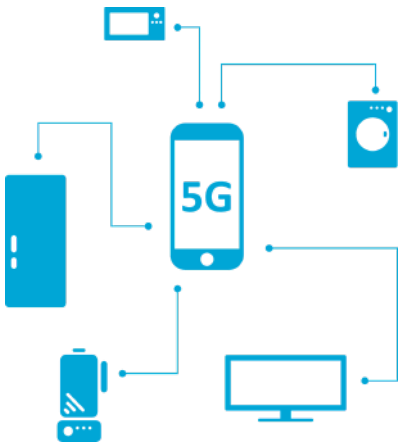
The CYD Campus Avionics Lab has already successfully supported the testing and security assessment of aircraft technologies, and results have been published for instance in the Aviation Village of the DEFCON hacker conference. Now, the lab is expanding to include Controller-Pilot Datalink Communication (CPDLC) technology. CPDLC is a data link used to exchange security-critical instructions between aircraft and air traffic controllers. The CYD Campus has already shown that without authentication CPDLC is not secure and that so-called man-in-the-middle attacks are possible. The aim now is to test this in practice in a laboratory environment with certified hardware.



Extension of the Cyber Avionics Lab with Controller-Pilot Datalink Communication (CPDLC)

5G Lab under Construction

5G technology expertise and competence are low in Switzerland, especially in the area of security and the core network. Most operators outsource the deployment and even the operation of the infrastructure, and academic institutions do not have access to research laboratories to train their students. A 5G research lab in Switzerland is of great importance to the DDPS and FUB. In the future, critical infrastructures will increasingly use 5G technology. The 5G research lab will bring the missing knowledge to the different organizations of the DDPS and explore the broad spectrum of security aspects.



Satcom Lab

To complement the existing improvised experimental platforms with small satellite antennas, a satcom lab will be established. At the center of this lab is a 2.5 meter diameter satellite dish mounted on a motorized 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. The laboratory is scheduled for completion in the summer of 2023.

Satcom Cyber Security Lab in Zurich

Data Science Lab

Deep learning algorithms require a high computing capacity. Graphics Processing Units (GPUs) are particularly optimized for the type of mathematical operations performed by these algorithms. To provide CYD Campus researchers with sufficient computing resources, a GPU cluster has been set up in the Data Science Lab. This comprises about 30 GPUs, which can be made available dynamically. Users only have to submit their task (code), which is then automatically executed on a free GPU. This makes it possible to submit several tasks at the same time. The GPU controller manages the assignment of tasks on the different GPUs. This infrastructure makes it easier for users to use and share GPUs, e.g. for machine translation, detection of fakes or prediction of time series. In addition, an FPGA server was set up this year to complement the GPUs and CPUs in the Lab.

Scion

To demonstrate the potential of new network technologies to secure traffic over Wide-Area Networks (WANs), a network laboratory will be established between the three CYD Campus sites (Thun, Lausanne and Zurich). The sites will be connected via ETH Zurich's new Scion technology to provide a secure and controllable routing. In addition, programmable switches at the sites provide the opportunity to implement new traffic obfuscation methods on the network and to study their efficiency. This laboratory infrastructure is used by researchers and partners of the CYD Campus for research and innovation projects.

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

11 Events

Conferences

16-18 November 21 Rennes European Cyber Security Week

More than 4000 public and private actors and 84 partners in the field of cybersecurity met in Rennes to identify and anticipate future technological developments. The CYD Campus participated in order to build networks with relevant stakeholders.

27-29 September 21 CYD Campus Conference & CRITIS

On September 28, 2021, the CYD Campus Conference took place at the EPFL SwissTech Convention Center in Lausanne (remote participation was also possible). The main topic of the conference was the security of critical information infrastructures. The conference was organized in collaboration with the 16th International Conference on Critical Information Infrastructure Security (CRITIS 2021), which was held on September 27-29.

7-9 September 21 Forum International de Cybersécurité, Lille, France

The forum is one of the largest annual European cybersecurity events and offers stakeholders the opportunity to network in the European cybersecurity ecosystem. In 2021, Switzerland was represented for the first time by the CYD Campus and a dozen other companies. The main goal of the CYD Campus participation was to find companies with innovative ideas in cybersecurity.

10-11 March 21 Swiss Cyber Security Days

Dr. Vincent Lenders, Dr. Luca Gambazzi and Giorgio Tresoldi prepared a video on Locked Shields, which was presented at the conference.

Challenges & Hackathons

11-15 October 21 Car Hackathon

Around 20 people from armasuisse, industry, universities, FUB, and fedpol took part in the Car Hackathon. Several vehicles were examined with regard to their cyber security and the exploits for specific vulnerabilities were tested. Among the vehicles tested were electric vehicles, classic gasoline-powered vehicles, and a Duro.

28 September 21 Cyber Startup Challenge

Startups could submit their innovative technology solutions under this year's motto "Strengthen your Information Sharing and Analysis Center (ISAC)" in the field of cyber threat intelligence with a focus on critical infrastructure protection. The winning Zurich-based company, Decentriq, was selected at the CYD Campus Conference on September 28, 2021.

Data Science Challenges

8 November 21:	Meme Classification
24 September 21:	Dialect Identification + GPU cluster
21 June 21:	FitBit Data
10 May 21:	IoT Device Fingerprints
29 March 21:	Tipping Points
15 January 21:	Early Warning Signals

Opening speech by the Head of CYD Campus at the CYD Campus Conference in Lausanne

Car Hackathon Thun

Forum International de Cybersécurité in Lille

Lunch Seminars

Due to the ongoing pandemic, many seminars had to be cancelled this year. These information events feature presentations by selected speakers on specific CYD topics for customers from the defense and federal administration.

15 November 21: Quantum-Resistent Edge. Referent: Stiepan Aurélien Kovac, itk.swiss

6 Sept 21: Cybersecurity enriched by Quantum Technologies. Referent: Jean-Sébastien Pegon, ID Quantique SA

19 May 21: Tutorial: Running programs at terabits per second in network switches (P4 and Intel Tofino), Speaker: Roland Meier, ETH Zurich

3 May 21: Startup Seminar: Mit drei Startups von Tech 4 Trust (Swiss Startup acceleration program in the field of digital trust and cybersecurity).

Speakers:

Nagib Aouini, CEO and founder DuoKey SA
Gregor Jehle, CEO P3KI GmbH
Simon Janin, CEO X80 Security SAS

Retreats

28 June - 2 July 21: Cyber Alp Retreat
CYD Campus researchers and selected research partners gave presentations on key topics in cybersecurity and data science. The event brought together stakeholders from the DDPS, industry and academia to exchange insights on current and future challenges and drivers in cyberspace.

Research Reports

The purpose of these Annual Research Reports is to provide information on current research topics for the benefit of clients and interested parties. The Reports were held in hybrid form, whereby approx. 80 participants attended. Some participants were from the Armed Forces Staff, Armed Forces Command Support Organisation (AFCSO) , GS VBS and NDB.

3 June 21: Research Reports 3a Cyberspace

10 August 21: Research Reports 3b Data Science

Lunchseminar on Quantum-Resistant Edge in Thun

Research Report Data Science in Thun

Cyber-Alp Retreat 2021 in Gstaad

Visits

16 November 21: Visit Military Aviation Authority, Thun

10 November 21: Visit Chief of the Armed Forces, Thun

1 November 21: Visit Cyber-Lehrgang 2021, Thun

15 October 21: Presentation of Data Science to students of ETH

8 September 21: Visit University of Applied Sciences Lucerne and ICT Warriors, Thun

TMM Event

2 December 21: Cybersecurity Technologies, CYD Campus Lausanne

Student Exchange

Every other week on Tuesdays, CYD students and interns report on the results of their research projects. In this context, all employees of the respectiv

Recruitment Platform for Students

8 October 21 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, and to inform them about the diverse opportunities that the CYD Campus offers to gain practical experience.

CYD Fellowship Workshop for Applicants:

5 August 21

26 January 21

Visit Cyber-Lehrgang of the Armed Forces

TMM Event on Cybersecurity Technologies in Lausanne

Student Exchange in Thun

12 Referates

- 9 November 21 — *Collaboration EPFL-CYD Campus: Manager's Lunch*, EPFL Innovation Park, Lausanne, Dr. Vincent Lenders
- 25 October 21 — *Panel discussion*, *Workshop on Systems Challenges in Reliable and Secure Federated Learning, ACM SOSP*, Dr. Gérôme Bovet
- 15 October 21 — *Panel on the future of digital trust*, Digital Trust 2025, Geneva, Dr. Vincent Lenders
- 8 October 21 — *EPFL Forum*, Career fair, Lausanne, Dr. Mathias Humbert
- 30 September 21 — *Security and Privacy in Wireless Communication Systems*, Closing meeting Cybersecurity Expert Group, DDPS, Dr. Daniel Moser
- 3 September 21 — *Understanding cyber threats*, DSC Security Week, Dr. Daniel Moser
- 27 August 21 — *Deep Fake Video Federal Councillor Viola Amherd*, Cadre Day DDPS, Dr. Gérôme Bovet
- 26 August 21 — *Fusion von OSINT und SAR-IMINT - NATO/PfP Research Program SET-279*, Information event on radar satellites, armasuisse, Thun, Dr. Albert Blarer
- 7 July 21 — *Présentation du CYD Campus*, visites des secrétaires généraux de la Confédération à l'EPFL», Dr. Vincent Lenders
- 9 June 21 — *Digital NRW ministerial trip to Switzerland - Roundtable: Cyber Security*, Dr. Vincent Lenders
- 1 June 21 — *Machine Learning for Intrusion Detection Systems: Challenges and Opportunities*, AFCSO TechTalk, Dr. Mathias Humbert
- 30 April 21 — *Presentation CYD Campus*, Federal Palace, Visit Minister of Defence, Austria, Dr. Vincent Lenders
- 21 April 21 — *Analyzing Cybersecurity Risks with and in Machine Learning*, SDSC (ETH/EPFL) & ZISC (ETH), Dr. Mathias Humbert
- 7 April 21 — *Fake News in Social Media: How to fight them?* , Kdo Op - armasuisse S+T, Dr. Ljiljana Dolamic und Dr. Vincent Lenders
- 25 March 21 — *Wireless Security in Critical Infrastructures: Legacy Debt and Opportunities*, ZISC (ETH), Dr. Martin Strohmeier
- 18 March 21 — *Secure and Fast Satellite Broadband*, CySat, Davos, Dr. Vincent Lenders
- 10 March 21 — *The role of AI in Cyberdefence*, Swiss Cyber Security Days, Fribourg, Dr. Vincent Lenders
- 25 February 21 — *Cyber-Defence Campus: Assessment after 2 years, Subcommittee FDFA/DDPS of the Council of States*, Dr. Vincent Lenders
- 17. February 21 — *Cyberdefence Research and Innovation: The Swiss Approach*, UK-Swiss Cyber Seminar, Bern, Dr. Vincent Lenders
- 10 February 21 — *Research on Aviation Cyber Security*, BAZL, Dr. Martin Strohmeier
- 21 January 21 — *How (not) to do wireless security*, Eurocontrol, Dr. Martin Strohmeier
- 20 January 21 — *Deception technologies*, AFCSO TechTalk, Dr. Luca Gambazzi

13 Scientific Publications

13.1 Papers

December

Classi-Fly: Inferring Aircraft Categories from Open Data

Martin Strohmeier, Matthew Smith, Vincent Lenders, Ivan Martinovic, ACM Transactions on Intelligent Systems and Technology (ACM TIST) Volume 36, Issue 6.

Are Those Steps Worth Your Privacy? Fitness-Tracker Users' Perceptions of Privacy and Utility

Lev Velykoivanenko, Kavous Salehzadeh Niksirat, Noé Zufferey, Noé Zufferey, Proceedings of the ACM on Interactive Mobile Wearable and Ubiquitous Technologies, Volume 5, Issue 4.

Adaptive Uplink Data Compression in Spectrum Crowdsensing Systems

Gérôme Bovet, Yijing Zeng, Roberto Calvo-Palomino, Domenico Giustiniano, Suman Banerjee, IEEE International Symposium on Dynamic Spectrum Access Networks (DySpan), virtual.

TechRank: A Network-Centrality Approach for Informed Cybersecurity-Investment

Anita Mezzetti, Dimitri Percia David, Thomas Maillart, Michael Tsesmelis, Alain Mermoud, arXiv.

From Scattered Sources to Comprehensive Technology Landscape: A Recommendation-based Retrieval Approach

Chi Thang Duong, Dimitri Percia David, Ljiljana Dolamic, Alain Mermoud, Vincent Lenders, Karl Aberer, arXiv.

Cyber-Security Investment in the Context of Disruptive Technologies: Extension of the Gordon-Loeb Model

Dimitri Percia David, Alain Mermoud, Sébastien Gillard, arXiv.

November

Federated Learning for Malware Detection in IoT Devices

Valérian Rey, Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdránc, Gérôme Bovet, Martin Jaggi. Computer Networks.

The IICT-Yverdon System for the WMT 2021 Unsupervised MT and Very Low Resource Supervised MT Task

Àlex R. Atrio, Gabriel Luthier, Axel Fahy, Giorgos Vernikos, Andrei Popescu-Belis, Ljiljana Dolamic, Sixth Conference on Machine Translation (WMT).

When Machine Unlearning Jeopardizes Privacy

Min Chen, Zhikun Zhang, Tianhao Wang, Tianhao Michael Backes, Mathias Humbert, Yang Zhang, ACM Conference on Computer and Communications Security (CCS).

Fixed Points in Cyber Space: Rethinking Optimal Evasion Attacks in the Age of AI-NIDS

Christian Schröder de Witt, Yongchao Huang, Philip H. S. Torr, Martin Strohmeier. arXiv.

September

Studying Neutrality in Cyber-Space: A Comparative Geographical Analysis of Honeypot Responses
Martin Strohmeier, Vincent Lenders, James Pavur, Ivan Martinovic, 16th International Conference on Critical Information Infrastructures Security (CRITIS).

GNSS Positioning Security: Automatic Anomaly Detection on Reference Stations
Stéphanie Lebrun, Colin Barschel, Stéphan Kaloustian, Raphaël Rollier, 16th International Conference on Critical Information Infrastructures Security (CRITIS).

Link Prediction for Cybersecurity Companies and Technologies: Towards a Survivability Score
Santiago Anton Moreno, Anita Mezzetti and William Lacube, 16th International Conference on Critical Information Infrastructures Security (CRITIS).

A semantic-based approach to analyze the link security and safety for Internet of Vehicle (IoV) and Autonomous Vehicles (AVs)
Martin Strohmeier, Maria Assunta Cappelli, Giovanna Di Marzo Serugendo, Anne-Francoise Cutting-Decelle, 6th International Workshop on Critical Automotive Applications: Robustness & Safety.

Think Before You Type: A Study of Email Exfiltration Before Form Submission
Asuman Senol, Acar Dunes, Mathias Humbert, SecWeb Workshop.

August

SLAP: Improving Physical Adversarial Examples with Short–Lived Adversarial Perturbations
Giulio Lovisotto, Henry Turner, Ivo Sluganovic, Martin Strohmeier, Ivan Martinovic, 30th Usenix Security Symposium.

LocaRDS: A Localization Reference Data Set
Matthias Schäfer, Martin Strohmeier, Mauro Leonardi, Vincent Lenders, Sensors 2021, Volume 21, 5516.

5G System Security Analysis
Gerrit Holtrup, William Lacube, Dimitri Percia David, Alain Mermoud, Gérôme Bovet, Vincent Lenders, arXiv.

June

Orbit-based Authentication Using TDOA Signatures in Satellite Networks,
Eric Jedermann, Martin Strohmeier, Matthias Schäfer, Jens B. Schmitt, Vincent Lenders, 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Abu Dhabi, UAE.

On Jamming Attacks in Crowdsourced Air Traffic Surveillance,
Mauro Leonardi, Martin Strohmeier, Vincent Lenders, IEEE Aerospace and Electronic Systems , Volume 36, Issue 6.

Secure Crowdsensing Platforms Through Device Behavior Fingerprinting
Pedro Miguel Sanchez Sanchez, Gregorio Martinez Perez, Alberto Huertas, Gérôme Bovet, Burkhard Stiller, Cybersecurity Research National Conferences (JNIC).

May

You talkin' to me? Exploring Practical Attacks on Controller Pilot Data Link Communications
Joshua Smailes, Daniel Moser, Matthew Smith, Martin Strohmeier, Vincent Lenders and Ivan Martinovic, 7th ACM Cyber-Physical System Security Workshop (CPSS).

Towards an AI-powered Player in Cyber Defense Exercises
Roland Meier, Artūrs Lavrenovs, Kimmo Heinäaro, Luca Gambazzi, Vincent Lenders, 13th International Conference on Cyber Conflict (CyCon).

In the Same Boat: On Small Satellites, Big Rockets, and Cyber-Trust
James Pavur, Martin Strohmeier, Vincent Lenders, Ivan Martinovic, 13th International Conference on Cyber Conflict (CyCon).

Flying in Private Mode: Understanding and Improving the Privacy ICAO Address Programme
Martin Strohmeier, Michel Guillaume, Journal of Aerospace Information Systems, Volume 18, Issue 8.

Learning the unknown: Improving modulation classification performance in unseen scenarios
Gérôme Bovet, Erma Perenda, Sreeraj Rajendran, Sofie Pollin, Mariya Zheleva, IEEE INFOCOM.

MARTA: Leveraging Human Rationales for Explainable Text Classification
Ines Arous, Ljiljana Dolamic, Jie Yang, Akansha Bhardwaj,Giuseppe Cuccu, Philippe Cudré-Mauroux, Proceedings of the AAAI Conference on Artificial Intelligence, Volume 35, Issue 7.

SafeAMC: Adversarial training for robust modulation recognition models
Javier Maroto, Gérôme Bovet, Pascal Frossard, arXiv.

April

On the benefits of robust models in modulation recognition
Javier Maroto, Gérôme Bovet, Pascal Frossard, SPIE, Conference on Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications III.

March

Blockchain in Cyberdefence: A Technology Review from a Swiss Perspective
Luca Gambazzi, Patrick Schaller, Alain Mermoud, Vincent Lenders, arXiv.

A Survey on Device Behavior Fingerprinting: Data Sources, Techniques, Application Scenarios, and Datasets
Pedro Miguel Sanchez Sanchez, José Marıa Jorquera Valero, Alberto Huertas Celdran, Gérôme Bovet, Manuel Gil Pérez, and Gregorio MartÌnez Pérez, IEEE Communications Surveys & Tutorials, Volume 23, Issue 2.

Graph Unlearning
Min Chen, Zhikun Zhang, Tianhao Wang, Michael Backes, Mathias Humbert, Yang Zhang, arXiv.

February

QPEP: An Actionable Approach to Secure and Performant Broadband From Geostationary Orbit

James Pavur, Martin Strohmeier, Vincent Lenders, Ivan Martinovic, Network and Distributed System Security Symposium (NDSS).

Crowdsourced Air Traffic Data from the OpenSky Network 2019–20

Martin Strohmeier, Xavier Oliver, Jannis Lübbe, Matthias Schäfer, Vincent Lenders, Earth System Science Data.

13.2 Student Research

CYD Fellows

Postdoc

Dr. **Andrei Kucharavy**	*Evolutionary Dynamics for Improved GAN Detection*	EPF Lausanne
Dr. **Dimitri Percia David**	*Technology Forecasting and Market Monitoring for Cyber-Defence*	University of Geneva

PhD

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*	EPF Lausanne

Master

Adalsteinn Jonsson	*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*	EPF Lausanne
Louis Merlin	*Recovering Type Information from Compiled Binaries to Aid in Instrumentation*	EPF Lausanne
Anita Mezzeti	*Modelling Portfolios of Cyber-Related Emerging Technologies: a Complex-System Approach*	EPF Lausanne
Zuowen Wang	*Understanding and Enhancing Adversarial Robustness for Machine Learning Models*	ETH Zurich

Students and Interns

Silvio Geel	*Security and Privacy of the BGAN Satellite Network*	Master Thesis, ETH Zurich
Dominique Portenier	*A Mode-S Uplink Spoofer for TCAS Testing*	Master Thesis, ETH Zurich
Pedro Miguel Sanchez	*Identical IoT device identification via hardware fingerprinting*	PhD, University of Murcia
Marco di Nardo	*Hacking Cars using the Digital Audio Broadcast*	Master Thesis, ETH Zurich
Boya Wang	*A Security analysis of FLARM*	Master Thesis ETH Zurich
Georg Baselt	*Safety and Privacy Issues of Satellite Communication in the* Aviation Domain	Bachelor Thesis ETH Zurich
Julian Huwyler	*QPEP in the Real World: Implementation of a Secure Satellite Communications Channel (QPEP)*	Master Thesis ETH Zurich
Philippe Panhaleux	*Development of a Distance Bounding Implementation for the Traffic Collision Avoidance System*	Master Thesis ETH Zurich
Jannik Brun	*Exploring Optimal Methods for Generating High-Precision Timestamps from Satellite Communication*	Master Thesis ETH Zurich
Leeloo Granger	*Wireless Attack Evaluation in a Cyber Avionics Lab*	Bachelor Thesis ETH Zurich
Benno Schneeberger	*Identifying IoT devices in the IPv6 address space*	Master Thesis ETH Zurich

Florian Lerch	*Adversarial Attacks on Sensors and ML Systems*	Master Thesis ETH Zurich
Michael Karpf	*High-Precision Timestamp Estimation from Satellite Communication Signals*	Master Thesis ETH Zurich
Adrien Prost	*Privacy-Preserving Intrusion Detection*	Master Thesis EPF Lausanne
Edoardo Debenedetti	*GAN-Leaks 2: Model Updates Edition*	Master Thesis EPF Lausanne
Ejub Talovic	*Aircraft fingerprinting using ADS-B messages*	Master Thesis EPF Lausanne
Etienne Bonvin	*Investigating Privacy Risks in Aggregated* Electromagnetic Spectrum: *Analysis of Electrosens*	Master Thesis EPF Lausanne
Eric Jollès	*Machine Learning for Intrusion Detection Systems*	Master Thesis EPF Lausanne
Stéphanie Lebrun	*GNSS positioning security: overview and anomaly detection on reference stations*	Master Thesis EPF Lausanne
Valérian Rey	*Behavior Fingerprinting of IoT Devices using Federated Learning*	Master Thesis EPF Lausanne
Valentina Pavliv	*Analyzing Personal Information Leakage from Mobile Applications Traffic*	Master Thesis EPF Lausanne
Victor Cochard	*Investigating Graph Embeddings for Cross-Platform Binary Vulnerability Detection*	Master Thesis EPF Lausanne

14 Communication

@Cyber-Defence Campus

@cydcampus

Web Communications

- 20.12.2021, Successful cooperation between the Cyber-Defence Campus and the German Federal Office for Information Security (BSI)
- 02.11.2021, Research associate at the CYD Campus receives professorship at the University of Lausanne
- 06.10.2021, Could artificial intelligence automatically detect fake news?
- 30.09.2021, Meet the finalists of the Cyber Startup Challenge 2021
- 08.09.2021, Cyber-Defence Campus Conference 2021
- 27.07.2021, The CYD Campus demonstrates new forms of attack against critical infrastructures
- 23.07.2021, Cyber-Defence Campus researchers receive Best Paper Award
- 23.06.2021, The Cyber-Defence Campus finds a critical security vulnerability in VPN software
- 10.06.2021, Call for the Cyber Startup Challenge 2021
- 25.05.2021, The Cyber-Defence Campus at the NATO CyCon Conference in Tallinn, Estonia
- 21.05.2021, Cyber-Defence Campus powers innovation

Press Releases

- 20.12.2021, Cyber-Defence Campus: International cooperation with the German Federal Office for Information Security
- 30.09.2021, «Cyber Startup Challenge 2021»: Startup company Decentriq convinces jury
- 25.05.2021, Research Projects of the Cyber-Defence Campus DDPS at the NATO Cyber Conflict Conference
- 22.03.2021, Neues Team beim Cyber-Defence Campus VBS zur Detektion von Software-Schwachstellen (german)

Armafolio

- December edition, Künstliche Intelligenz im Einsatz gegen Desinformation in sozialen Netzwerken (german)

Media

- 15.10.2021, Der Schlüssel für eine effektive Cyber Defence liegt im Teamwork, Smart Media, distribution channel Tagesanzeiger (german)

15 Outlook 2022

In the coming year, the CYD Campus will further expand its collaboration with universities and the private sector, particularly in the areas of digitalization, artificial intelligence and innovation. The DDPS, but also the entire federal administration, is facing major technological challenges in these three areas. The following developments and planned activities of the CYD Campus, which are to be implemented in 2022 in accordance with the Cyber DDPS strategy, are also worth mentioning:

- Raise the CYD Campus to the level of the national technical competence network for cyberdefense with universities and industry. Particularly, support shall be expanded to federal agencies outside the DDPS that are engaged in the cyber domain, such as critical infrastructure operators.
- Assisting in the development of the Cyber Command. Most notably regarding the Cyber Training Center (CTC), Mobile Cyber Means (MCM), Pre-Service Training, and the Cyber Lehrgang.
- Further development of an automated technology radar (TMM 2.0), which uses existing databases, websites and directories to identify trends and technologies at an early stage and assess their importance for Switzerland. This tool will be used to support the scouting and monitoring activities of the CYD Campus, but also to better manage Switzerland's security-relevant technology and industry base (STIB).
- Expansion of the CYD Campus antenna site Zurich. Due to space constraints, the CYD Campus at ETH Zurich will have to move to larger premises in summer 2022. The new location will provide workspace as well as the possibility to hold seminars and workshops.
- In 2022, a new communication concept is to be implemented. In particular, the CYD Campus website is to be completely redesigned with more content and current news for the cyberdefence community.
- The laboratory infrastructures of the CYD Campus will be further expanded, especially for the projects in the area of 5G security, SATCOM security, electric vehicle security and the Future Internet.
- Further development of the CYD Fellowship program to identify and foster scientific cyber talent as early as possible. A new fellowship for proof-of-concepts is intended to promote the innovative strength of young talents and better integrate them into the innovation processes of the DDPS.
- Deployment of one person to the CCDCoE in Tallinn, Estonia. One CYD Campus employee will be permanently stationed in Tallinn at the CCDCoE starting in 2022 to specifically promote cooperation with NATO in the area of technology and research.

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

More information:

https://cydcampus.ch