Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Federal Department of Defence,
Civil Protection and Sport (DDPS)
armasuisse
Science + Technology

# Cyber-Defence Campus Conference on Cyber Threat & Technology Intelligence

## Tuesday, the 3rd of November 2020

## SwissTech Convention Center, EPFL
## Rue Louis Favre 2, 1024 Ecublens, Schweiz

CYD | CYBER DEFENCE CAMPUS

# About The Event

Criminal hackers have a long history of sharing experiences, tools, and vulnerabilities; this has contributed to the success of major cyberattacks. The goal of this conference is to explore various measures to make co-operation, information sharing and collective intelligence also effective on the defender side.

As early as twenty years ago, the first Information Sharing and Analysis Centers (ISACs) have been established as a central resource for sharing information on cyber threats to critical infrastructure. In the same vein, threat intelligence platforms help organizations aggregate, correlate, and analyze threat data from multiple sources in (almost) real-time to support defensive actions. Open source solutions where also proposed as a counterweight to «black-hat» hackers successfully working together, for instance the MISP Threat Sharing Platform or the Open Threat Exchange (OTX), a crowd-sourced computer-security platform.

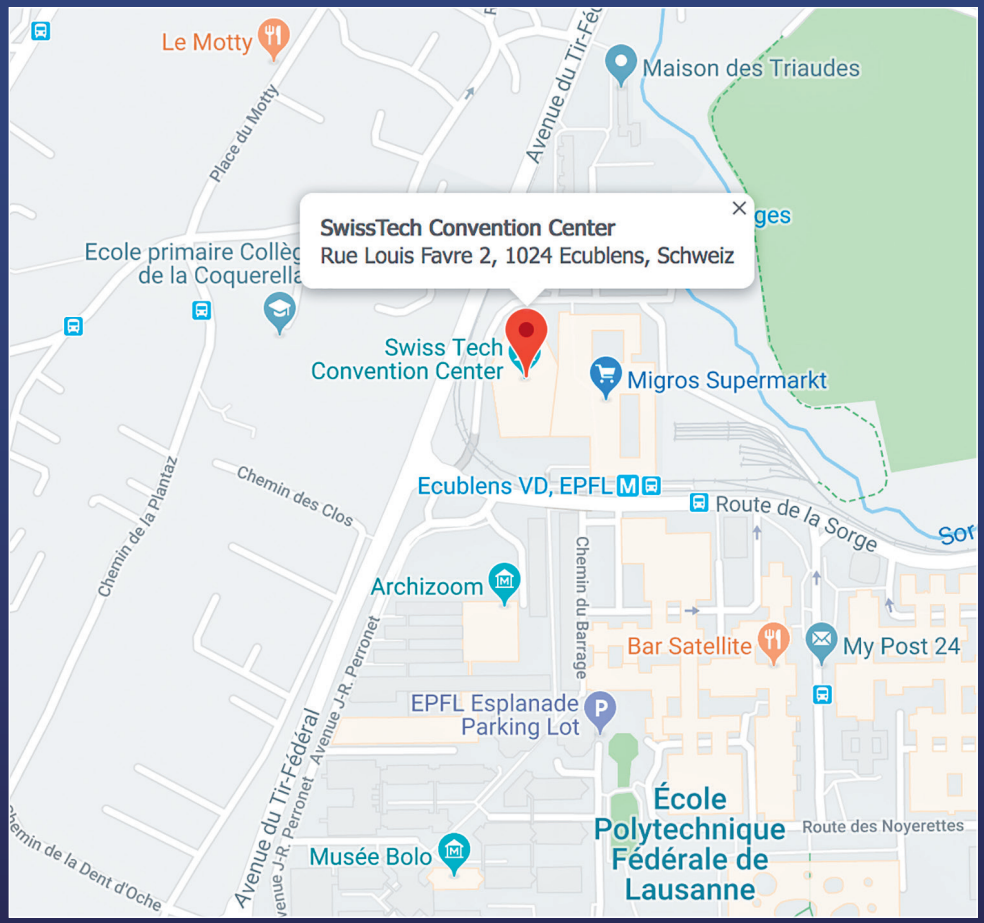
The Cyber Threat Intelligence (CTI) discipline, based on intelligence techniques and methods, aims to collect and filter all relevant information from the cyberspace, in order to draw up portraits of attackers, threats or technological trends (sectors of activity affected, methods used, etc.). CTI sources include open source intelligence, social media intelligence, human intelligence, technical intelligence or intelligence from the deep and dark web. Thus, the tools used by large Security Operations Centers (SOCs) produce hundreds of millions of events per day, from endpoint and network alerts to log events, making it difficult to filter down to a manageable number of suspicious events for triage.

All in all, this profiling enables early detection of cyberattacks and better anticipation of cyber-risks. However, a proper threat intelligence approach should be complemented by technology intelligence, an activity that enables organizations to monitor and forecast the technological opportunities and threats that could affect the future growth and survival of their business. As emphasized by the National strategy for the protection of Switzerland against cyber risks (NCS, 2018-2022), an early identification of technological trends constitutes an important aspect for developing the Swiss cyber-defence. In that respect, the CYD Campus cordially invites all stakeholders to bridge the gaps between academia, the industry, and governmental organizations working in the field of cyber-defence.

Program Chair
Dr. Alain Mermoud

armasuisse, Science + Technology
Cyber-Defence Campus

# Location of the Event




**SwissTech Convention Center**
**Rue Louis Favre 2**
**1024 Ecublens**
**Schweiz**

**Car Park: Parking les arcades**

**A block of rooms have been reserved for our conference at the Starling Hotel Lausanne. The special room rate (195.– CHF incl. breakfast) will be available until the 1st of October or until the group block is sold-out, whichever comes first.**
**You can book your room here:**
**https://bit.ly/conferencehotelcydcampus**
**Code: CYDCAMP**

# Conference Program
# Tuesday, the 3rd of November

| | |
|---|---|
| 08.30 | **Registration open – Welcome Coffee** |
| 09.00 | **Welcome & Overview**<br>**Dr. Thomas Rothacher,** armasuisse Science and Technology (S+T), Director<br>**Dr. Alain Mermoud,** armasuisse S+T, Head of Technology Monitoring and Forecasting, CYD Campus |
| 09.15 | **Welcome from EPFL**<br>**Prof. Edouard Bugnion,**<br>Vice-President for Information Systems, EPFL |
| 09.30 | **Cyber-Defence Campus Updates**<br>**Dr. Vincent Lenders,** armasuisse S+T, Director CYD Campus |
| 09.45 | **TBD**<br>**Major General Alain Vuitel,** Head of Armed Forces Command Support Organisation |
| 10.30 | **Coffee Break – Networking** |
| 11.00 | **The Swiss Approach to National Cyber Security**<br>**Florian Schütz,** Federal Cyber Security Delegate<br>Head of National Cyber Security Centre |
| 11.30 | **TBD**<br>**Marc Henauer,** MELANI Operation and Information Centre (OIC) |
| 12.00 | **Lunch with demo/poster session** |
| 13.30 | **Technology Landscape Monitoring:**<br>**A Data Integration Challenge (provisional)**<br>**Prof. Karl Aberer,** Head of Distributed Information System Laboratory, EPFL |
| 14.00 | **Peeking into the Future of Quantitative Threat Intelligence and Technology Forecasting for Cyber-Defence**<br>**Dr. Thomas Maillart,** Senior Researcher at University of Geneva<br>**Dr. Dimitri Percia David,** Post-doc at University of Geneva |
| 14.45 | **Coffee Break – Networking** |
| 15.15 | **MISP Threat Sharing – a decade of successes and failures in Threat Information Sharing**<br>**Christophe Vandeplas,** Malware and Forensic Analyst at NATO |
| 15.45 | **AWK technology radar: a methodology for evaluating security technologies**<br>**Dr. Adrian Marti,** Head of Cyber Security & Privacy at AWK |
| 16.15 | **Cyber-security startup competition**<br>**Dr. Colin Barschel,** armasuisse S+T, Director of Industry Relations, CYD Campus |
| 17.00 | **Wrap-up** |

# Speakers

**Dr. Thomas Rothacher**
**Director of armasuisse Science+Technology, Thun**
**Deputy National Armaments Director**
Thomas Rothacher is Director of Science and Technology at armasuisse, the Federal Office of Defence Procurement. He has done his MSc and PhD in physics at the University of Berne. Rothacher also holds an Executive MBA from the University of St. Gallen and was studying at the Naval Postgraduate School in Monterey, CA. As board member of armasuisse and national research director, he is responsible for supporting the Swiss armed forces in the procurement of complex technical systems and for the national military research programs in the fields of reconnaissance and surveillance, communication, information security, protection and safety and unmanned mobile systems/robotics.

**Dr. Alain Mermoud**
**armasuisse S+T, Head of Technology Monitoring and Forecasting, CYD Campus**
Alain Mermoud is the Head of Technology Monitoring and Forecasting at the Cyber-Defence Campus. His main research interests are in the area of emerging technologies, disruptive innovations, (cyber) threat intelligence and the economics of (cyber) security. In 2019, he earned his PhD in Information Systems from HEC Lausanne. His PhD research focused on security information sharing and cooperation in the context of critical infrastructure protection. In 2015, he won the Cyber 9/12 Atlantic Council Strategy Challenge as head of team Switzerland. Prior to that, he worked 5+ years in the banking industry and as Lecturer at ETHZ. Alain Mermoud earned his MSc in Business Administration and his BSc in Information Science from the University of Applied Sciences Western Switzerland as a Hirschmann-scholarship holder and obtained a MBA in Strategic Management and Business Intelligence from the Ecole de Guerre Economique in Paris. He also holds a militia Intelligence Officer position in the Military Intelligence Service of the Swiss Armed Forces with the rank of Captain on active-duty.

**Edouard Bugnion**
**Vice-President for Information Systems, EPFL**
Edouard Bugnion joined EPFL in 2012, where his focus is on datacenter systems. His areas of interest include operating systems, datacenter infrastructure (systems and networking), and computer architecture. Before joining EPFL, Edouard spent 18 years in the US, where he studied at Stanford and co-founded two startups: VMware and Nuova Systems (acquired by Cisco). At VMware from 1998 until 2005, he played many roles including CTO. At Nuova/Cisco from 2005 until 2011, he helped build the core engineering team and became the VP/CTO of Cisco's Server, Access, and Virtualization Technology Group, a group that brought to market Cisco's Unified Computing System (UCS) platform for virtualized datacenters.
Prof. Bugnion is a Fellow of the ACM. Together with his colleagues, he received the ACM Software System Award for VMware 1.0 in 2009. His paper Disco: Running Commodity Operating Systems on Scalable Multiprocessors» received a Best Paper Award at SOSP ‹97 and was entered into the ACM SIGOPS Hall of Fame Award in 2008. At EPFL, he received the OSDI 2014 Best Paper Award for his work on the IX dataplane operating system.

**Dr. Vincent Lenders**
**Head of Cyber-Defence Campus, armasuisse S+T**
Vincent Lenders is the Director of the Cyber-Defence Campus and head of the Cyber Security and Data Science Department at armasuisse Science and Technology. He is also the cofounder and chairman of the executive boards at the OpenSky Network and Electrosense associations. He graduated with a Msc and PhD degree in Electrical Engineering and Information Technology from ETH Zurich and was also Postdoctoral Researcher at Princeton University. He has led during eight years the Swiss military research program on «Cyberspace and Information» and he was Industrial Director of the Zurich Information Security and Privacy Center (ZISC) at ETH Zurich from 2012 to 2016. His research work has appeared in more than 120 publications at peer-reviewed international conferences and journals and has received various best paper awards.

**Major General Vuitel**
**Head of Armed Forces Command Support Organisation**
Major General Vuitel is responsible for the Command Support Organisation of the Swiss Armed Forces. He is responsible for the command and control capabilities of the armed forces and the national crisis management, Cyber Defence and electronic operations as well as the agencies that run the IT and communications technology in the administration of the DDPS and the armed forces. He answers directly to the Chief of the Armed Forces. The Head of Armed Forces Command Support Organisation is in charge of Command Support Brigade 41.

**Florian Schütz**
**Federal Cyber Security Delegate**

Florian Schütz has an MA in Computer Science and a Master of Advanced Studies in Security Policy and Crisis Management from the ETH Zurich. Through his professional activity of more than eight years at RUAG Switzerland Ltd, including as Head of Cyber Security, he gained comprehensive insights into the processes and working methods of a company affiliated with the federal government, as well as the Federal Administration in general. During this time, Florian Schütz was also deployed to Israel for one year in the Business Development Cyber & Intelligence sector, where he gained significant experience and knowledge in one of the most dynamic and worldwide leading locations for all aspects of cyber security. Thanks to his last position as Head of IT Risk & Security at Zalando SE, Florian Schütz also has extensive experience in the private sector. He led a team of about 30 employees there.

**Marc Henauer**
**Head of MELANI OIC**

Marc Henauer is since 2010 the Head of the MELANI Operation and Information Centre (OIC). This unit is part of the Federal Intelligence Service within the Swiss Ministry of Defence, Civil Protection and Sports. The MELANI OIC Unit is responsible for the analytical and operative parts of the Swiss Analysis and Reporting Unit for Information Assurance (MELANI), as well as for establishing the Situational Picture on Cyber-Threats. MELANI's mandate lays with supporting the Swiss Critical Infrastructures within their Information Assurance Process. Strategic analyst for economic and cyber criminality within the Service of Analysis and Prevention from 2001 to 2003, before heading MELANI and part of the Cybercrime Coordination Unit (CYCO) from 2003 to 2009. Studied at the University of Zurich Economic Science, as well as Media and Communication Management at the University of St. Gallen. Master of Arts in Foreign Service (National Security Studies) from the Georgetown University in Washington DC in 1999.

**Prof. Dr. Karl Aberer**
**Head of Distributed Information Systems Laboratory, EPFL**

Karl Aberer is a full professor for Distributed Information Systems at EPFL since 2000. Karl Aberer received his Ph.D. in mathematics in 1991 from the ETH Zurich. From 1991 to 1992 he was postdoctoral fellow at the International Computer Science Institute (ICSI) at the University of California, Berkeley. In 1992 he joined the Integrated Publication and Information Systems institute (IPSI) of GMD in Germany, where he was leading the research division Open Adaptive Information Management Systems. From 2005 to 2012 he was the director of the Swiss National Research Center for Mobile Information and Communication Systems (NCCR-MICS, www.mics.ch). From 2012 to 2016 he was Vice-President of EPFL responsible for information systems. He is co-founder and CEO of LinkAlong, a startup established in 2017 providing analytics capabilities for open source documents based on technologies for knowledge extraction developed in his research.

**Dr. Thomas Maillart**
**Senior Researcher at University of Geneva**

Thomas Maillart aims to investigate, model and enhance human collective intelligence, through better understanding of incentives, structures and dynamics of social interactions online and in the physical world. In particular, Thomas is interested in the danger and opportunities arising from the fast expanding cyberspace. Thomas Maillart holds a Master from EPFL (2005) and a PhD from ETH Zurich (2011). At ETH Zurich, Thomas received the Zurich Dissertation Prize in 2012 for his pioneering work on cyber risks and spent 2 years researching at the ETH Zurich Center for Law and Economics. Before joining the University of Geneva, Thomas Maillart was a post-doctoral researcher at UC Berkeley until 2016. Thomas Maillart co-founded a cybersecurity startup in 2005, and has consulted on cybersecurity for various governmental and private organizations.

**Dr. Dimitri Percia David**
**EPFL Cyber-Defence Campus Distinguished Postdoctoral Fellow**

Dimitri Percia is a postdoctoral researcher at the University of Geneva (supervised by Dr. Thomas Maillart) and an EPFL Cyber-Defence Campus Distinguished Postdoctoral Fellow. His research topics are related to technology forecasting and market monitoring for cyber-defence. By adopting an econophysics approach, he analyses collective intelligence networks and cascading processes in complex systems in order to investigate and model the production-capability networks, the innovation structures and dynamics underlying the hype cycle of technologies. Prior to his current job, Dimitri was a researcher and scientific collaborator at the Military Academy at ETH Zurich, and a data analyst responsible of market-prices forecasting for a commodity trading company. Dimitri holds a PhD degree in Information Systems from HEC Lausanne.

# Cyber Start-up Challenge on Day 1

**Christophe Vandeplas**
**Malware and Forensic Analyst at NATO**
Christophe Vandeplas is the founder of the MISP Threat Sharing project. Today it is the most popular collection of CTI tools, resources and industry standards that foster Threat Information sharing. It is used around the globe by many governments, industry, financial sector, but also by hobbyists. Its open source development is performed and has been funded by many organizations, including CIRCL and the European Union, and the project has more than 140 unique contributors. Christophe has also contributed to the organisation the FOSDEM and BruCON during many years and regularly presents at various Cyber Security conferences around Europe. The NATO Cyber Security Centre where he supports Incident Response, Malware & Forensic analysis, Threat Hunting and CTI related matters currently employs him.

**Dr. Adrian Marti**
**Head of Cyber Security & Privacy at AWK**
Adrian Marti has been with AWK Group since 2001. He has led the cyber security practice since 2008. Since 2018, he is the chief information security officer (CISO) of AWK Group. Adrian Marti has 20 years of experience in the consulting business. As part of his successful professional practice, he built the cyber security & Privacy portfolio of AWK Group. He led numerous in-formation security projects on a strategic, conceptual and implementation layer in the public and private sector. Adrian Marti started his professional career with a degree and doctorate in experimental physics from the University of Bern. In 1996 he graduated from the William E. Simon School of Business Administration with an Executive MBA. In addition, Adrian Marti obtained various certifications in the field of information security: CISSP, CISM, CRISC, lead author ISO 27001. Adrian Marti has been appointed as a partner at AWK Group on July 1st, 2020.

**Dr. Colin Barschel**
**Scientific Project Manager, Cyber-Defence Campus, armasuisse**
Colin Barschel studied physics at the RWTH Aachen University in Germany, where he also obtained his Ph.D. in high energy physics. He worked for Ericsson Research on mobile networks and security and at CERN and Liverpool in scientific collaborations. As director of industry relations, Mr. Barschel creates partnerships between armasuisse and industry actors. The objective is to facilitate knowledge transfer and strengthen the R & D efforts on all sides and to translate results into demonstrators and innovative solutions.

**The Cyber-Defence Campus is looking for innovative technologies and explores the startup market by organizing the Cyber Startup Challenge 2020.**

The goal of the challenge is to discover the startup technology landscape around the subject of Cyber Threat Intelligence (CTI) and to bring innovative technologies to the Swiss Armed Forces. Companies are encouraged to register, the best candidate will be selected through an internal selection and will be able to implement its solution.
For this challenge, three startup finalists will pitch their businesses during the conference «Cyber Threat & Technology Intelligence» on November 3rd, 2020 in Lausanne.
A committee will choose one company as the finalist for the Startup Challenge. Finally, the selected startup is awarded a contract of up to CHF 100'000.– to integrate a Proof of Concept of its technology within the Swiss Armed Forces.

**This challenge is not a tender; it serves as market exploration to find promising technologies best suited for the Swiss Armed Forces' demands.**

## What we are looking for

We are looking for novel solutions in CTI that can have a significant impact in the day-to-day operation of the Swiss Armed Forces. The solution will be integrated in the existing infrastructure. The technology does not need to be fully mature yet, but a convincing Proof of Concept should be implementable within a year and with less than CHF 100'000.–.

## Some examples

Below are some examples of CTI technologies of interest; however, we are also looking to discover relevant technology areas:

- Faster threat analysis: finding out how a threat behaves
- Compare binary elements and find similarities
- Aggregate feeds to identify emerging topics (i.e., thread feed from different providers scanned together and identify the same threat with different names)
- Semantic analysis of documents
- Summarize text and identify topics in a hacker forum
- Facilitate the comprehension of texts in another language, including slang
- Analyze network traffic or metadata to identify patterns that correspond to an actor
- Correlation of events and signatures
- Sharing information about cyber threats with different partners («Need to Know» vs. «Need to Share»)

More information and subscription, please visit
**https://bit.ly/startupchallengecydcampus**

# Helpful Information

## Wifi information

The wifi is called **«Free_STCC»**
As soon as you login on this wifi,
you will get redirected with all indications

## Contact before and during the conference

Moo Khelifi
armasuisse
+41 79 156 34 54
monia.khelifi@ar.admin.ch

CYD | CYBER DEFENCE CAMPUS