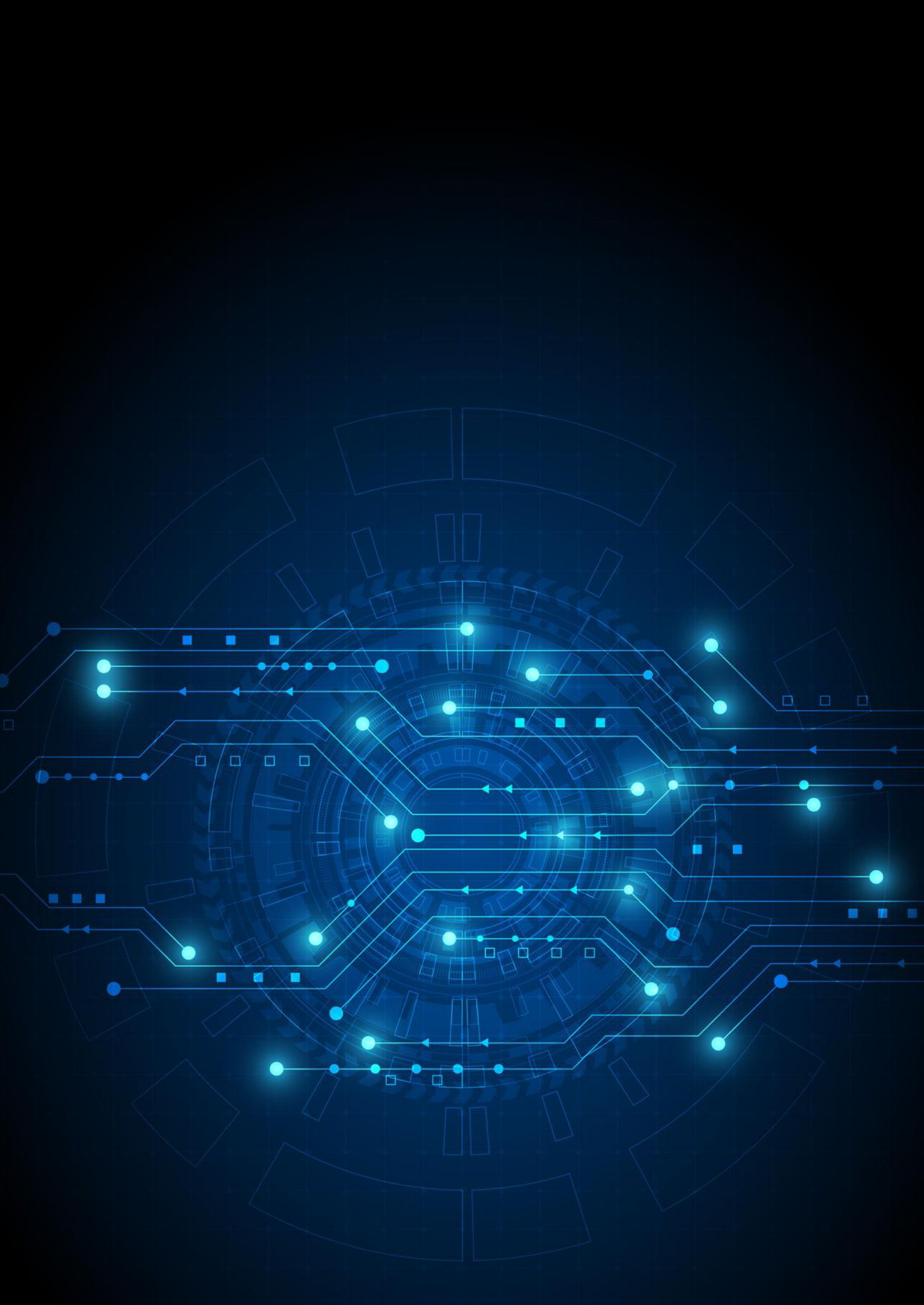
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung
Bevölkerungsschutz und Sport
armasuisse
Wissenschaft und Technologie

Cyber-Defence Campus

Jahresbericht 2022

CYD
CYBER DEFENCE CAMPUS



Inhaltsverzeichnis

IMPRESSUM

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

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

Bildernachweis: Wo nicht anders vermerkt: Quelle VBS/DDPS, Pixabay, Adobe Stock

Vorwort

Das Jahr 2022 war sowohl sicherheitspolitisch wie auch technologisch ein besonderes Jahr. Zu Beginn des Jahres hat Russland die Ukraine militärisch angegriffen. Die Cybervorfälle in Zusammenhang mit der Invasion verdeutlichen, dass Cybermittel zur Unterstützung militärischer Aktionen Normalität geworden sind. Die zunehmende internationale Vernetzung und Interdependenz führt dazu, dass Cyberangriffe grenzüberschreitende Auswirkungen haben und somit auch Schweizer Einrichtungen gefährden können. Gemäss dem Zusatzbericht 2022 zum «Sicherheitspolitischen Bericht 2021» muss in einer eskalierenden Situation mit direkten Cyberangriffen gegen Ziele in der Schweiz gerechnet werden.
Zwei Monate nach der Invasion in der Ukraine stellte die Schweizer Armee die «Gesamtkonzeption Cyber» vor. Dieses Konzept zeigt auf, wie die Armee ihre Fähigkeiten im Cyber-Bereich weiterentwickeln soll. Die Armee muss in der Lage sein, sich zu schützen und Bedrohungen aktiv abzuwehren. Die Umsetzung der Strategie wird schrittweise erfolgen, mit dem Aufbau eines Cyber Kommandos im Jahr 2024 und bis in die 2030er Jahre dauern.
Im Dezember hat der Bundesrat entschieden ein neues Bundesamt für Cybersicherheit im VBS zu gründen. Das geplante Bundesamt soll eine nationale Melde- und Anlaufstelle zu Cyberangriffen bereitstellen, Informationen und Warnungen verbreiten und die Bevölkerung für den Schutz vor Angriffen aus dem Netz sensibilisieren und die zudem die Bundesverwaltung vor Cyberangriffen schützen.

2022 war auch ein bahnbrechendes Jahr für Entwicklungen im Bereich der künstlichen Intelligenz. Das Unternehmen OpenAI hat zwei KI-basierte Systeme, DALL-E 2 und ChatGPT, vorgestellt, die in der Lage sind, automatisch Bilder bzw. Texte in so hoher Qualität zu generieren, dass sie menschlichen Fähigkeiten nahekommen. Die Auswirkungen für die Cyber-Defence, den CYD Campus und die Gesellschaft im Allgemeinen sind erheblich. Wie Bundesrätin Viola Amherd an der REAIM-Konferenz 2023 in Den Haag betonte, kann der Einsatz von künstlicher Intelligenz in der Verteidigung viele Möglichkeiten bieten, gleichzeitig müssen aber auch Risiken und ethische Aspekte berücksichtigt werden.
Beim CYD Campus hat sich im Jahr 2022 viel bewegt. Rückblickend haben wir im vierten Jahr seit der Gründung des CYD Campus bedeutende Fortschritte gemacht. So hat sich beispielsweise die Zahl der Partnerorganisationen, die mit dem CYD Campus zusammenarbeiten, auf mehr als 60 erhöht. Es freut mich ganz besonders, dass wir die Zahl der Studienplätze ausbauen konnten. Im 2022 konnten 13 Studierende von Schweizer Universitäten als CYD Fellows ihre Forschungsarbeit durchführen und weitere 39 Studierende absolvierten im Rahmen des Talentförderungsprogramms am CYD Campus ein Hochschulpraktikum oder eine Masterarbeit. Die Schweizer Cyber Community konnten wir dank unseren Anlässen wie die CYD Campus Konferenz in Bern, den Cyber Alp Retreat in Sachseln, die durchgeführten Hackathons, oder die Cyber Startup Challenge und Jam Sessions effektiv vernetzen und deutlich stärken. Ausserdem ist es gelungen, die internationale Zusammenarbeit zu intensivieren, indem wir zum Beispiel einen unserer Cyber-Experten für drei Jahre an das NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estland, entsenden konnten.
In Zürich wurde im November zusammen mit der ETH Zürich und unseren Industriepartnern die neuen Räumlichkeiten des CYD Campus an der Zollstrasse 62 eingeweiht, die uns deutlich mehr Raum für die gemeinsame Durchführung von Projekten und Veranstaltungen mit unseren Partnern bieten. Alleine im Jahr 2022 wurden standortübergreifend über 50 Projekte durchgeführt und über 30 wissenschaftliche Publikationen veröffentlicht. Ein Höhepunkt war zum Beispiel der Aufbau eines nationales Testbeds für Netzwerksicherheit, welches die drei CYD Campus Standorte (Thun, Lausanne und Zürich) über die neuartige SCION-Technologie der ETH Zürich vernetzt.
Diese erfreulichen Entwicklungen tragen zu unserer Mission bei: Die Verbesserung der Cyberverteidigung in der Schweiz.

Der vorliegende Jahresbericht gibt Auskunft über die öffentlichen, nicht klassifizierten Aktivitäten des CYD Campus im Jahr 2022. Ich wünsche Ihnen eine spannende Lektüre.

Thun, 31. Januar 2023

Dr. Vincent Lenders
Leiter Cyber-Defence Campus

1 Über den Cyber-Defence Campus

1.1 Strategieeinbettung und Schlüsselaufgaben

Aufgrund des sich wandelnden Ökosystems und der steigenden Bedrohung durch Cyberattacken in allen Lebensbereichen hat die Schweizer Regierung die Cybersicherheit zu einem zentralen und nationalen Sicherheitsanliegen erklärt. Das Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) verstärkt den Einsatz von Ressourcen für die Cyberverteidigung und macht sie zu einer strategischen und operativen Priorität. Aus diesem Grund entstand im Jahr 2016 der erste Aktionsplan für Cyberdefence (APCD). Angesichts der rasanten Weiterentwicklung der Cyber-Bedrohungslage in den letzten fünf Jahren wurde für den Zeitraum 2021-2024 eine neue «Strategie Cyber VBS» erarbeitet, die auf dem Aktionsplan aufbaut. Sowohl der Aktionsplan als auch die neue «Strategie Cyber VBS» sind auf die übergeordnete Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) abgestimmt.

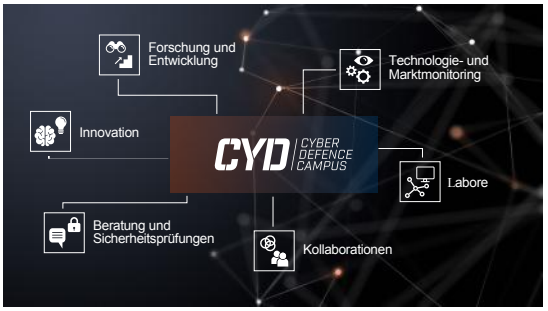
Strategie Cyber VBS 2021 - 2024

Als Teil des APCD und der «Strategie Cyber VBS» wird im VBS seit vier Jahren der Cyber-Defence (CYD) Campus entwickelt und betrieben. Er ist beim Bundesamt für Rüstung (armasuisse) angesiedelt. Der CYD Campus bietet dem VBS eine Antizipations- und Wissensplattform zur Identifikation und Bewertung technologischer, wirtschaftlicher und gesellschaftlicher Cyber-Trends. Um möglichst eng mit den Hochschulen, dem VBS und der Industrie zusammenarbeiten zu können, ist der CYD Campus an drei Standorten vertreten: Am Hauptstandort Thun (armasuisse Wissenschaft und Technologie), im Innovationspark an der EPFL in Lausanne und seit diesem Jahr neu and der Zollstrasse 62 in Zürich. Dies erlaubt es ihm, gemäss den Bedürfnissen der Schweizerischen Eidgenossenschaft, effizient Know-how aufzubauen und Cyber-Expertise bereitzustellen. Gerade der neue Standort in Zürich erlaubt es dem CYD Campus, durch die grösseren Räumlichkeiten einen idealen Raum für Kollaboration zu schaffen sowie Platz für neue Talente zu bieten.

Der CYD Campus wirkt dementsprechend als Bindeglied zwischen der Industrie, der staatlichen Verwaltung und der Wissenschaft. In der Ausrichtung der «Strategie Cyber VBS» legt die Chefin VBS, Bundesrätin Viola Amherd, die Handlungsfelder und die entsprechenden Aufgabenverteilungen fest. Der CYD Campus hat heute folgende drei Schlüsselaufgaben:

Früherkennung von Trends im Cyber-Bereich: Dies beinhaltet ein umfassendes Technologie- und Marktmonitoring, ein internationales Scouting von Startups und die Pflege eines Kooperationsnetzwerks.

Forschung und Innovation von Cyber-Technologien: Durch die Zusammenarbeit mit Hochschulen und der Industrie werden aufkommende Cyberrisiken identifiziert und innovative Lösungen entwickelt, um Bedrohungen im Cyber-Raum wirksam zu begegnen. Ausserdem ist es das Ziel des CYD Campus, die Sicherheit und Resilienz der bestehenden Cyber-Systeme zu gewährleisten und zu erhöhen.



Kernkompetenzen des Cyber-Defence Campus

Ausbildung von Cyberspezialistinnen und -spezialisten: Beim CYD Campus werden Talente auf Master-, PhD- und Postdoc-Stufe sowie Hochschulpraktikantinnen und Hochschulpraktikanten für zukünftige Herausforderungen ausgebildet. Zudem definieren und betreuen Experten des CYD Campus zahlreiche studentische Projekte.

Das Ziel dieses Jahresberichts ist es, Einblicke in die Umsetzung der oben genannten Schlüsselaufgaben im Jahr 2022 des Cyber-Defence Campus zu gewähren. Dabei wird ein kurzer Überblick über das CYD Campus Team sowie über einige Highlights des Jahres 2022 gegeben. Die öffentlichen Tätigkeiten im Rahmen von Forschungsprojekten, Kundenaufträgen und Demonstratoren werden ebenfalls erläutert. Weiter werden die Arbeiten im Jahr 2022 in Bezug auf die Erweiterung der Laborinfrastrukturen thematisiert und Tätigkeiten des Technologie- und Marktmonitorings vorgestellt. In den letzten Kapiteln dieses Berichts wird ein Überblick über Veranstaltungen, Publikationen, Referate sowie einen Ausblick auf das Jahr 2023 gewährt.

1.2 Partner

Der CYD Campus ist organisatorisch im VBS bei armasuisse Wissenschaft und Technologie angesiedelt. Rund 60 weitere inländische und ausländische Organisationen aus Wissenschaft, Industrie und dem öffentlichen Sektor wirken als Partner mit.

Bund	Hochschulen	Industriepartner
National		
Bundespolizei fedpol	Berner Fachhochschule (BFH)	Adnovum
Bundesamt für Statistik BFS	Ecole polytechnique fédérale de Lausanne (EPFL),	Anapaya
Bundesamt für Zivilluftfahrt BAZL	Center for Digital Trust (C4DT)	Astrocast
Eidgenössisches Departement für auswärtige Angelegenheiten EDA	Eidgenössische Technische Hochschule Zürich (ETHZ)	Brunner Elektronik AG
Nachrichtendienst des Bundes NDB	Fachhochschule Nordwestschweiz (FHNW)	CYSEC
Nationales Zentrum für Cybersicherheit NCSC	Haute Ecole du Paysage, d'Ingénierie et d'Architecture de Genève (HEPIA)	Decentriq
Schweizer Armee	HES-SO Valais-Wallis	FLARM Technology
Swisstopo	Hochschule Luzern (HSLU)	IBM Research
Swissnex	Hochschule für Wirtschaft und Ingenieurwissenschaften des Kantons Waadt (HEIG-VD)	Kudelski Security
	Militärakademie an der ETH Zürich	Noser Engineering
	Ostschweizer Fachhochschule (OST)	RUAG
	Scuola universitaria professionale della Svizzera italiana (SUPSI)	Swisscom
	Universität Freiburg	Tune Insight
	Universität Genf	
	Universität Lausanne	
	Universität Neuchâtel	
	Universität St. Gallen	
	Universität Zürich	
	Zürcher Hochschule für Angewandte Wissenschaften (ZHAW)	
	Zurich Information Security and Privacy Center (ZISC)	
International		
Bundesamt für Sicherheit in der Informationstechnik (BSI), DE	KU Leuven, BEL	Countercraft
European Defence Agency EDA	TU Kaiserslautern, DE	CybExer Technologies
KRITIS	IMDEA, ESP	Onekey
Luxemburgische Armee	Universität Luxemburg	Plug and Play
NATO CCDCOE	Universidad de Murcia, ESP	Sero Systems
US Department of Defense	Universidad Rey Juan Carlos, ESP	
	University of Oxford, UK	
	University of Southern California (USC), USA	
	Northeastern University, USA	

Liste aller Partner des Cyber-Defence Campus 2022

1.3 Personen

Die Leitung des CYD Campus besteht aus Mitarbeitenden des Fachbereichs Cyber Sicherheit und Data Science von armasuisse W+T.

CYD Campus Leitung

Dr. Vincent Lenders

Leiter des CYD Campus und Fachbereichsleiter

Dr. Bernhard Tellenbach

Leiter Forschungsprogramm Cyberspace und Gruppe Cybersicherheit

Stefan Engel

Leiter Business Development und Stellvertretender Leiter des CYD Campus

Dr. Colin Barschel

Leiter Innovation und Industriekollaborationen

Dr. Gérôme Bovet

Leiter Forschungsprogramm und Gruppe Data Science

Dr. Alain Mermoud

Leiter Technologie und Marktmonitoring

Giorgio Tresoldi

Leiter internationale Beziehungen und Scouting

Mitarbeitende Schwerpunkt Cybersicherheit

Dr. Martin Strohmeier ist Experte für die Sicherheit von cyber-physischen Systemen und wissenschaftlicher Projektleiter

Daniel Hulliger ist Pentester, Schwachstellenforscher und technischer Projektleiter

Damian Pfammatter ist Pentester, Schwachstellenforscher und wissenschaftlicher Projektleiter

Llorenç Roma ist Pentester und wissenschaftlicher Projektleiter

Dr. Daniel Moser ist Experte für die Sicherheit von drahtloser Kommunikation, Pentester und wissenschaftlicher Projektleiter.

Dr. Miguel Keer ist wissenschaftlicher Projektleiter

Dr. Roland Meier ist Experte für die Sicherheit von Netzwerken und wissenschaftlicher Projektleiter (Eintritt November 2022)

William Lacube ist zuständig für die Kollaboration mit dem NATO CCDCOE in Estland und wissenschaftlicher Projektleiter

Dr. Carlo Matteotti ist Kryptologe und betreut Studierende und CYD Fellows als CYD Mentor

Mitarbeitende Schwerpunkt Data Science

Dr. Ljiljana Dolamic ist Expertin für Natural Language Processing und wissenschaftlicher Projektleiterin

Dr. Etienne Voutaz ist Data Scientist und wissenschaftlicher Projektleiter

Dr. Metin Feridun ist Big Data Spezialist und wissenschaftlicher Projektleiter (Pensionierung Oktober 2022)

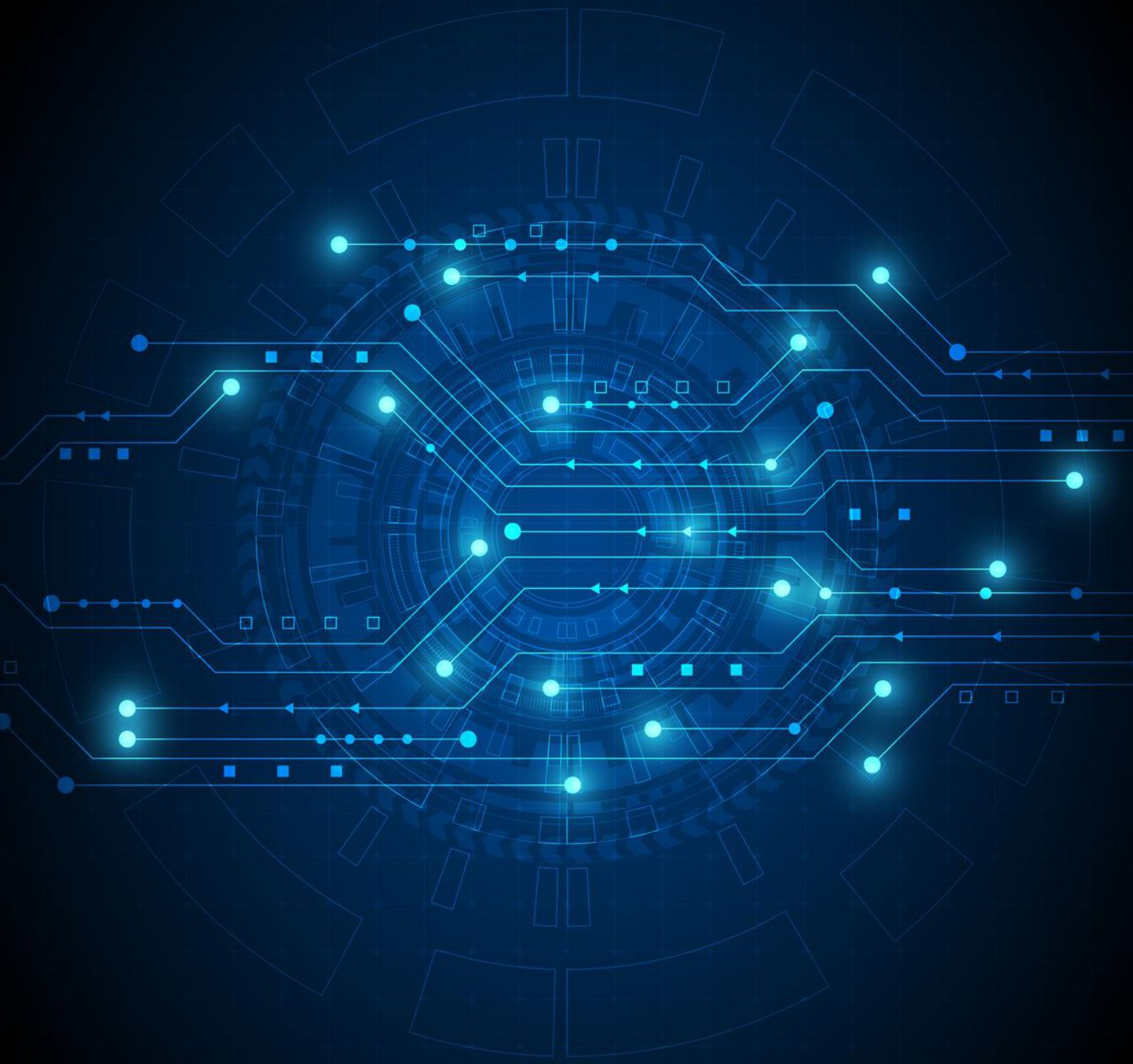
Dr. Albert Blarer ist Data Scientist und wissenschaftlicher Projektleiter

Ivo Stragiotti ist zuständig für Laborinfrastrukturen und technischer Projektleiter

Dr. Raphael Meier ist Experte für Bildverarbeitung und Machine Learning sowie wissenschaftlicher Projektleiter

Dr. Jonas Liechti ist Big Data Spezialist und wissenschaftlicher Projektleiter (Eintritt August 2022)

Dr. Hông-Ân Sandlin ist Expertin für Datenanalyse und Machine Learning sowie wissenschaftliche Projektleiterin (Eintritt Januar 22)



Support

Monia Khelifi

Leiterin Administration und

Event Management

Amina Bouslami

Sachbearbeiterin CYD Campus

Lausanne (ab Juni 2022)

Sarah Frei

Kommunikation und

Sachbearbeiterin CYD Campus

Zürich (ab April 2022)

Hochschulpraktikant/innen

Um die Cyber-Expertise der Studierenden zu erhöhen und die Resilienz der Schweiz gegenüber Cyber-Bedrohungen langfristig zu stärken, bietet der Cyber-Defence Campus Hochschulpraktika an allen drei Standorten in Thun, Lausanne und Zürich an. Im 2022 konnten 27 Studierende ein Praktikum beim Cyber-Defence Campus absolvieren. Die Praktikantinnen und Praktikanten stammen aus verschiedenen Hochschulen.

Perceval Faramaz, November 22 – Oktober 23, Internationale Beziehungen, Lausanne

Francesco Intoci, Oktober 22 – März 23, Cybersicherheit, Lausanne

Louis Leclair, Oktober 22 – März 23, Cybersicherheit, Lausanne

Alessandro Tavazzi, September 22 – Februar 23, Technologie Monitoring, Lausanne

Eric Jedermann, September 22 – Februar 23, Cybersicherheit, Thun

Lucas Crijns, September 22 – Februar 23, Cybersicherheit, Lausanne

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

Marc Egli, September 22 – Februar 23, Cybersicherheit, Lausanne

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

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

Michiel Lüchinger, August 22 – Juli 23, Kommunikation, Thun

Valentin Mulder, Mai 22 – April 2023, Technologie Monitoring, Lausanne

Sarah Ismail, Mai 22 – April 2023, Technologie Monitoring, Lausanne

Johannes Willbold, März 22 – August 22, Cybersicherheit, Thun

Beatrice Dall'Omo, März 22 – August 22, Cybersicherheit, Thun

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

François Burguet, März 22 – August 22, Technologie Monitoring, Lausanne

Jacques Roitel, Februar 22 – Juli 22, Technologie Monitoring, Lausanne

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

Alexander Glavackij, Februar 22 – Dezember 22, Technologie Monitoring, Lausanne

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

Benjamin Killian, September 21 – Februar 22, Cybersicherheit, Lausanne

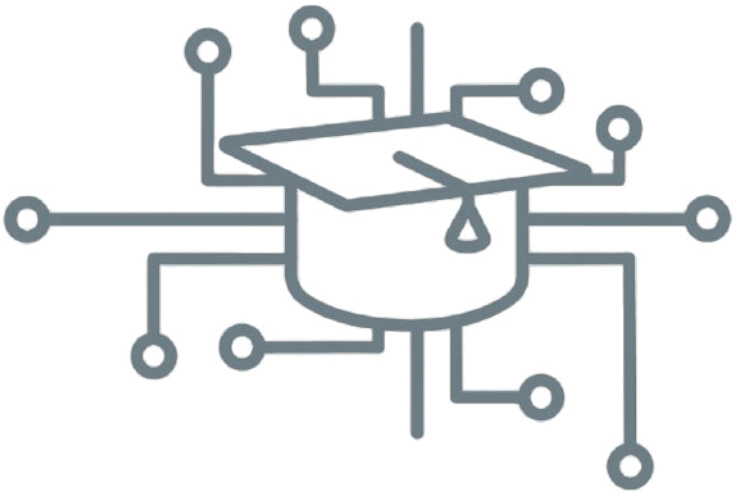
Samad Emrys Durussel, September 21 – Februar 22, Data Science, Lausanne

Huzar Marin, September 21 – Februar 22, Cybersicherheit, Lausanne

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

Michael Tsesmelis, Juni 21 – Mai 22, Technologie Monitoring, Lausanne

Sarah Frei, April 21 - März 22, Kommunikation, Thun



CYD Fellows

Im Jahr 2020 hat der CYD Campus zusammen mit der EPFL ein Cyber-Defence (CYD) Fellowship Programm lanciert, um den Studierenden die Möglichkeit zu geben, sich in Themen der Cyber-Defence zu vertiefen und die Kompetenzen in der Schweiz in diesem zu stärken. Dadurch können die Studierenden bereits während des Studiums einen Forschungsbeitrag für die Cyberabwehr der Schweiz leisten. Bei den CYD Fellowships handelt es sich um ein kompetitives Talentprogramm, das den Studierenden einen CYD Experten beziehungsweise eine CYD Expertin für die Betreuung der Forschungsarbeit zur Seite stellt. Die CYD Fellows sind an einer Schweizer Hochschule immatrikuliert und führen ihre Forschung in den Räumlichkeiten des CYD Campus im EPFL Innovationspark in Lausanne, an der Zollstrasse in Zürich sowie am Hauptsitz in Thun durch. CYD Fellowships werden mehrmals jährlich für Masterstudierende, Doktoranden sowie Postdocs vergeben und gewähren eine Vergütung für die Lebenshaltungskosten. Im Jahr 2022 waren 13 Fellows aktiv:

Jodok Vieli, Master Thesis Fellow, ETHZ, Oktober 22 – März 23, Projekttitel: *Systemization of DNS DoS: Attack Characterization, Mitigation, and Measurement*, CYD Mentor: Dr. Bernhard Tellenbach

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

Louis-Henri Merino, Doctoral Fellow, EPFL, Juni 2022 – Mai 24, Projekttitel: *Coercion-Resistant Remote E-Voting Systems with Everlasting Privacy*, CYD Mentor: Dr. Bernhard Tellenbach

Alessandro Stolfo, Doctoral Fellow, ETHZ, Januar 22 – Dezember 25, Projekttitel: *Privacy-Preserving Learning of Neural Language Models*, CYD Mentor: Dr. Ljiljana Dolamic

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

Adalsteinn Jonsson, Master Thesis Fellow, ETHZ, Dezember 21 – Juni 22, Projekttitel: *Binary Similarity Techniques for Malware Detection*, CYD Mentor: Dr. Martin Strohmeier

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

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

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

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

Dr. **Andrei Kucharavy**, Postdoc Fellow, EPFL, Dezember 20 - November 22, Projekttitel: *Evolutionary dynamics for improved GAN detection*, CYD Mentorin: Dr. Ljiljana Dolamic

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

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

Studierende

CYD Campus Mitarbeitende definieren und betreuen studentische Projekte auf Bachelor-, Master- und PhD-Stufe. Die Studierenden führen ihre Projekte in den Räumlichkeiten des CYD Campus der EPFL, der ETHZ sowie auf dem Campus in Thun durch. Im Jahr 2022 wurden Arbeiten von zwölf Studierenden durch den CYD Campus begleitet.

Lukas Baege, ETHZ, Oktober 22 – April 23, Betreuer: Dr. Martin Strohmeier

Pascal Schärli, ETHZ, Oktober 22 – März 23, Betreuer: Dr. Bernhard Tellenbach

Silvan Niederer, ETHZ, September 22 – Januar 23, Betreuer: Llorenç Roma

Pedro Miguel Sanchez Sanchez, Universidad de Murcia, September 22 – Dezember 22, Betreuer: Dr. Gérôme Bovet

Enrique Tomas Martinez Beltran, Universidad de Murcia, September 22 – Dezember 22, Betreuer: Dr. Gérôme Bovet

Yago Lizarribar, IMDEA Networks Institute, Juni 22 – September 22, Betreuer: Dr. Gérôme Bovet

Mathis Lindner, ETHZ, Februar 22 – August 22, Betreuer: Dr. Martin Strohmeier

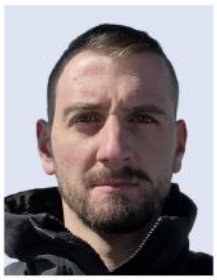
Sébastien Gillard, Université de Fribourg, 21 – 23, Betreuer: Dr. Alain Mermoud

Dominique Portenier, ETHZ, September 21 – Februar 22, Betreuer: Dr. Daniel Moser

Silvio Geel, ETHZ, September 21 – Februar 22, Betreuer: Dr. Daniel Moser

Marco di Nardo, ETHZ, September 21 – Februar 22, Betreuer: Dr. Daniel Moser

Florian Lerch, ETHZ, September 21 – Januar 22, Betreuer: Dr. Martin Strohmeier




Angehörige der Armee (AdA)

Wm. Michael Bosshard (Namen geändert), August 22 – Oktober 22, Data Science, Thun

Weitere Angehörige der Armee, die ihren Armeedienst im Lab 42, einer Innovationsabteilung des Cyber Bataillons 42, leisten, nutzten im Jahr 2022 die Räumlichkeiten des CYD Campus.

2 Highlights

Brokenwire

CYD Campus Mitarbeiter Martin Strohmeier hat zusammen mit Forschungspartnern der Universität Oxford eine Schwachstelle namens Brokenwire im Combined Charging System (CCS) von Elektrofahrzeugen entdeckt. CCS ist eine der am weitesten verbreiteten Gleichstrom-Schnellladetechnologien für Elektrofahrzeuge. Der Angriff unterbricht die notwendige Steuerkommunikation zwischen dem Fahrzeug und dem Ladegerät, so dass die Ladevorgänge unterbrochen werden. Der Angriff kann drahtlos aus der Ferne mittels elektromagnetischer Interferenz durchgeführt werden, so dass einzelne Fahrzeuge oder ganze Fahrzeugflotten gleichzeitig gestört werden können. Darüber hinaus kann der Angriff mit handelsüblicher Funkhardware und minimalen technischen Kenntnissen durchgeführt werden.

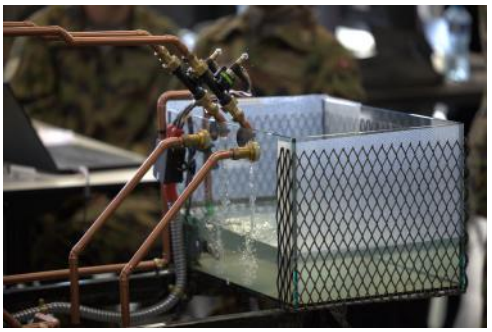
Demonstration von Brokenwire.

Die Forscher demonstrierten den Angriff in einem kontrollierten Labor und im Anschluss an sieben Fahrzeuge unterschiedlicher Hersteller und 18 Gleichstrom-Hochleistungsladegeräte unterschiedlicher Hersteller und 18 Gleichstrom-Hochleistungsladegeräte. Sie haben auch eine Meldung an die Industrie gemacht sowie verschiedene Gegenmassnahmen vorgeschlagen, mit denen sich die Auswirkungen begrenzen lassen. Brokenwire hat unmittelbare Implikationen für einen Grossteil der schätzungsweise zwölf Millionen batteriebetriebenen Elektrofahrzeuge, die sich weltweit im Verkehr befinden. Darüber hinaus hat es weitreichende Folgen für die neue Welle der Elektrifizierung von Fahrzeugflotten, sowohl für private Unternehmen als auch für wichtige öffentliche Dienste. Darüber hinaus betrifft Brokenwire elektrische Schiffe, Flugzeuge und schwere Nutzfahrzeuge.

Mehr Informationen:
Brokenwire Webseite & Publikation

ICS Hackathon in Thun

Der CYD Campus veranstaltete vom 19. bis 23. September zusammen mit dem Cyber Bataillon 42 einen Hackathon rund um industrielle Kontrollsysteme (ICS) und operative Technologien (OT).
Zu den über 30 Teilnehmenden gehörten Forschende des CYD Campus und der Schweizer Armee, Mitarbeitende des NCSC und Swissgrid, Soldaten des Cyber Bataillons 42, Studierende der Hochschule Luzern, ETH Zürich und Ruhr Universität Bochum, sowie Experten aus der Privatwirtschaft, wie z. B aus dem Unternehmen ALSEC Cyber Security Consulting und Nozomi Networks. Die Teilnehmenden wurden in funktionsübergreifende Teams mit unterschiedlichen Schwerpunkten im Bereich der industriellen Steuerungssysteme eingeteilt. Dies erlaubte es den Gruppen, gezielte Schwachstellenanalyse durchzuführen, unterschiedliche Angriffsvektoren untersuchen und geeignete Gegenmassnahmen zu entwickeln. Zudem ermöglichte dies ein vernetztes und intensives Arbeiten in kleineren Gruppen.
Schwachstellentests bei ICS-Systemen sind im Vergleich zu Informationssystemen schwierig umzusetzen, da schwere Schäden verursacht werden können. Um sie dennoch durchführen und Angriffe simulieren zu können, sowie für Ausbildungs- und Trainingszwecke, sind entsprechende Labore besonders geeignet. Deshalb hat der CYD Campus zwei Labore für die Infrastruktur des Hackathons bereitgestellt, die jeweils ein anderes industrielles Steuerungssystem simulieren. Das eine ist die Darstellung eines Pumpspeicherkraftwerks. Beim zweiten handelt es sich um die Rekonstruktion eines Schweizer Energieunterwerks zur Entwicklung von Angriffs- und Verteidigungsstrategien, dem sogenannten Krinflab. Mit dem Hackathon verfolgte der CYD Campus drei Ziele: Die Erweiterung des im VBS vorhandenen Wissens in diesem relevanten Bereich, die Vernetzung von Fachleuten aus Industrie, Hochschulen und öffentlicher Verwaltung sowie die Unterstützung von jungen Talenten, die ihre Expertise auf diesem Gebiet vertiefen wollen.



Modell eines Pumpspeicherkraftwerks: CYD Campus ICS-Labor in Thun.

Krinflab: Rekonstruktion eines Schweizer Energieunterwerks zur Entwicklung von Angriffs- und Abwehrstrategien.

Mehr Informationen: CYD Campus Hackathon Mitteilung

Trends bei Datenschutz- und Verschlüsselungstechnologien 2025

Militärs und Regierungen setzen seit langem Verschlüsselungstechnologien ein, um geheime Kommunikationen zu erleichtern. Heute spielen Verschlüsselungstechnologien eine genauso wichtige Rolle für den Schutz unserer Wirtschaft und Zivilgesellschaft. Sie sind wichtige Voraussetzungen für die laufende Transformation der digitalen Wirtschaft und der Online-Gesellschaft. Die Anfang 2022 vom Cyber-Defence Campus lancierte Studie gibt einen Überblick über die sich wandelnde Landschaft der Verschlüsselungs- und Datenschutztechnologien sowie deren globale Nutzungstrends. Im Auftrag der Schweizer Regierung hat der CYD Campus die 38 wichtigsten Verschlüsselungs- und Datenschutztechnologien identifiziert, um deren voraussichtliche Entwicklungen bis 2025 zu analysieren und die Auswirkungen auf die Bereiche Militär, Zivilgesellschaft und Wirtschaft zu ermitteln. Rund 50 Experten und Expertinnen aus der Wissenschaft, der Schweizer Regierung und der Industrie haben an dieser Studie mitgewirkt. Unter ihnen waren zahlreiche Forschende, Praktikant/innen und CYD Fellows des CYD Campus. Die Studie ist eine Referenz für Organisationen und Einzelpersonen, die in den kommenden Jahren kohärente und wirksame Strategien zum Schutz und zur Verschlüsselung von Daten entwickeln müssen. Die Technologien sind in fünf Kategorien unterteilt:

1. Verschlüsselungsgrundlagentechnologien werden verwendet, um andere Verschlüsselungsanwendungen zu erstellen;
2. Low-Level-Anwendungen: Konzentration auf grundlegende Funktionalitäten;
3. High-Level-Anwendungen: Schwerpunkt auf komplexeren Funktionalitäten;
4. Datenschutztechnologien: Datenschutz ohne Verschlüsselung;
5. Anwendungsfälle: Konkrete Möglichkeiten, wie Technologien zusammen verwendet werden können, um eine tragfähige Gesamtlösung zu schaffen.

Alain Mermoud und Valentin Mulder stellen die Studie an der CYD Campus Konferenz vor.

Die Studie wurde auf der CYD Campus Konferenz 2022 vorgestellt und wird im Sommer 2023 als Buch veröffentlicht.

Eröffnung neuer CYD Campus Standort Zürich

Ein weiteres Highlight des CYD Campus im Jahr 2022 war die Neueröffnung der Räumlichkeiten an der Zollstrasse 62 in Zürich. Gleichzeitig mit der offiziellen Neueröffnung des CYD Campus Zürich am 24. November 2022 wurde zudem die Einführung von SCION gefeiert. SCION ist eine neuartige Internet-Architektur, die vor zehn Jahren an der ETH Zürich entwickelt und in den letzten fünf Jahren durch das ETH-Spin-off Anapaya Systems marktfähig gemacht wurde. Die Technologie ersetzt das unsichere Internet-Routing-Protokoll durch ein sichereres und effizienteres Protokoll.
Das VBS ist daran interessiert, diese Technologie für die Schweizer Cyberabwehr einzusetzen und testet diese Technologie beim CYD Campus zusammen mit Schweizer Industriepartnern. Die drei CYD Campus Standorte in Thun, Lausanne und Zürich wurden hierfür mit SCION-Netzwerkanschlüssen der Firmen Swisscom, Sunrise und SWITCH ausgerüstet und für drei Jahre als nationale Testinfrastruktur für die Armee und Sicherheitsbehörden zur Verfügung gestellt.

Neueröffnung CYD Campus Büro in Zürich.

Cyber-Defence Campus Konferenz

Eine zentrale Aufgabe des CYD Campus ist die Vernetzung von Wissenschaft, Industrie und staatlichen Akteuren im Bereich der Cyberverteidigung. Zu diesem Zweck organisiert der CYD Campus regelmässig Veranstaltungen zu verteidigungs- und sicherheitsrelevanten Cyber-Themen. Ein jährlicher Veranstaltungshöhepunkt ist die Cyber-Defence Campus Konferenz mit über 300 Besucherinnen und Besuchern.

Podiumsdiskussion Studie Datenschutz- und Verschlüsselungstechnologien 2025.

Die CYD Campus Konferenz 2022 fand am 26. Oktober im Kursaal in Bern statt. Im Rahmen der Veranstaltung referierten Expertinnen und Experten aus der öffentlichen Verwaltung, Akademie und Industrie zu Schlüsselthemen im Bereich der Sicherung von zukünftigen digitalen Infrastrukturen. Nebst Referaten zu den Entwicklungen im Bereich der Kommunikationsnetze (5G+), des globalen Finanzsystems, Entwicklungen im Bereich der Kommunikationsnetze (5G+), des globalen Finanzsystems, der Verbreitung von (Des-)Informationen oder auch der Kryptographie wurde die Vortragsreihe abgerundet mit einem Einblick in die Konzeption und Durchführung realitäts-naher Cyber-Defence-Trainings wie «Locked Shields».

Cyber Startup Challenge 2022

Im Juni 2022 startete zum dritten Mal in Folge der Aufruf zur Cyber Startup Challenge. Im Rahmen der Challenge präsentierten 36 Startups aus verschiedenen Ländern ihre innovativen Technologien im Bereich der Netzwerkerkennung und Sicherheit von IoT-Geräten. Nach der Evaluation durch Cyberexpertinnen und -experten des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) wurden schliesslich die drei Finalisten ONEKEY, Narrowin und Sepio an die CYD Campus Konferenz eingeladen. An der Konferenz durfte jeder der Finalisten einen Pitch halten, bei dem das Startup ONEKEY die Jury des VBS letztlich überzeugen konnte.

ONEKEY hat eine Technologie entwickelt, die Sicherheitsschwachstellen automatisch ermittelt. Anhand der «Software Bill of Materials (SBOM)» und automatisch generierten «Digital Twins» überprüft ONEKEY die betriebliche Software auf kritische Sicherheitsschwachstellen und Compliance-Verstösse. Einerseits bietet die SBOM eine detaillierte Übersicht über alle Komponenten einer Software. Andererseits ist ein «Digital Twin» ein virtuelles Abbild eines Systems und ermöglicht dessen Untersuchung im Labor, ohne den Quellcode, das Netzwerk oder den physischen Zugang zu den Geräten.

Mehr Informationen:
Finalisten 2022 & Medienmitteilung Cyber Startup Challenge

Colin Barschel, Leiter Innovation CYD Campus und Florian Lukavsky, Mitgründer und CTO von ONEKEY.

Vertretung der Schweiz beim NATO CCDCOE

William Blonay, Mitarbeiter des CYD Campus, hat im Februar 2022 sein Amt als Vertreter der Schweiz beim NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estland, angetreten und wird es drei Jahre lang ausüben. Das CCDCOE ist ein von der NATO akkreditiertes Cyber-Kompetenzzentrum, dessen Ziel es ist, die Forschungs- und Ausbildungszusammenarbeit im Bereich der Cyberabwehr international zu stärken. Dies wird erreicht durch die Organisation gemeinsamer Übungen und die Durchführung von Forschungsprojekten, technischen Schulungen und Konferenzen.

Zu den Flaggschiffen des CCDCOE gehören die jährliche internationale Konferenz über Cyberkonflikte (CyCon), das Tallinn Manual und «Locked Shields», eine der weltweit grössten Cyberverteidigungsübungen (mehr Infos im nächsten Highlight), bei der auch William Blonay im Jahr 2022 im Red und Green Team mitwirkte.
Die Schweiz profitiert seit ihrem Beitritt als «Contributing Nation» im Jahr 2019 vom Informations- und Wissensaustausch sowie von den diversen gemeinsamen Forschungs- und Ausbildungsaktivitäten des CCDCOE. Diese Kooperation trägt ebenfalls zur Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) und der Strategie Cyber VBS 2021-2024 bei. Vor dem Hintergrund der veränderten weltpolitischen Lage ist es der Schweiz ein besonderes Anliegen, die internationale Zusammenarbeit insbesondere im Bereich der Verteidigung zu vertiefen.

Die Mitgliedstaaten des CCDCOE entsenden jeweils eine bis zwei Expertinnen oder Experten als Vertreter nach Tallinn. Diese sind in verschiedenen Kompetenzbereiche wie Technologie, Strategie, Operationen, Unterstützung, Ausbildung und Training sowie Recht tätig. Die Schweiz ist gegenwärtig mit zwei Personen beim CCDCOE vertreten: Neben William Blonay, der dem Kompetenzbereich Technologie angehört, repräsentiert Lisa Schauss, Mitglied der Führungsunterstützungsbasis der Armee (FUB) und Teil des Kompetenzbereichs Bildung und Ausbildung, die Schweiz beim CCDCOE.
Um mehr über Williams Erfahrungen am CCDCOE zu erfahren, lesen Sie das Interview in der Dezember-Ausgabe 2022 des armafolio.

Cyber-Defence Übung «Locked Shields»

Das CCDCOE organisierte im April 2022 die Locked Shields Cyber-Defence Übung, welche seit 2010 jährlich stattfindet. Der CYD Campus beteiligt sich unter anderem direkt an der Organisation der Übungen, indem er Fachleute in die Green und Red Teams entsendet. Diese beiden Teams sind für die Organisation und Durchführung der Übung zuständig und setzen sich aus Experten aller teilnehmenden Staaten zusammen. Die Schweizer Armee nimmt regelmässig mit ihrem eigenen Blue Team oder gemeinsam mit anderen Ländern teil, um ihre Experten und Expertinnen in der Cyber-Verteidigung zu schulen.

Während der Übung arbeiten Red Teams als Angreifer gegen Blue Teams, die als Cyber-Rapid-Reaction-Team nationale IT-Systeme und kritische Infrastrukturen des fiktiven Inselstaat Berylia gegen grossangelegte Cyberangriffe verteidigen müssen. Insgesamt nahmen über 2000 Teilnehmerinnen und Teilnehmer aus 32 Nationen teil. Die aus Mitgliedstaaten und Partnern gebildeten Teams müssen nicht nur zahlreiche komplexe cyber-physische Systeme schützen, sondern auch in der Lage sein, strategische und taktische Entscheidungen zu treffen, Vorfälle zu melden und Herausforderungen in den Bereichen Forensik, Recht, Medienarbeit und Informationskriegsführung zu bewältigen. Ziel der Übung war es, die Fähigkeiten und Kenntnisse der Teilnehmenden im Bereich der Cyberverteidigung zu verbessern und die Zusammenarbeit zwischen den verschiedenen Nationen und Organisationen zu fördern.

Aufgrund der zahlreichen Angriffe und der Komplexität der Übung ist Locked Shields auch ein ideales Umfeld, um Produkte zur Cyberabwehr zu testen. Im Kapitel 6.1 «Resultate der Innovationsprojekte» wird die Zusammenarbeit zwischen dem Cyber-Defence Campus und der Industrie in diesem Zusammenhang erläutert.

William Blonay an seinem ersten Tag als Vertreter der Schweiz am CCDCOE.

Teil der Übung «Locked Shields» im April 2022.

3 Talentförderung

Fachkräfte im Bereich Cybersicherheit und Datenwissenschaften sind in der Schweiz und in vielen anderen Ländern rar. Die Förderung und Ausbildung von neuen Cyber-Talenten ist daher eine zentrale Herausforderung und gehört deshalb zu den drei Kernaufgaben des CYD Campus. Um die Cyber-Expertise der Studierenden zu erhöhen, verfolgt der CYD Campus unterschiedliche Ansätze.

Zum einen bietet er Hochschulpraktika an allen drei Standorten in Thun, Lausanne und Zürich an. Darüber hinaus werden studentische Projekte auf Bachelor-, Master- und PhD-Stufe definiert und von CYD Campus Mitarbeitenden betreut. Diese Studierenden sind an einer Universität immatrikuliert und werden von einem Mentor oder einer Mentorin des CYD Campus betreut. Des Weiteren hat der CYD Campus zusammen mit der EPFL im Jahr 2020 das CYD Fellowship Programm lanciert, um Studierenden die Gelegenheit zu geben und zu motivieren, ihre Kompetenzen auf dem Gebiet der Cyberverteidigung zu stärken.

Im Jahr 2022 wurden 27 Hochschulpraktikant/innen beschäftigt und zwölf studentische Arbeiten durch CYD Campus Wissenschaftler/innen betreut. Zudem waren 13 CYD Fellows aktiv. Ziel ist es, auf diese Weise eine neue Generation von Cyber-Talenten zu fördern. Damit erbringt der CYD Campus einen substanziellen Beitrag zur Bekämpfung des Fachkräftemangels im hochspezialisierten Cyber-Bereich mit dem langfristigen Ziel, die erforderlichen Cyber-Kompetenzen für die Regierung, Wissenschaft und Wirtschaft in der Schweiz sicherzustellen.

Seit dem Jahr 2022 haben ebenfalls Angehörige des Cyber-Lehrgangs die Möglichkeit, beim Cyber-Defence Campus ihr Praktikum zu absolvieren. Der Cyber-Lehrgang wurde erstmals in der Rekrutenschule (RS) 2018 als Pilotprojekt gestartet und hat zum Ziel, die Cyber-Defence Kompetenzen der Schweizer Miliz Armee zu stärken. Der Lehrgang richtet sich an Informatiker EFZ, Maturanden sowie Studierende. Im Jahr 2022 konnte der erste Rekrut des Cyber-Lehrgangs beim CYD Campus ein Praktikum absolvieren.

Um einen tieferen Einblick in die Arbeiten der CYD Fellows, der Hochschulpraktikant/innen und der Angehörigen der Armee (AdA) zu erhalten, wurden im Rahmen dieses Jahresberichts Interviews durchgeführt.

Sarah Ismail - Hochschulpraktikantin in Lausanne im Bereich Technologie Monitoring

Mit welchem Forschungsthema hast du dich während deiner Zeit bei CYD Campus beschäftigt?

Meine Forschung konzentriert sich auf Datenschutz- und Verschlüsselungstechnologien. Das Ziel ist es, aktuelle Trends dieser Technologien anhand der öffentlichen Aufmerksamkeit über die Seitenaufrufe bei Wikipedia vorherzusagen. Die Studie identifiziert, misst und analysiert die zeitlich variierende öffentliche Aufmerksamkeit, die den einzelnen Technologien zuteil wird, unter Verwendung anderer Datensätze wie arXiv, Google Trends und OpenAlex.

Inwiefern konntest du bei deiner Arbeit vom Wissen und den Ressourcen des CYD Campus profitieren?

Einerseits lernte ich neue technische Fertigkeiten, wie z. B. das Programmieren in einer Programmiersprache, die ich zuvor noch nicht beherrschte. Andererseits konnte ich mit hochspezialisierten und kompetenten Leuten auf ihrem Gebiet zusammenarbeiten. Dies erleichterte das Lernen und den Austausch von Wissen. Ausserdem bietet der CYD Campus viele Hilfsmittel, die es einem ermöglichen, seine Forschung in einer angenehmen und geeigneten Umgebung durchzuführen.

Wenn du zukünftigen Praktikanten einen allgemeinen Rat für ihre Zeit beim CYD Campus geben könntest, wie würde dieser lauten?

Ich kann nur empfehlen, nicht zu zögern, mit den Kollegen zu kommunizieren und ihnen Fragen zu stellen, denn das fördert die Zusammenarbeit, den Ideenaustausch und vor allem die Kreativität.

Was war deine Motivation, ein Praktikum beim CYD Campus zu absolvieren?

Cybersicherheit ist ein brandaktuelles Thema. Wie man in den Nachrichten mitverfolgen konnte, kam es in den letzten Jahren zu mehreren Datenschutzverletzungen. Das hat meine Neugierde und den Wunsch geweckt, mehr über Cybersicherheit zu erfahren. Zudem bin ich von der Forschungswelt fasziniert und möchte mich in diesem Bereich entfalten.

Wo siehst du dich in zehn Jahren?

In zehn Jahren möchte ich solide Berufserfahrung als Business Analystin gesammelt haben, eventuell im Bereich der Cybersicherheit. Ausserdem möchte ich eine Position mit Verantwortung, in der ich an verschiedenen Projekten arbeiten kann.

Interview mit Luca Crijns - Hochschulpraktikant in Lausanne im Bereich Cybersicherheit

Mit welchem Forschungsthema befasst du dich während deiner Zeit bei CYD Campus?

Ich arbeite an einem Netzwerkfilter, der in der Lage ist, Ströme aus dem Netzwerkverkehr mit Geschwindigkeiten von 100 Gbps auf der Grundlage von konfigurierbaren Regeln zu extrahieren. Das Filtern nach IP-Adressen und Ports ist sehr verbreitet und kann mit vielen Hardware-Lösungen durchgeführt werden. Die «Deep Packet Inspection» und die Filterung auf Basis der Nutzlast von Paketen wird jedoch meist mit Software durchgeführt. Ich habe mehrere Hardware-Lösungen in Kombination mit entsprechender Software getestet, um dies zu ermöglichen.

Inwiefern kannst du bei deiner Arbeit vom Wissen und den Ressourcen des CYD Campus profitieren?

Zusätzlich zu meinem Betreuer habe ich einen technischen Betreuer, der mir helfen kann, wenn ich technische Schwierigkeiten mit der Hardware und Software habe. Er hat sich als sehr wertvoll erwiesen, wenn ich Fragen habe oder etwas besprechen möchte.

Wenn du zukünftigen Praktikanten einen allgemeinen Rat für ihre Zeit beim CYD Campus geben könntest, wie würde dieser lauten?

Für mich hat es sich als nützlich erwiesen, am Ende der Woche ein wöchentliches Update über das Projekt zu senden. Auf diese Weise stellt man automatisch sicher, dass man am Ende der Woche Fortschritte gemacht hat. Ausserdem sollte man daran denken, dass der Betreuer einem zur Seite steht und man meist zu einem Gespräch vorbeikommen kann, wenn man nicht weiterkommt. Es hat wenig Sinn, lange Zeit auf den Bildschirm zu starren und zu überlegen, was man tun soll.

Was ist deine Motivation, ein Praktikum beim Cyber-Defence Campus zu absolvieren?

Meine Motivation war, Neues zu lernen. Ich komme aus der Mathematik und hatte vorher keinerlei Erfahrung mit Netzwerken. Deshalb habe ich dieses Praktikum gewählt, um mein Wissen und meinen Horizont zu erweitern. Ich war mir zuvor nicht sicher, ob ich mir vorstellen könnte, in einem Bereich zu arbeiten, der eng mit der Mathematik verbunden ist.

Wo siehst du dich in zehn Jahren?

Ehrlich gesagt, weiss ich es nicht. Da mir die Arbeit auf dem CYD Campus gefällt, möchte ich wahrscheinlich etwas Vergleichbares machen. Das ist zwar eine etwas simple Antwort, aber mehr Details dazu kann ich im Moment nicht geben.

Interview mit Wachtmeister Michael Bosshard (Cyber-Lehrgang, Namen geändert)

Mit welchem Forschungsthema hast du dich während deiner Zeit bei CYD Campus beschäftigt?

Während meiner Zeit beim CYD Campus habe ich hauptsächlich an Deep Learning Methoden für Graphen gearbeitet. Deep Learning Methoden für Graphen sind ein relativ junges Forschungsgebiet, das schnell wächst. Insbesondere untersuchte ich Klassifizierungsaufgaben unter Verwendung «Conventional Convolutions» sowie modernerer Methoden wie EdgePooling und Graphvariations-Autoencodern. Das Ziel war es, Aufgaben auf Graphenebene zu optimieren, die mit statischen Methoden wesentlich mehr Zeit in Anspruch nehmen würden.

Inwiefern kannst du bei deiner Arbeit vom Wissen und den Ressourcen des CYD Campus profitieren?

Der CYD Campus konnte mir ein solides Umfeld bieten, in dem ich einerseits genügend Unterstützung erhielt, um meine Forschungsziele zu verfolgen, und das andererseits auch eine wissenschaftliche Herausforderung bot.

Wenn du zukünftigen Praktikanten einen allgemeinen Rat für ihre Zeit beim CYD Campus geben könntest, wie würde dieser lauten?

Der wichtigste Rat, den ich geben würde, ist der, dass es sich lohnt, das Umfeld und die Umgebung des CYD Campus kennenzulernen, da es viele Einrichtungen und Strukturen gibt, die dich während deiner Forschung unterstützen.

Was war deine Motivation, ein Praktikum beim CYD Campus zu absolvieren?

Meine Hauptmotivation für mein Praktikum war es, meine datenwissenschaftlichen Fähigkeiten einzusetzen, um in der Welt der Cybersicherheit und des Schutzes von Vermögenswerten etwas zu bewirken. Da ich einen rein naturwissenschaftlichen Hintergrund habe (Mathematik), fand ich es sehr interessant, mein Wissen anhand von Anwendungsfällen anzuwenden und weiterzuentwickeln.

Wo siehst du dich in zehn Jahren?

In zehn Jahren erhoffe ich mir, dass ich mich zu einem erfahreneren Datenwissenschaftler entwickelt habe und auf ein breites Spektrum verschiedener Methoden und Ansätze zurückgreifen kann. Ich kann nicht sagen, ob ich im öffentlichen oder im privaten Sektor arbeiten werde, aber ich bin zuversichtlich, dass die Aufgaben, die ich übernehmen werde, immer noch herausfordernd und motivierend sein werden.

Interview mit Lina Gehri - Master CYD Fellow in Zürich

Mit welchem Forschungsthema hast du dich während deiner Zeit bei CYD Campus beschäftigt?

Ich habe Modelle für maschinelles Lernen entwickelt, um Command-and-Control-Angriffe zu erkennen. Mein Ziel war es, die Modelle so zu generalisieren, dass sie in der Lage sind, Command-and-Control-Verkehr in verschiedenen und ungewohnten Netzwerkumgebungen zu erkennen. Zum Trainieren und Testen verwendete ich Netzwerkverkehr, der während der umfangreichen Cyberverteidigungsübung «Locked Shields» erfasst wurde.

Inwiefern kannst du bei deiner Arbeit vom Wissen und den Ressourcen des CYD Campus profitieren?

Der grösste Vorteil war, dass ich viel Unterstützung von verschiedenen Personen am CYD Campus erhielt. Wenn ich eine Frage hatte oder Hilfe brauchte, halfen mir ihre kombinierten Erfahrungen und ihr Wissen sehr und viele neue Ideen kamen während der Diskussionen über meine Arbeit auf.

Wenn du zukünftigen CYD Fellows einen allgemeinen Rat für ihre Zeit beim CYD Campus geben könntest, wie würde dieser lauten?

Nutzt die Gelegenheit, geht ins Büro und sprecht mit den Leuten dort über das, was ihr tut, egal ob es um eure Abschlussarbeit oder eure jüngsten Interessen geht.

Was war deine Motivation, ein Praktikum beim CYD zu absolvieren?

Ich hatte bereits beschlossen, meine Masterarbeit in Zusammenarbeit mit dem CYD Campus zu schreiben, als mein Betreuer mir von den Fellowships erzählte und mich ermutigte, mich zu bewerben. Es schien eine grossartige Gelegenheit zu sein, Gleichgesinnte kennenzulernen und mit ihnen zusammenzuarbeiten, also beschloss ich, es zu versuchen.

Wo siehst du dich in zehn Jahren?

Hoffentlich lerne ich immer noch Neues und bin immer noch begeistert von der Arbeit, die ich tue. Für Details müsste man mir die Frage in 9.5 Jahren wieder stellen.

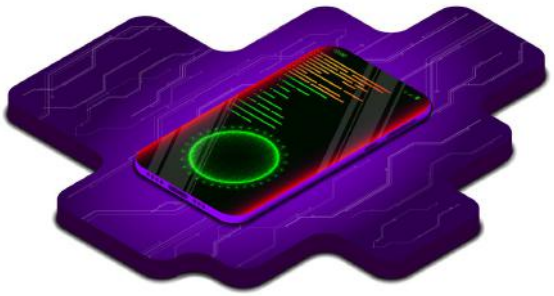
4 Forschung

Die Forschung des CYD Campus ist eine Investition in eine nachhaltige Sicherstellung des benötigten Expertenwissens und der wissenschaftlich-technischen Kompetenzen für die Aufgaben und Tätigkeiten des Bundes im Bereich der Cyber-Defence. Als integraler Teil des Technologiemanagements bildet sie auch die Basis für ein fundiertes Roadmapping künftiger Technologien und für Innovationsvorhaben des VBS. Damit leistet sie sowohl einen Beitrag zur Entwicklung von zukünftig erforderlichen operationellen Cyber-Defence-Fähigkeiten, als auch zur wissenschaftlich-technischen Abstützung von Planungen und Beschaffungen im VBS.

Forschungsprojekte werden zusammen mit den Hochschulen und Industriepartner umgesetzt.

4.1 Projekte Bereich Cybersicherheit

Sichere mobile Betriebssysteme



Mobile Geräte (Smartphones) sind für effizientes Arbeiten unverzichtbar, aber ihre Mobilität und Vernetzung bieten viele Angriffsmöglichkeiten. Der Schutz von vertraulichen und geheimen Informationen ist daher besonders erschwert. Ziel ist es, ein handelsübliches mobiles Gerät für den Datenaustausch von sensitiven Informationen und Anwendungen einzusetzen. Dieses Gerät ermöglicht es Informationen, sei es bei einem Anruf, einer Nachricht oder über eine App, bis auf Stufe «vertraulich» auszutauschen. Die grösste Herausforderung besteht darin, die beste Architektur für ein sicheres mobiles Betriebssystem zu finden, die ein Gleichgewicht zwischen Sicherheit, Machbarkeit und Benutzerfreundlichkeit bietet.
Es werden zwei Ansätze verfolgt, um die sensiblen Daten zu schützen: Der erste Ansatz besteht in einer Kompartimentierung der Risiken. Das bedeutet, dass die Angriffsfläche auf das System verschachtelt wird, damit die Auswirkungen eines Angriffs minimiert werden können. Dazu wurden zwei Architekturen für ein sicheres mobiles Betriebssystem entwickelt, einschliesslich einer Risikoanalyse. Die Cybersicherheit umfasst nicht nur das mobile Betriebssystem, sondern auch die Hardware, die kryptographischen Komponenten und die Härtung der Bootkette (Signaturen). Der zweite Ansatz versucht die Ausführung einer Anwendung vom Betriebssystem und dem Hersteller zu trennen, um die Souveränität über die Anwendung zu gewährleisten und die Sicherheit zu erhöhen.

Souveräne Smartphone-Architektur

Das Smartphone gehört für viele Menschen zum Kern ihres digitalen Lebens. Allerdings bieten sie nicht die gleiche Flexibilität wie PCs, auf denen die Nutzer beliebige Software installieren und ausführen können. Denn die Anbieter der führenden Betriebssysteme wie iOS und Android können diktieren, welche Anwendungen genutzt werden können, wie sie ausgeführt werden und auf welche Telefonressourcen sie zugreifen können. Dies ist nicht ideal, da die Nutzer ihre Sicherheit und ihre Privatsphäre den Anbietern von Betriebssystemen anvertrauen und die von ihnen auferlegten Funktionseinschränkungen akzeptieren müssen. Angesichts der weiten Verbreitung von Android und iOS ist ein sofortiger Ausstieg aus diesen Ökosystemen keine praktische Lösung. Als Alternative wird die Entwicklung einer neuen Smartphone-Architektur vorgeschlagen, die den Nutzerinnen und Nutzern die Kontrolle zurückgibt und gleichzeitig die Kompatibilität mit den aktuellen Smartphone-Ökosystemen sicherstellt. Ein solches Design wird auf Basis von Fortschritten bei «Trusted Execution Environments» für ARM und RISC-V vorgeschlagen und analysiert.

Erkennung von Software- und Geräteschwachstellen: Microsoft Windows Anwendungen

Die Schwachstellenforschung im Bereich der Windows-basierten Systeme und Anwendungen hat zum Ziel, unbekannte Sicherheitslücken aufzudecken. Durch den Fokus auf Softwares, welche von den Stakeholdern (Organisationen innerhalb des VBS, aber auch der übrigen Bundesverwaltung) eingesetzt werden, entsteht neben der Forschungstätigkeit auch ein direkt messbarer Nutzen für die IT-Sicherheit der Bundesverwaltung. Neben dem Aufbau von Kompetenzen zum Auffinden und Ausnutzen von Schwachstellen, wurden im vergangenen Jahr mehrere, teils kritische Sicherheitslücken entdeckt und in Form von Advisories an die Stakeholder kommuniziert. Die betroffenen Hersteller wurden ausführlich über die Schwachstellen informiert und durch die Bereitstellung voll funktionsfähiger Proof of Concept Exploits dazu animiert, diese so schnell wie möglich zu beheben.

Erkennung von Software- und Geräteschwachstellen: IoT Geräte

Vernetzte Geräte, die oft als Internet der Dinge (IoT) bezeichnet werden, sind heute allgegenwärtig, wobei ihre Anwendungen oft sicherheitskritisch sind. Die Erkennung potenzieller Schwachstellen in solchen Geräten ist daher von entscheidender Bedeutung, stellt jedoch oft eine Herausforderung dar. Insbesondere hat ein Analyst bzw. eine Analystin in der Regel keinen Zugriff auf den Quellcode der auf dem Gerät laufenden Programme, die folglich nur als maschinenausführbarer Binärcode vorliegen. Im Gegensatz zum Quellcode, der für den Menschen leichter zu verstehen ist, sind im Binärcode viele Abstraktionen (z.B. Funktionsnamen) nicht mehr vorhanden, was die Analyse stark erschwert. Ausserdem hängt der Binärcode von der verwendeten Prozessorarchitektur ab, die sich bei IoT-Geräten oft stärker unterscheidet (z. B. ARM, MIPS) als bei herkömmlichen Computern (häufig x86). Im Rahmen dieses Forschungsprojektes werden Techniken zur (semi-) automatisierten Analyse von IoT-Binaries erprobt und die Machbarkeit mit entsprechendem Proof of Concept-Tools demonstriert.

Erkennung von Software- und Geräteschwachstellen: Linux Kernel

Der Linux Betriebssystemkern (engl. Linux Kernel) bildet heutzutage die Grundlage für diverse Betriebssysteme, welche wiederum auf einer Vielzahl von Geräten (Desktop-PCs, Serversystemen, mobile- oder elektronischen Kleingeräte, etc.) verwendet werden. Ein praktikabler Ansatz zur Identifizierung potenzieller Sicherheitsprobleme im Linux-Kernel ist die Verwendung eines sogenannten Kernel-Fuzzers, der auf Basis unvorhergesehener Eingaben mögliches Fehlverhalten im Kernel erkennen soll. Der wohl bekannteste dieser Fuzzer für den Linux-Kernel ist syzkaller. Für die aktuelle Kernelversion listet eine öffentliche Instanz von syzkaller mehr als 1000 solcher Fehlverhalten auf, bei denen allerdings unklar ist, ob sie auch tatsächlich ausnutzbar sind, d.h. ob es sich um echte Schwachstellen handelt. Im Rahmen dieses Forschungsprojektes wird an einem automatisierten Verfahren gearbeitet, um diese Ausnutzbarkeit zu beurteilen. Dies ist zentral, um die Kritikalität identifizierter Fehlverhalten einzustufen und entsprechend priorisiert beheben zu können.

Kontrollierbares Routing im Internet

Bei herkömmlichen Internettechnologien haben die Endnutzer keine Transparenz und keine Kontrolle über den Weg des Datenverkehrs zum Zielort. Insbesondere das Fehlen von Informationen über Netzwerkgeräte verringert die Vertrauenswürdigkeit des Weiterleitungspfads und verhindert, dass Endbenutzeranwendungen, die bestimmte Routerfunktionen benötigen, ihr volles Potenzial ausschöpfen können. Ausserdem führt der Kontrollverlust dazu, dass Anwendungen über unerwünschte Routen kommunizieren, während alternative Pfade mit wünschenswerteren Eigenschaften unbrauchbar bleiben. In diesem Projekt wurde von den CYD Campus Forschenden ein System entwickelt, das es Anwendungen ermöglicht, den Datenverkehr flexibel weiterzuleiten, möglicherweise über mehrere Pfade, entsprechend benutzerdefinierter Präferenzrichtlinien, wobei Informationen über Router offengelegt und von autonomen Systemen transparent bescheinigt werden. Die Granularität dieser Informationen wird von jedem autonomen System individuell gewählt und schützt vor der Weitergabe sensibler Netzwerkdetails an Angreifer. Die Forschenden demonstrierten die Machbarkeit ihres Systems, indem sie es auf einem SCION-Testnetzwerk einsetzten und so einen hohen Durchsatz auf handelsüblicher Hardware nachweisen konnten.

Secure Wide Area Networking

Angesichts des wachsenden Bedarfs an sicheren Verbindungen zwischen Büros, Partnern und Cloud-basierten Anwendungen sind private Netze auf der Grundlage von MPLS (Multiprotocol Label Switching), VPN (Virtual Private Network) oder ähnlichen Technologien nicht länger eine praktikable Option für den Aufbau sicherer WANs (Wide Area Networks). In diesem Projekt werden alternative Technologien wie SCION von Anapaya/ETHZ und programmierbare Router untersucht, um eine sichere Kommunikation zu ermöglichen und Informationen zwischen Unternehmensstandorten, vertrauenswürdigen Partnern und Cloud-Anbietern zu übertragen. Ziel ist es, sichere Routing-Techniken zu entwickeln und zu evaluieren, darunter explizites Pfad-Routing, sichere Routen-Attestierung, Abwehr von Distributed-Denial-of-Service (DDoS)-Angriffen und Verkehrsverschleierung. Diese Techniken werden in einem 2022 entwickelten Testbed demonstriert, das die CYD Campus in Thun, Lausanne und Zürich verbindet.

Programmierbare Netzwerke

Jüngste Fortschritte bei programmierbaren Netzwerkgeräten machen es möglich, benutzerdefinierte Programme sowohl in der Kontroll- als auch in der Datenebene auszuführen. In diesem Forschungsprojekt wird untersucht, wie diese neuen Möglichkeiten die Netzwerksicherheit verbessern können. Insbesondere konzentriert sich das Projekt auf die Verschleierung von Netzwerken, eine Methode zur Verbergung sensibler Informationen, die nicht durch herkömmliche Sicherheitsmassnahmen wie Verschlüsselung geschützt sind.

Im Jahr 2022 lag der Schwerpunkt auf sogenannten Verkehrsanalyse-Angriffen. Diese Angriffe machen sich die Tatsache zunutze, dass selbst bei verschlüsseltem Datenverkehr Informationen über die Grösse und das Timing von Paketen durchsickern. Veröffentlichte Angriffe zeigen, dass diese Informationen ausreichen, um Details über die laufende Kommunikation zu ermitteln. Leider sind die bestehenden Abwehrmechanismen in Bezug auf die Sicherheit und/oder Leistung begrenzt.

In Zusammenarbeit mit Forschenden der ETH Zürich wurde ein System entwickelt, das den Netzwerkverkehr so verschleiert, dass Verkehrsanalyse-Angriffe nicht mehr möglich sind. Das System läuft auf programmierbaren Netzwerkgeräten mit hoher Übertragungsgeschwindigkeit, was es besonders für den Schutz von Wide Area Networks geeignet macht.

Aufklärungsplattformen für Cyber-Bedrohungen

Cybersicherheitsinformationen sind in der Regel höchst sensibel und vertraulich, weshalb Organisationen nur ungern diese Daten mit Dritten teilen, selbst wenn eine aggregierte Analyse gemeinsamer Bedrohungen erhebliche Vorteile für die Reaktionsfähigkeit und Sicherheit bieten würde. Als Reaktion auf diesen Zielkonflikt entwickeln Forschende des CYD Campus eine Plattform, die Garantien bietet, dass Nutzer/innen nur auf die globalen Erkenntnisse (Cyber-Bedrohungsmodelle) zugreifen können. Jede Institution behält dabei die volle Kontrolle über ihre Datensätze. Ermöglicht wird dies einerseits durch die Entwicklung einer verteilten Architektur ohne zentralisierte Datenbank und andererseits durch die Integration fortschrittlicher kryptografischer Techniken, die auf dem Modell der homomorphen Mehrparteienverschlüsselung basieren. Dies erlaubt den Institutionen eine sichere Zusammenarbeit mit wichtigen sensiblen Daten, die normalerweise nicht gemeinsam genutzt werden, was zu neuen und besseren Bedrohungslage führt. Im 2022 wurden zwei Prototypen entwickelt und evaluiert für den Austausch von Daten aus MISP (Malware Information Sharing Platform) Datenbanken und aus Netzwerk Intrusion Detektion Systeme (NIDS) wie Suricata.

Quantensichere Kryptographie

Die voranschreitende Forschung im Bereich Quantencomputer birgt kryptologische Risiken. Bisher eingesetzte digitale Signaturverfahren (Digital Signature Schemes) sowie asymmetrische Kryptosysteme (Public Key Encryption), welche in Bezug auf klassische Computer sicher sind, können mit Quantencomputern gebrochen werden. Daher hat das National Institute of Standards and Technology (NIST) die Standardisierung von quantensichere Public-Key-Verfahren in den letzten Jahren vorangetrieben. Im Juli 2022 wurden die ersten vier quantensichere Krypto-Algorithmen durch NIST bestimmt. Darunter ist ein Algorithmus für die Verschlüsselung (CRYSTALS-Kyber) und drei Algorithmen für die digitale Signatur (CRYSTALS-Dilithium, FALCON und SPHINCS). Beim CYD Campus wurden die Kandidaten der letzten Evaluationsrunde untersucht, die codebasiert sind (Finalist «Classic McEliece», «BIKE» und «HQC») oder auf multivariaten Polynomen (Finalist «Rainbow» und «GemSS») beruhen. Da allgemein empfohlen wird, in Zukunft klassische Algorithmen mit quantensicheren Methoden zu kombinieren, wird aktuell untersucht, wie ein sicherer Mehrfachschlüsselaustausch implementiert werden kann, wenn die Algorithmen in hybrider Form verwendet werden.

Schutz vor Pulswellen Distributed-Denial-of-Service (DDoS) Angriffe

Pulswellen- Distributed-Denial-of-Service (DDoS)-Angriffe sind eine neue Art von Netzwerkangriffen, die aus kurzen, hochfrequenten Verkehrsimpulsen bestehen. Solche Angriffe zielen auf die Achillesferse moderner DDoS-Abwehrsysteme ab: ihre Reaktionszeit. Durch die kontinuierliche Anpassung ihrer Angriffsvektoren gelingt es den Pulswellenangriffen, bestehende Verteidigungsmassnahmen unwirksam zu machen. In diesem Projekt verwenden die CYD Campus Forschenden programmierbare Switches, um eine netzwerkinterne DDoS-Abwehr, die gegen Pulswellen-Angriffe wirksam ist, zu entwickeln. Dazu nutzen sie Aggregate-based Congestion Control (ACC), ein Mechanismus, der seit zwei Jahrzehnten zur Bewältigung von Überlastungsereignissen mit hoher Bandbreite existiert. Die Forschenden schlagen ACC-Turbo vor, eine überarbeitete Version von ACC, die Angriffsmuster durch die Anwendung von Online-Clustering-Techniken im Netzwerk entschärft. Auf diese Weise identifiziert ACC-Turbo Angriffe in Echtzeit und begrenzt den Angriffsverkehr effizient. Der CYD Campus hat ACC-Turbo vollständig auf P4-Switches implementiert und evaluiert es für eine Vielzahl von Angriffsszenarien.

Hacking Micro Drones

Unbemannte Luftfahrzeuge (Unmanned Aerial Vehicles - UAVs), auch als Drohnen bekannt, stellen eine Revolution im Bereich der Sicherheit und des Militärs dar. Aufgrund der jüngsten Fortschritte bei der Miniaturisierung und der sinkenden Kosten sind Mini-UAVs auch im zivilen Bereich sehr beliebt geworden. Diese Drohnen sind in der Regel zu klein und zu schwach, um mit tödlichen Waffen ausgerüstet zu werden. Dennoch stellen sie eine Bedrohung für das Militär und die Sicherheitsbehörden dar, da sie mit leistungsstarken Sensoren ausgestattet sind und zur Infiltration oder Datenerfassung über Sperrgebiete eingesetzt werden können. Das Militär und die Sicherheitsbehörden sind daher bestrebt, Fähigkeiten zu entwickeln, um der Bedrohung durch Mini-UAVs zu begegnen. Ziel dieses Projekts ist es, verschiedene Techniken zur Blockierung und Übernahme von Mini-Drohnen zu erforschen, um die von ihnen ausgehende Bedrohung zu neutralisieren. Insbesondere wird untersucht, ob es möglich ist, die drahtlosen Kontroll- und Navigationskanäle durch fortgeschrittene Signalstörungs-, Signalspoofing- und Signalmanipulationsangriffe zu diesem Zweck zu nutzen. In diesem Jahr lag der Schwerpunkt auf dem komplexen Multi-Drohnen-GPS-Spoofing, das im Labor erfolgreich demonstriert wurde.

Versuchsaufbau im Labor um Drohnen über GPS Spoofing kontrolliert zu übernehmen.

Side-channel attacks and hardware backdoors

Jedes elektronische Gerät erzeugt elektromagnetische Emissionen. Die erzeugten elektromagnetischen Signale können mit der internen Funktionsweise der emittierenden elektronischen Komponenten in Zusammenhang stehen. Ein böswilliger Angreifer kann die ausgestrahlten Signale abfangen und sie untersuchen, um Informationen über das sendende Gerät zu erhalten. Die Praxis des Abhörens und des Schutzes vor Abhören sowie deren Untersuchung wird in einem Rahmen zusammengefasst, der als TEMPEST bekannt ist. Bei Videomonitoren können die gesendeten Signale zur Rekonstruktion des Inhalts verwendet werden. Es wurde bereits gezeigt, wie ein Angreifer die Signale des Verbindungskabels zwischen einem PC und einem Videomonitor nutzen kann, um interne Informationen des Monitors zu extrahieren.

Die Forscher des CYD Campus haben gezeigt, wie ein Angreifer mit Hilfe von QR-Codes interne Daten gewinnen kann, indem er die vom Videomonitor ausgehenden Signale auswertet. Sie evaluierten und testeten systematisch verschiedene Angriffsszenarien. Die Ergebnisse zeigen, wie mit diesem Angriff grosse Mengen an Informationen von einem bis zu 50 Meter entfernten Ziel, aus verschiedenen Räumen und sogar aus verschiedenen Stockwerken gestohlen werden können. Die Arbeit führte zu einer Veröffentlichung und wurde auf der wissenschaftlichen Konferenz CRITIS 2022 in München vorgestellt.

Cloud-Umgebungen für die Datenverarbeitung

CYD Campus Forschende evaluierten das ARCA Trusted Operating System (OS), welches als Flaggschiff des Schweizer Startups CYSEC gilt. Arca Trusted OS ist ein gehärtetes Linux-basiertes Betriebssystem, das mit einem sicheren Kubernetes-Orchestrator kombiniert wird, um Intrusionen einzudämmen und die Kompromittierung von Daten in Containern vor Ort, in der Cloud und am Rande des Netzwerks zu verhindern.

Darüber hinaus bewerteten sie die Sicherheit der ARCA-Appliance (d. h. ARCA Trusted OS, das auf einem Bare-Metal-Server läuft), um mögliche Einsatzszenarien der Streitkräfte zu verstehen, bei denen diese Lösung zum Tragen kommen könnte. Zu diesem Zweck war ein besseres Verständnis dieser Lösung und ihrer Sicherheitsmerkmale erforderlich. Um dieses Ziel zu erreichen, lieferten die Forschenden des CYD Campus eine detaillierte Beschreibung der Lösung, einschliesslich der verschiedenen Module, Komponenten und Funktionen, die Teil der ARCA-Appliance sind. Sie überprüften auch die wichtigsten sicherheitsrelevanten Merkmale (d.h. HW/SW-Komponenten, Betriebssystem-Härtungsmassnahmen usw.), die den auf der ARCA-Appliance laufenden Anwendungen angeboten werden, mit dem Schwerpunkt, ob sie im Vergleich zu Alternativen ein höheres Sicherheitsniveau bieten und ob sie für die Verwendung im Kontext der Streitkräfte geeignet sind.

Schutz von unsicheren Avionik-Systemen

Dieses Forschungsprojekt befasst sich mit der Analyse von Schwachstellen in der Avionik-Hardware und den damit verbundenen drahtlosen Protokollen. In den vergangenen Jahren haben CYD Campus Forschende mit Hilfe des Avionik-Labors in Thun Angriffe auf die Technologien ADS-B (Automatic Dependent Surveillance–Broadcast), CPDLC (Controller-Pilot Data Link Communications) und FLARM sowohl theoretisch als auch in der Praxis analysiert. FLARM ist ein Kollisionswarngerät für Leichtflugzeuge und Drohnen, das in der Schweiz entwickelt wurde und weltweite Beachtung und Verbreitung gefunden hat. Im Jahr 2022 widmeten sich die Forschenden der praktischen Analyse des Kollisionswarnsystems TCAS (Traffic Collision Avoidance System), das in grösseren Flugzeugen eingesetzt wird. Darüber hinaus wurden die Auswirkungen von Hochfrequenzstörungen des Global Positioning System (GPS) in Verkehrsflugzeugen, insbesondere nach dem Ausbruch des Ukraine-Krieges, untersucht. Beide Aktivitäten werden im Jahr 2023 neben praktischen Angriffen auf CPDLC und einer Sicherheitsanalyse der europäischen U-Space-Technologiekandidaten fortgesetzt.

Cyber in der Luft- und Raumfahrt

Cybersicherheit in der Luft- und Raumfahrt ist seit der Gründung des CYD Campus ein zentrales Forschungsthema. Im Aerospace gibt es viele grundlegende Gemeinsamkeiten, auch im Bereich der Cybersicherheit. So werden zum Beispiel viele veraltete Technologien verwendet, die oft schon seit 20 oder sogar 40 Jahren unverändert im Einsatz sind. Insbesondere im Bereich der drahtlosen Kommunikationstechnologien führt diese Tatsache zu fundamentalen Sicherheitsproblemen, da die Inhalte weder verschlüsselt noch authentifiziert sind. Doch selbst dort, wo Inhalte verschlüsselt werden, geschieht dies oft nicht mit offenen, sicheren Standards, sondern mit schwachen proprietären Systemen, die dem Kerkhoff'schen Grundsatz über sichere Kryptosysteme widersprechen. In diesem Jahr hat der CYD Campus im Rahmen seiner Arbeiten an der Avionik-Datenverbindung ACARS (Aircraft Communication Addressing and Reporting System) mehrere solcher Verfahren identifiziert, die in einem Strom von gemischten Daten (verschlüsselt, unverschlüsselt und schwach verschlüsselt) automatisch erkannt werden können. Weitere Arbeiten zur Entschlüsselung einiger der gefundenen Chiffren sind im Gange.

Deep Learning for Security (Steganografie)

Zwischen kriminellen Abhörern und hochmodernen sicheren Kommunikationssystemen findet ein ständiges Wettrüsten statt, das die kontinuierliche Weiterentwicklung bestehender Protokolle sowie neuartige Methoden und Modellierungsansätze zur Analyse von Cyber-Bedrohungen durch reale Seitenkanalangriffe erfordert. Ein besonders wichtiges Merkmal leistungsstarker kryptografischer Protokolle ist die Fähigkeit, Verschlüsselung unter plausibler Bestreitbarkeit durchzuführen, da der alleinige Einsatz von Verschlüsselungsverfahren von repressiven Regimen auf der ganzen Welt zunehmend ins Visier genommen wird und kryptografische Kanäle, die beispielsweise auf VPNs beruhen, häufig blockiert werden. In diesem Projekt wurden neuartige, nachweislich sichere Methoden für die steganografische Kommunikation in Texten entwickelt, die auf Forschungen zum Deep Multi-Agent Reinforcement Learning in kooperativen Spielen basieren. Es ist geplant, diese Methode weiter zu verfeinern und auf andere Kommunikationsarten wie Audio zu erweitern.

Sicherheit von elektrischen Fahrzeugen und Ladeinfrastrukturen

Im Zuge der Umstellung des VBS auf Elektrofahrzeuge muss auch die Sicherheit der vorhandenen Ladeinfrastrukturen überprüft werden. Es wurden bereits Vorarbeiten geleistet, die gezeigt haben, dass bei bestimmten Systemen, die die so genannte Power Line Communication (PLC) nutzen, der Datenfluss aus der Ferne drahtlos abgefangen werden kann. Dies kann verschiedene Auswirkungen auf die Sicherheit und den Datenschutz von Fahrzeugen und Infrastruktur haben. Während des CYD Campus Car Hackathon in Thun im Oktober 2021 wurde ein aktiver Angriff auf ein Ladesystem entwickelt, bei dem ein aufwandsarmer, sogenannter Denial-of-Service (DoS)-Angriff den Ladevorgang drahtlos unterbricht und beendet. Der als Brokenwire bezeichnete Angriff wurde dem nationalen Zentrum für Cybersicherheit gemeldet, und alle beteiligten Forschenden sind im Austausch mit den Auto- und Ladeherstellern, um ihn zu entschärfen. Die Analyse solcher Angriffe und möglicher Gegenmassnahmen wurde im Laufe des Jahres 2022 durchgeführt.

Untersuchung von Sicherheitsschwachstellen bei elektrischen Fahrzeugen und Ladeinfrastrukturen in Thun.

4.2 Projekte Bereich Data Science

Verteilte IoT Sensoren: Hardware- und Verhaltensanalyse

Internet-of-Things (IoT)-Geräte sind heute in zahlreichen Anwendungsfällen allgegenwärtig, einschliesslich im militärischen Kontext, was sie zu einem attraktiven Ziel für Cyberangriffe macht. Leider legen die Hersteller beim Entwicklungsprozess weder bei der Hardware noch bei der Software den Schwerpunkt auf die Sicherheit. Zum Beispiel verfügen die weit verbreiteten IoT-Geräte nicht über eine fälschungssichere Kennung, so dass sie leicht imitiert werden können. Durch die Betrachtung von Hardwareunterschieden, wie z. B. der Uhrendrift, trainieren CYD Campus Forschende Modelle für maschinelles Lernen, um Hardware-Fingerabdrücke zu erkennen, die eine eindeutige Identifizierung eines IoT-Gerätes ermöglichen. Diese Fingerabdrücke könnten in Zukunft als zusätzliche Sicherheit in verschiedenen Anwendungen verwendet werden. Ebenso erstellen sie Software-Fingerabdrücke, die das normale Verhalten eines IoT-Geräts modellieren. Der Campus trainiert Modelle des maschinellen Lernens, um zu erkennen, ob sich ein Gerät auf unerwartete Weise verhält, was die Erkennung von Cyberangriffen wie beispielsweise Botnets oder Ransomwares ermöglicht. Zu diesem Zweck werden Metriken wie Prozessaufrufe und Ressourcenzuweisungen aus dem Betriebssystem verwendet.

Verteilte IoT-Sensoren: Modulationsklassifizierung und kollaboratives IoT

Das elektromagnetische Spektrum ist eine vielseitig genutzte Ressource und gleichzeitig für zahlreiche Systeme, wie z. B. Telekommunikation, Radar und Ortung, entscheidend. Deshalb muss es vor Cyberangriffen, welche diese Systeme beeinträchtigen könnten, geschützt werden. Automatische Algorithmen zur Modulationsklassifizierung versuchen Modulationen zu identifizieren. Einige Expertensysteme und Ansätze, die auf maschinellem Lernen basieren, liefern zwar gute Ergebnisse, haben aber Probleme, wenn sie mit unbekannten Parametern zu tun haben, wie z. B. mit dem Kanal oder der Sampling-Rate, für die sie nicht trainiert wurden. In diesem Projekt werden die Transfer-Learning-Methoden erforscht, die den Einsatz kostengünstiger Software Defined Radios ermöglichen. Dank des Transfer-Lernens ist der CYD Campus in der Lage, Modulationen unter bisher unbekannten Bedingungen zu klassifizieren, die bei traditionellen Ansätzen normalerweise zu Fehlklassifikationen führen.

Arbeitsgruppe Künstliche Intelligenz mit den USA

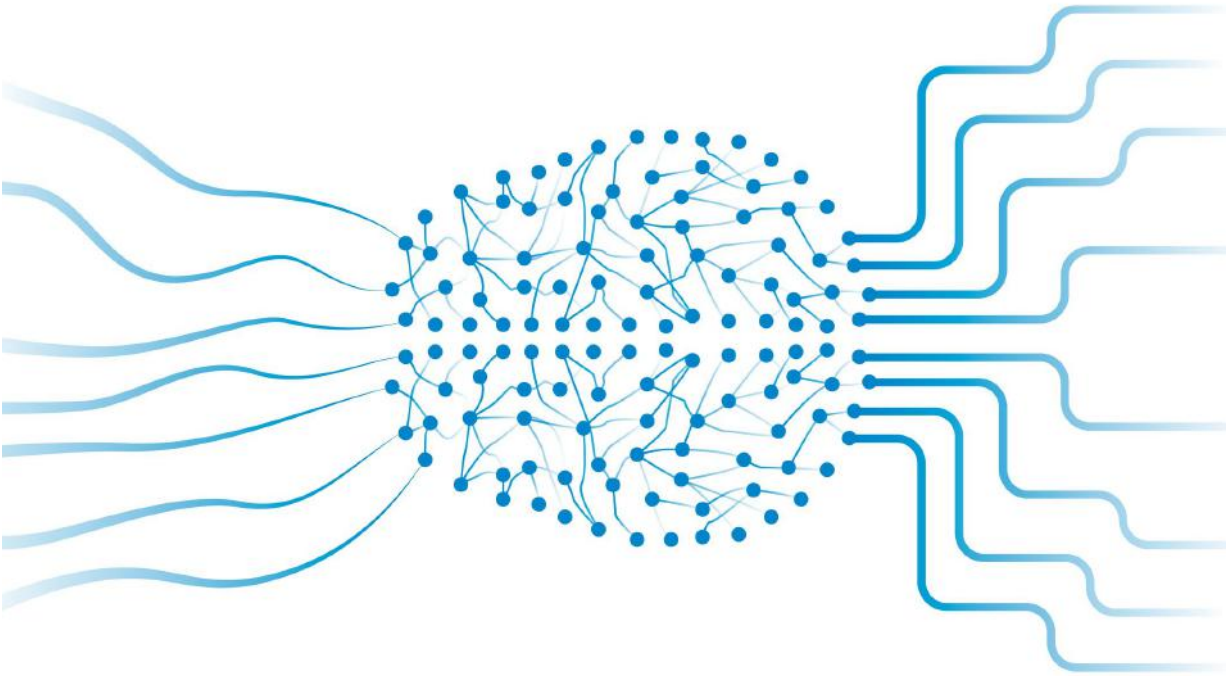
Vertretende des CYD Campus und des US-Verteidigungsministeriums tauschen sich seit mehreren Jahren regelmässig zum Thema Künstliche Intelligenz aus. Dabei wurden insbesondere gemeinsame Grundlagenkenntnisse in diesem Bereich gewonnen und entsprechende Anwendungen identifiziert. Hierzu wurden aktuelle technische Möglichkeiten untersucht, mögliche Technologielösungen entwickelt und gemeinsame Aktivitäten initiiert. Identische Interessensgebiete bestehen bei der Überwachung neuer Technologien, dem Internet der Dinge sowie dem dezentralen maschinellen Lernen. Im Jahr 2022 wurde zusammen mit dem US Army Research Lab eine NATO Arbeitsgruppe (IST-ET-121) aufgestellt und gemeinsam geleitet. In diesem Rahmen fanden alle vier Wochen Sitzungen statt, welche den internationalen Teilnehmern der Arbeitsgruppe (CHE, USA, CAN, SWE, ESP, GER, CCDCOE) ermöglichte über die Anwendung von maschinellem Lernen auszutauschen.

Informationsbeschaffung Cyberspace: Stratosphäre

Um Daten analysieren zu können, muss man sie erst einmal beschaffen. Der Cyberspace ist zwar de facto ein eigener Raum, Cyberrisiken können sich heutzutage jedoch auch auf den Luft- und Weltraum auswirken, etwa auf Flugzeuge und Satelliten. Daher ist es wichtig, die Cyberrisiken in einer mehrdimensionalen Umgebung zu betrachten. In diesem Projekt wird beabsichtigt, Daten an einem strategischen Ort zu sammeln, nämlich in der Stratosphäre. Diese ist besonders interessant, da sie sich zwischen Satelliten und der Erde befindet. Das bedeutet, dass die Forschenden des CYD Campus in der Lage sind, Signale zu sammeln und zu orten. Zu diesem Zweck entwickeln sie eine Höhenplattform, die von einem Wetterballon getragen wird. Die Nutzlast wird ein Software Defined Radio enthalten, das Signale und Kommunikation empfangen und Sender auf der Erde oder im Weltraum orten kann.

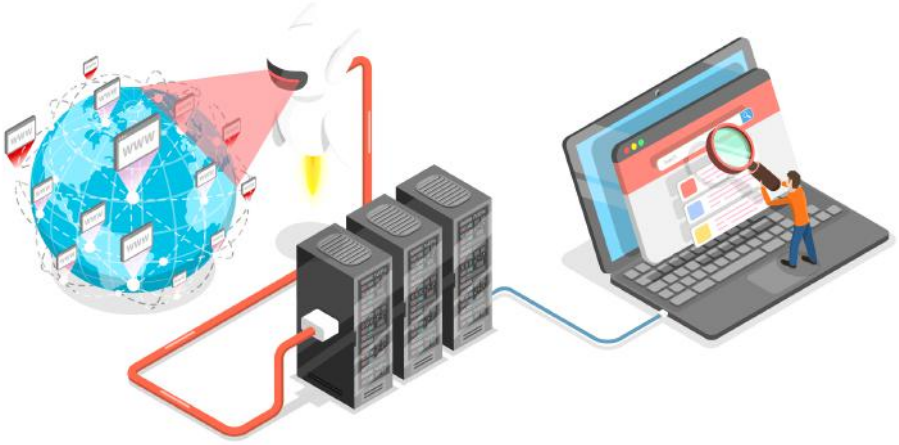
Computer gestützte Datenanalyse: Robustheit von Deep Learning Modellen

Machine Learning Modelle haben in den letzten Jahren an Bedeutung gewonnen. Sie kommen nicht mehr nur in speziellen Fachanwendungen zum Einsatz, sondern sind in vielen Anwendungen zu finden, darunter auch in Smartphones zur Erkennung der Nutzeraktivitäten. Aus dieser Beobachtung lässt sich eine zentrale Frage ableiten: Sind diese Modelle robust gegenüber Angriffen? Es scheint, dass die überwiegende Mehrheit der Modelle leicht von einem Angreifer bzw. einer Angreiferin überwunden werden kann. Da dies in einem militärischen Kontext verheerende Folgen haben könnte, müssen die Modelle gegen gegnerische Angriffe robust gemacht werden. In diesem Projekt befassen sich Mitarbeitende des CYD Campus mit Deep Learning Modellen und untersuchen Methoden, um ihre Robustheit zu erhöhen. Zu diesem Zweck haben sie die Trainingsmenge mit gegnerischen Stichproben erweitert, die von Angreifenden verwendet werden könnten. Die Ergebnisse zeigen, dass die Robustheit von Modellen, die mit solchen gegnerischen Mustern trainiert wurden, im Vergleich zur normalen Genauigkeit zunimmt.



Erkennung von Fakes in sozialen Medien: Effiziente Identifizierung von Fehlinformationen und Desinformationen in sozialen Medien

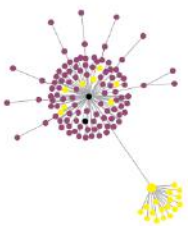
Im Falle einer sich schnell ausbreitenden Pandemie ist es notwendig, schnell relevante Informationen über die Krankheit zu erhalten. Twitter ist ein beliebtes Medium, um sich in Echtzeit über globale Ereignisse zu informieren. Das Netzwerk dient jedoch auch der Verbreitung von Fehlinformationen. Irreführende Online-Inhalte haben zahlreiche Menschen zu einer Reihe von Annahmen verleitet, die eine Gefahr für sie selbst und für die Gesellschaft im Allgemeinen darstellen. Wir konnten beobachten, wie Menschen die Existenz der Pandemie leugnen, glauben, dass Impfstoffe gefährlicher sind als das Virus selbst, und gewaltsam gegen die von den Regierungen ergriffenen Massnahmen zur Eindämmung der Pandemie protestierten. Ziel dieses Projekts ist die Entwicklung einer robusten Methode zur Erkennung von Fehlinformationen in den sozialen Medien (insbesondere Twitter), die vom jeweiligen Anwendungsbereich unabhängig ist, indem ereignisspezifische Fehlinformationen zu beliebigen Themen schnell klassifiziert und die absichtlichen Versuche der Manipulation der öffentlichen Meinung durch die sozialen Medien identifiziert werden.



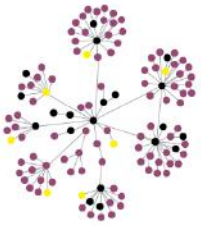
Erkennung von Fakes in sozialen Medien: Identifizierung von Radikalisierung

Verdächtiges Verhalten in sozialen Medien wird unter verschiedenen Bezeichnungen wie Fake News, Desinformation, kompromittierte Konten, Identitätsbetrug, Propaganda, Hassreden oder Radikalisierung beschrieben. Alle genannten Verhaltensweisen haben eine gemeinsame Eigenschaft: Sie spalten die Gesellschaft. Das Projekt zielt darauf ab, Radikalisierungsereignisse für einzelne Nutzer in sozialen Medien zu erkennen und vorherzusagen. Die Grundannahme ist, dass die meisten Menschen, die sich radikalisieren, nicht von Anfang an so eingestellt sind. Radikalisierung ist ein Prozess, der sich im Laufe der Zeit entwickelt. Dieser Prozess kann insbesondere eine allmähliche Verschiebung hin zu immer extremeren Positionen sein. Auch wenn die Grenze zwischen Radikalisierung und Nicht-Radikalisierung fliessend sein kann, wird dieser Prozess vereinfacht und binarisiert. Da das Hauptziel des Projekts die Vorhersage von Radikalisierungsereignissen ist, ist es notwendig, den Zeitpunkt zu definieren, an dem eine Verschiebung hin zu einer radikalen Haltung stattgefunden hat. Die lexikalische Diversität der Beiträge eines Nutzers ist in der Regel in dem Zeitraum, in dem das Radikalisierungsereignis eintritt, hoch und danach geringer, weshalb CYD Campus Forschende diese Information als Indikator für eine Verhaltensänderung verwenden. Durch die Ermittlung der einflussreichsten Merkmale im Informationsfluss ist es möglich, Frühwarnsignale zu geben, wenn die Tendenz zur Radikalisierung festgestellt werden kann.

Tweets Verbreitungsbaum



von Fake News



von echten Nachrichten

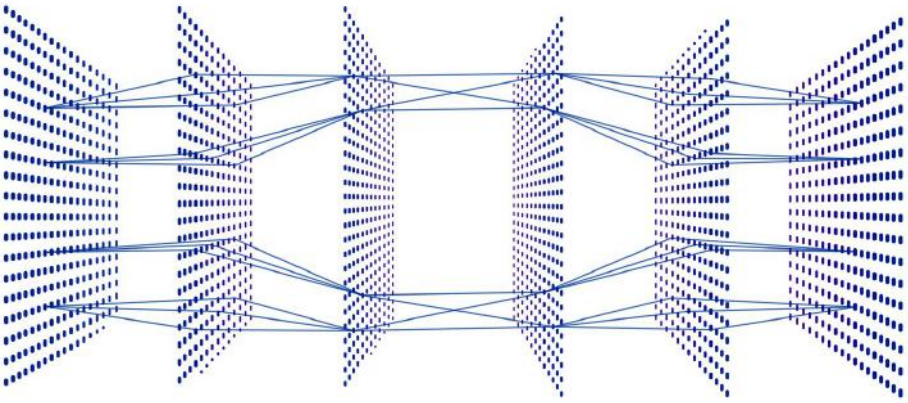
- der zentrale Wurzelknoten zeigt einen Nachrichtenbericht an;
- die schwarz markierten Knoten zeigen die hoch einflussreiche Nutzer;
- die pink markierten Knoten zeigen Retweets;
- die gelb markierten Knoten zeigen Zitate der originalen Nachricht oder von einem Retweet.

Untersuchung multimodaler Embeddings zur Charakterisierung von Informationsoperationen

Informationsoperationen sind in den sozialen Medien allgegenwärtig geworden, weshalb die Nachfrage nach Werkzeugen, die solche Inhalte identifizieren, verfolgen und analysieren können, gestiegen ist. Beiträge in sozialen Medien sind oft multimodal, d.h. sie bestehen mitunter oft aus Text- und Bildinhalten. Jüngste Fortschritte im Bereich des Deep Learning ermöglichen die Nutzung von Datensätzen im Internet, um hochdimensionale uni- und multimodale Daten auf niedrigdimensionale Darstellungen zu verdichten, die für nachgelagerte Aufgaben verwendet werden können. Ziel ist es, zu untersuchen, ob solche Modelle zur Analyse von Informationsoperationen auf Twitter unter Verwendung von Zero- und Few-Shot-Learning eingesetzt werden können. Untersucht wurde die Fähigkeit solcher Modelle, Bildtypen, Themen und die Emotionalität von Beiträgen in den sozialen Medien zu charakterisieren.
Im Bereich der Emotionalität von Bilddaten wurde in diesem Rahmen eine neuartige Zero-Shot-Methode unter Verwendung von Contrastive Language-Image Pre-Training (CLIP) und speziell konstruierter Textbausteine implementiert, um die Valenz eines bestimmten Bildes zu klassifizieren (11-stufige Likert-Skala, von 1 sehr negativ bis 11 sehr positiv mit 6 als neutralem Wert). Es konnte gezeigt werden, dass der CLIP-basierte Ansatz eine bessere Leistung bei der Vorhersage von Valenzwerten erzielt als weit verbreitete Baseline-Methoden (ResNet-Architekturen). Darüber hinaus wurde eine Methode zur Klassifizierung von 6 Grundemotionen (+1 neutrale Emotion) implementiert, die eine Kombination aus eingebetteten CLIP-Merkmalen und traditionellen Methoden des maschinellen Lernens (SVM, Random Forests, logistische Regression) verwendet.
Zusammenfassend lässt sich sagen, dass das Projekt ein solides theoretisches und praktisches Verständnis von CLIP für Zero-/Few-Shot-Klassifikationsaufgaben im Kontext der Analyse von Informationsoperationen liefert. Darüber hinaus wurde eine API entwickelt, die die entwickelten Algorithmen implementiert und zu Demonstrationszwecken und zur Untersuchung der Machbarkeit zur Verfügung steht. Die Experimente haben die Wirksamkeit grosser vortrainierter Modelle für die Klassifizierung nach verschiedenen Merkmalen von Posts in sozialen Medien demonstriert. Solche Modelle können eine entscheidende Rolle bei der dynamischen Analyse dieser Datensätze spielen.

Automatische Klassifizierung von Bildinformationen: Authentifizierung und Integrität von Videos gegenüber Manipulationen

Ziel dieses Forschungsprojekts ist die Entwicklung einer Methode, die eine digitale Signatur von Videodaten implementiert. Mittels einer solchen Signatur soll es möglich sein, die Authentizität der Videodaten (d.h. Herkunft und Integrität des Inhalts) zu überprüfen. Ein solches Verfahren ist insbesondere im Hinblick auf die zunehmende Bedrohung durch manipulierte Videoinhalte (z.B. Deep Fake-Videos) von grosser Bedeutung. Offiziell produzierte Videoinhalte könnten z.B. mit einer digitalen Signatur versehen werden, die wiederum vom Empfänger elektronisch verifiziert werden kann. In diesem Sinne kann die elektronische Signatur als präventive Massnahme gegen manipulierte Videoinhalte gesehen werden. Für die Umsetzung wird an einer Kombination von kryptographischen Primitiven mit modernen Deep Learning Methoden (sogenannte Vector-Quantized Variational Autoencoders) geforscht. Ein erster funktionsfähiger Prototyp ist für kurze Videosequenzen verfügbar.



Multimodale Informationsbeschaffung und -fusion: Erfassung und Visualisierung von Datenflüssen in der Onlinewerbebranche

In diesem Forschungsprojekt werden Methoden zur client-basierten Erfassung und Visualisierung von Datenflüssen an Dritte (Third-Parties) in Zusammenhang mit Onlinewerbung untersucht. Das Ziel dieses Projekts ist es besser zu verstehen, was für Datenflüsse an Third-Parties entstehen, wenn man sich im Internet bewegt. Es wurde bereits gezeigt, dass Onlinewerbung nebst dem Sammeln von personenbezogenen Informationen auch zur Finanzierung von Plattformen für die Verbreitung von Desinformation und Malware verwendet wird. In diesem Projekt entstand daher eine Plattform, die zur Sensibilisierung von Mitarbeitenden für diese Themen eingesetzt werden kann. Dabei wurde auf das Tool «webXray» für die Analyse und D3.js für die Darstellung der Daten zurückgegriffen. Die Visualisierungen umfassen Netzwerke, die einen Eindruck über wirtschaftliche Beziehungen zwischen Webseiten und Third-Parties vermitteln, sowie auch deskriptive Statistiken, welche Aufschluss über das Ausmass der gesammelten Daten vermitteln.

Erkennung von Cyberangriffen auf elektrische Systeme

Die Energiewende verändert die Topologie der Stromnetze. Der Ausstieg aus der Kernenergie und die zunehmende Elektrifizierung der Verkehrsmittel zwingen die Stromnetze dazu, nach neuen Betriebsmodi zu arbeiten. Es ist daher zu erwarten, dass die Produktions- und Verbrauchsmuster in den kommenden Jahren durch zunehmende Unsicherheit und grössere Schwankungen geprägt sein werden. Dieser Wandel wirkt sich auch auf die Cybersicherheit dieser Netze aus. Die neuen Bedingungen erfordern von den Netzwerkakteuren, insbesondere den Betreibern, mehr Flexibilität und kürzere Reaktionszeiten sowie neue Instrumente für die Cybersicherheit. Der CYD Campus entwickelt Methoden des maschinellen Lernens, um bestimmte Arten von Cyberangriffen zu erkennen. Insbesondere konnte durch die Analyse von Produktions- und Verbrauchszyklen gezeigt werden, dass Verzerrungs- und Wiederholungsangriffe schnell und effizient erkannt werden.

Frühwarnsignale in OSINT: Antizipation von Konflikten

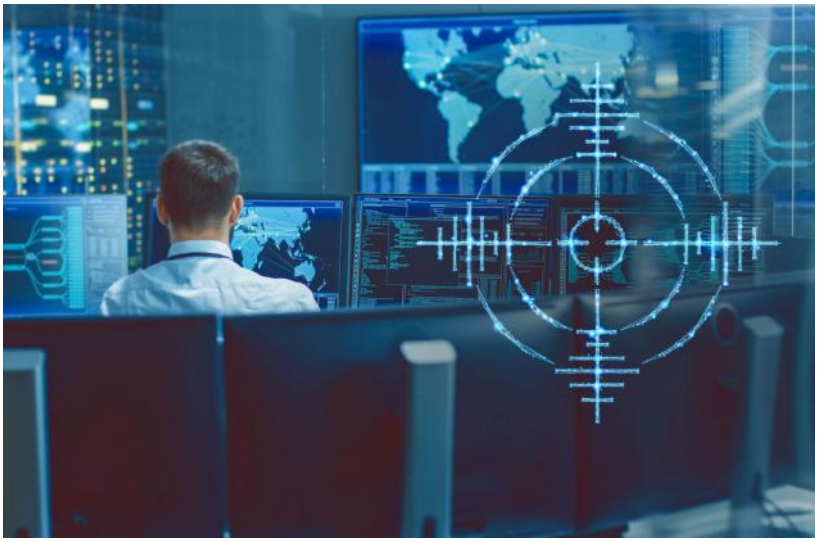
Die Antizipation von Konflikten ist eine wichtige Aufgabe für Regierungen und Streitkräfte. Das Wissen um potenzielle Konflikte oder Instabilitäten kann die geopolitische Strategie weitgehend beeinflussen und eine bessere Vorbereitung ermöglichen. In letzter Zeit haben mehrere offene Quellen damit begonnen, Daten zu sammeln, die für die Konfliktvorhersage von entschei dender Bedeutung sein können. In diesem Zusammenhang ist die ACLED-Datenbank (The Armed Conflict Location & Event Data Project) zu nennen, die zahlreiche tägliche Berichte über Demonstrationen, Proteste, Unruhen und Todesopfer aus vielen Ländern enthält. Die Mitarbeiter des CYD Campus entwickelten statistische Methoden, um so genannte Tipping Points, die einen Richtungswechsel anzeigen, zu identifizieren und vorherzusagen. Soziale Medien wurden auch genutzt, um soziale Instabilitäten mithilfe von Techniken des maschinellen Lernens zu modellieren und zu erkennen.

Data-Science-Methoden für Technologie- und Marktmonitoring: Erweiterung und Verknüpfung der Taxonomie

Um Technologie- und Marktentwicklungen zu verfolgen, muss man in der Lage sein, Technologien zu erkennen, sie zu unterscheiden und ihre Beziehungen zueinander zu verstehen. Unter Verwendung der technologiebezogenen Konzepte in- nerhalb des Wikipedia-Graphen wird beim CYD Campus eine Methode zur Identifizierung der realen Position eines neuen Kon zepts innerhalb einer bestehenden Taxonomie auf der Grundlage semantischer und relevanter Ähnlichkeiten vorgeschlagen. Darüber hinaus wird ein Rahmen für die Erkennung des technologiebezogenen Konzepts in einem unstrukturierten Text geschaf fen, indem der Ansatz des Concept Tagging verwendet wird, der keine Extraktion der Oberflächenform aus dem Rohtext beinhaltet. Auf diese Weise ist es möglich, sich auf den semantischen Inhalt eines Dokuments und nicht auf seine Textform zu konzentrieren und Konzepte zu erkennen, die nicht ausdrücklich im Text erwähnt werden. Darüber hinaus kann die Beant- wortung von Fragen als zugrundeliegende Aufgabe genutzt werden, um sowohl die Technologien miteinander zu verknüpfen als auch die Technologien mit den Unternehmen, die sie bearbeiten.

Data Science-Methoden für Technologie- und Marktmonitoring: Früherkennung und Überwachung von Technologien

Ziel des Projekts ist es, ein Online-Monitoring von Technologien und Technologie-Akteuren in öffentlich zugänglichen Informationsquellen durchzuführen. Das Monitoring bezieht sich auf die frühzeitige Erfassung von Erwähnungen neuer Techno- logien, von Akteuren im Technologiebereich und von Fakten im Zusammenhang mit neuen Beziehungen zwischen Technologien und Technologieakteuren. Das Ziel dieses Projekts ist es, die folgenden Forschungsfragen zu beantworten: «Wie wird Neuheit erfasst?», «Können wir Modelle trainieren, um Neuheit zu erfassen und zu identifizieren?» und «Können wir die Menge der Informationen, die der Benutzer verarbeiten muss, reduzieren?». CYD Campus Forschende beantworten diese Fragen, indem sie die gegebene Aufgabe in eine Frage/Antwort-Aufgabe umwandeln und dabei die vorab trainierten Sprachmodelle in einem Zero-Shot- und Fine-Tuned-Setting nutzen.



Maschinelles Übersetzen: Identifizierung von Dialekten

Die Identifizierung von Sprachdialekten ist aus der Perspektive der Linguistik und der algorithmischen Verarbeitung natürlicher Sprache eine sehr anspruchsvolle Aufgabe. In diesem Projekt lag der Schwerpunkt auf der Entwicklung von Methoden zur Identifizierung von Sprachen in kurzen Textproben (z. B. Social-Media-Posts, Kurznachrichten), wobei der Schwerpunkt auf dem verrauschten Text und der Ähnlichkeit der Sprachen lag. Um diese spezifischen Herausforderungen zu bewältigen, entwickeln die Forscher einen Sprach-/Dialekt-Klassifikator, der robust gegenüber Rauschen ist, wobei unter «Rauschen» jede Abweichung von der Standard- oder bekannten Schrift verstanden wird. Als Einheiten, auf denen die Klassifizierung beruht, fokussieren sich die Forscher auf Zeichen und Teilwörter. Der Wechsel von der Wort- zur Teilwort-Tokenisierung eröffnet einen weiten Spielraum für Tokenisierungsmöglichkeiten: Jeder beliebige Substring eines Wortes (Teilwort) ist potenziell ein gutes Token, insbesondere für die Dialektidentifikation, bei der subtile lexikalische Unterschiede auf der Teilwortebene verborgen sein können. Darüber hinaus kann die Wahl der besten Teilwort-Tokenisierungsmethode von der zu verarbeitenden Sprache und der nachgelagerten Aufgabe abhängen.

Maschinelles Übersetzen: Universal Adversarial Perturbations

Dieses Projekt zielt darauf ab, Universal Adversarial Perturbations (UAP) zu untersuchen, die verschiedene moderne Deep Learning Modelle für die Aufgabe des Natural Language Processing (NLP) und insbesondere für die Aufgabe der Textübersetzung täuschen würden. Im Gegensatz zur Bildverarbeitung wurden Angriffe auf NLP- und neuronale maschinelle Übersetzungssysteme (NMT) bisher nur wenig untersucht. Da NMT-Systeme in hochsensiblen Anwendungen eingesetzt werden, ist die Erforschung gegnerischer Angriffe, insbesondere UAPs, für das NMT-Modell von entscheidender Bedeutung. Durch die Entwicklung eines Algorithmus zur Generierung von UAPs wird versucht, die Verwundbarkeit von NMT-Systemen zu analysieren und ihr Verhalten zu verstehen, indem die Existenz von UAPs erklärt wird. Das Projekt konzentriert sich auf universelle Angriffe auf NLP- und NMT-Systeme. Beispielsweise wird ein White-Box-Angriffsszenario betrachtet, bei dem die Forschenden Zugang zu den Parametern des Modells, seiner Struktur und den Trainingsdaten haben. White-Box-Angriffe sind interessanter als Black-Box-Angriffe, da sie eher zielgerichtet sind. Ein Blackbox-Angriff simuliert realitätsnah den Angriff eines typischen Internet-Hackers. White-Box-Angriffe beziehen sich auf einen Angriff mit bestimmten Detailkenntnissen über die innere Funktionsweise des Systems. White-Box-Angriffe decken in der Regel mehr Schwachstellen des NMT-Modells auf, da sie auf die Modellparameter zugreifen können. Die Forschenden bewerten auch die Übertragbarkeit der vorgeschlagenen White-Box-Angriffe auf Black-Box-Einstellungen, welche in der Praxis eher anwendbar sind. Dieses Projekt ermöglicht eine bessere Charakterisierung der Anfälligkeit von NMT-Systemen und zeigt die Notwendigkeit auf, starke Verteidigungsmechanismen und robustere NMT-Systeme für reale Anwendungsfälle zu entwickeln.

Maschinelles Übersetzen: Familien von Sprachen und Dialekten

Die maschinelle Übersetzung hat seit der Einführung von Modellen neuronaler Netze erhebliche Fortschritte gemacht, und sogenannte Transformatoren sind derzeit Standard für Sprachpaare mit einer grossen Menge an parallelen Übersetzungsdaten, sogenannte ressourcenstarke Sprachpaare. Für Sprachpaare mit schwachen Ressourcen oder im Falle komplett fehlender paralleler Übersetzungsdaten ist zusätzlicher Aufwand erforderlich. Der Schwerpunkt dieses Projekts liegt auf Lösungen für den Umgang mit einer ressourcenschwachen Sprache, wenn ressourcenreiche Sprachen aus derselben Familie verfügbar sind. Um die ersten Übersetzungsmodelle zu trainieren, wurde Transfer-Learning unter Verwendung verschiedener Hochsprachen eingesetzt, das von den Forschern auf die gegebene ressourcenarme Sprache feinabgestimmt wurde. Darüber hinaus wird die Rückwärtsübersetzung als Technik zur Erweiterung der parallelen Übersetzungsdaten eingesetzt, wenn nur einsprachige Quellen zur Verfügung stehen. Alle diese Techniken verbessern nachweislich die Qualität der Übersetzung in ressourcenarmen Umgebungen. Darüber hinaus wurde die «unsupervised» NMT durch eine Vereinfachung der bestehenden Architekturen praktisch ohne Leistungsverlust verbessert, gefolgt von einem Algorithmus zur adaptiven Planung der Trainingsaufgaben. Des Weiteren haben die Wissenschaftlerinnen und Wissenschaftler die Tokenisierungs-Modelle optimiert, indem sie entweder ein Alignment von Teilwörtern in der Ausgangs- und Zielsprache oder eine neue Methode zur Konstruktion von Teilwörtern verwendet haben.

5 Kunden und Portfolio Auswertung

Das Cyber Dispositiv des Bundes ist in drei Bereiche eingeteilt: Cybersicherheit (EFD), Cyberverteidigung (VBS) und Cyberstrafverfolgung (EJPD). Der CYD Campus erbringt primär Leistungen für den Bereich Cyberverteidigung. Dank den Synergien, insbesondere im technologischen Bereich, profitieren aber auch die anderen zwei Bereiche von den Leistungen des CYD Campus. Direkte Leistungen werden jährlich in Dienstleistungsvereinbarungen festgehalten. Der CYD Campus erbrachte im 2022 Leistungen zu Gunsten der Beschaffung, Verteidigung und Verwaltung.

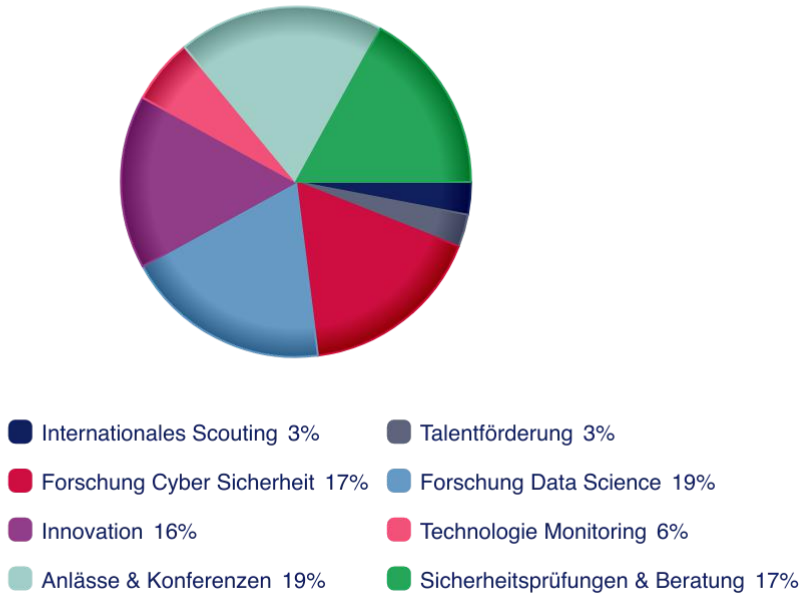
Im 2022 wurden, unter anderem, für nachfolgende Organisationen Arbeiten geleistet:

- armasuisse
- Gruppe Verteidigung
  - Armeestab
  - Projekt Kommando Cyber
  - Führungsunterstützungsbasis der Armee (FUB)
  - Kommando Operationen
  - Kommando Ausbildung
- Nachrichtendienst des Bundes
- Eidgenössisches Finanzdepartement – Nationales Zentrum für Cybersicherheit NCSC
- Bundesamt für Bevölkerungsschutz
- Bundesamt für Polizei fedpol

Die Auswertung der CYD Campus Portfolios für das Jahr 2022 ist in unterer Abbildung dargestellt. Die wichtigsten Kernleistungen lagen in den Bereichen Forschung, Innovation, Sicherheitsprüfungen und Beratung sowie in der Durchführung von Veranstaltungen für die Cyber-Community. Die Legende in der Tabelle gibt Aufschluss über die Verteilung der Aufträge, die im Rahmen der Portfolios im Jahr 2022 bearbeitet wurden.

Hinweis: Aus Klassifikationsgründen werden die Auftragsleistungen im Jahresbericht nicht detaillierter beschrieben.

Portfolio-Auswertung CYD Campus
2022



6 Innovation

Der CYD Campus unterstützt technologische Innovationen für Verwaltungseinheiten und die Verteidigung mit einer Technologiereife (TRL) von 4 bis 6.
Ziel der Innovationsprojekte ist beim Kunden bzw. Auftraggeber Resultate der Forschung oder neue Bedürfnisse in Form von Demonstratoren umzusetzen und die Anwendbarkeit der Technologie beim Kunden in der Praxis zu beweisen.

6.1 Resultate der Innovationsprojekte

Aus Klassifikationsgründen können keine expliziten Resultate präsentiert werden, weshalb eine generische Übersicht ausgewählter Resultate gewährt wird.

Secure Smartphone

Ziel des Projekts ist die Verbesserung der Sicherheit eines Smartphone-Betriebssystems durch die Integration von Virtualisierung und der SCION-Technologie. SCION ist eine innovative Internet-Architektur, die robuste Sicherheit, effiziente Paketweiterleitung und skalierbare Routing-Funktionen bietet, indem sie Netzwerke in isolierte Domänen organisiert. In diesem Projekt wurde ein SCION-Gateway in Android integriert, das den gesamten nativen Applikationsdatenverkehr durch das sichere SCION-Netzwerk leitet. Virtualisierung wurde eingesetzt, um Sicherheitsrisiken zu isolieren und mehrere Instanzen des Android-Betriebssystems bereitzustellen, die jeweils ein unterschiedliches Mass an Vertraulichkeit aufweisen. Unter Verwendung von Android 13 und einem Pixel 6-Gerät hat das Projekt erfolgreich die Fähigkeit demonstriert, Linux auf einer virtuellen Maschine auf einem Smartphone auszuführen und dabei zum ersten Mal das native Display zu nutzen.

SCION-Technologie

Der CYD Campus hat am Aufbau eines SCION-Netzwerks gearbeitet, das die drei CYD Campus Standorte in Thun, Lausanne und Zürich verbindet.
Das Ziel im Jahr 2022 war es, ein SCION-Testbed einzurichten, um diverse state-of-the-art Netzwerkangriffe und Abwehrmassnahmen zu testen: Sichere Routing-Techniken, einschliesslich explizites Path-Routing, sichere Routenbestätigung, Abwehr von Distributed Denial-of-Service (DDoS)-Angriffen und Verkehrsverschleierung.
Im November 2022 wurde eine funktionale Verbindung zwischen den Standorten des CYD Campus über unabhängige Dienstleistungsanbieter hergestellt und erfolgreich getestet, wodurch die weitere Erforschung des SCION-Protokolls sichergestellt wird.

Inbetriebnahme des SCION-Testbed mit Toni Eder, Generalsekretär VBS und Ivo Stragiotti, Mitarbeiter CYD Campus.

5G

5G ist die neueste Generation von Mobilfunknetzen, die im Vergleich zu früheren Generationen erhebliche Fortschritte bei Geschwindigkeit, Kapazität und Konnektivität bietet. Derzeit stützt sich 5G noch auf das vorherige 4G-Netz als Backbone, aber die vollständige 5G-Stand-Alone-Architektur (SA) wird in Zukunft für die kommerzielle Nutzung eingeführt werden. 5G SA führt neue Funktionen wie Network Slicing ein, aber auch neue Sicherheitslücken, die es zu schliessen gilt. Der CYD Campus untersucht die Auswirkungen von Network Slicing auf die Sicherheit und sucht nach Möglichkeiten, die Schwachstellen zu minimieren. In Zukunft können Network Slices genutzt werden, um 5G-Instanzen zu isolieren, zum Beispiel für die Regierung.
Ein weiterer Sicherheitsaspekt von 5G ist Lawful Interception (LI), bei dem Telekommunikationsbetreiber abgefangene Netzwerkdaten an Strafverfolgungsbehörden weitergeben. Das 5G SA-Kernnetz soll verhindern, dass sensible Informationen von Unbefugten abgefangen werden, indem es eine Schnittstelle bereitstellt, die nur für authentifizierte Strafverfolgungsbehörden zugänglich ist. Der CYD Campus arbeitete an einem Projekt zur Entwicklung einer datenschutzfreundlicheren und skalierbaren LI-Schnittstelle durch die Kombination von Technologien wie der vollständig homomorphen Verschlüsselung (FHE) und der Informationstheorie.

Homomorphe Verschlüsselung zur Stärkung der kollektiven Cyber-Resilienz

Verteidigungssysteme verlieren an Wirksamkeit, wenn sie keinen Zugang zu einer stets aktuellen und umfassenden Datenbasis haben. Gleichzeitig sind Informationen zur Cybersicherheit hochsensibel und vertraulich. Dies führt zu einem Spannungsverhältnis zwischen den Vorteilen einer verbesserten Reaktionsfähigkeit auf Bedrohungen und den Nachteilen einer Weitergabe kritischer Informationen an Dritte. Die Software von Tune Insight entschärft diesen Konflikt, denn sie ermöglicht es den Beteiligten, selbst kritische und wertvolle Cybersicherheitsinformationen gemeinsam zu nutzen, ohne einander Details übermitteln oder offenlegen zu müssen. Auf diese Weise können alle Beteiligten wertvolle Erkenntnisse gewinnen und Modelle für maschinelles Lernen auf der Grundlage umfassenderer und relevanterer kollektiver Bedrohungsdaten erstellen, was eine bessere Verteidigung ermöglicht.
Der CYD Campus entwickelt und erprobt diese neue Softwarelösung gemeinsam mit Tune Insight, dem Universitätsspital Zürich (USZ) und anderen kritischen Infrastrukturen im Gesundheitswesen. Ziel ist es, dass sich Organisationen in der Schweiz, gemeinsam besser gegen Cyberangriffe verteidigen können.

Cyber Toolkits für Cyber-Verteidigungsübung «Locked Shields»

Bei der Übung «Locked Shields» müssen sich Blue Teams gegen eine Vielzahl von Cyberangriffen verteidigen. Im Laufe der Übung wurden im Jahr 2022 über 8000 Angriffe gegen jedes Blue Team durchgeführt. Während die meisten dieser Angriffe automatisiert sind, führten die Red Teams auch manuelle, ausgeklügelte Angriffe durch, wobei sie einen nationalstaatlichen Gegner nachahmten. Locked Shields ist eine optimale Gelegenheit, um verschiedene Technologien und spezifische Produkte für die Reaktion auf einen Cyberangriff zu testen. Aus diesem Grund ist der CYD Campus eine Partnerschaft mit innovativen Schweizer Unternehmen eingegangen, um dem Schweizer Blue Team die geeignetsten und innovativsten Werkzeuge zur Verfügung zu stellen.

Die Infrastruktur, die jedes Team zu verteidigen hatte, bestand aus über 40 Webanwendungen, die auf einer Reihe von virtuellen Maschinen betrieben wurden. Wie in einem richtigen Netzwerk wiesen diese Anwendungen und Webserver Schwachstellen und Bugs auf, waren teilweise fehlerhaft konfiguriert, oder einfach nicht auf die neueste Version aktualisiert. Jedes dieser Szenarien kann es einem Angreifer ermöglichen, in das Netzwerk eines Unternehmens oder einer Organisation einzudringen. Um den Schwierigkeitsgrad zu erhöhen, hatte das Red Team vor Beginn der Übung mehrere Hintertüren, wie z. B. Web-Shells eingeschleust, die ihnen einen leichteren Zugang ermöglichten. Da das Aktualisieren und Patchen aller Dienste, die dem Übungsinternet (und damit Angriffen) ausgesetzt sind, zu zeitaufwändig wäre, wurde beschlossen, die Airlock Web Application Firewall als Teil des Cyber Toolkits für das Schweizer Blue Team einzusetzen. Diese wurde zum Schutz einer breiten Palette von Anwendungen eingesetzt, von Webmail bis zu Websites, von Software-Repositories bis zu Schnittstellen von Diensten, die von kritischen Infrastrukturen genutzt werden. Im Folgenden wird der Einsatz dieses Produkts beschrieben.

Die erste Phase der Übung bestand zum grössten Teil aus automatisierten und bekannten Angriffen (OWASP Top 10). Dank des gut gepflegten Standard-Regelsatzes der Airlock Web Application Firewall (WAF) war die Infrastruktur erfolgreich geschützt. Obwohl die Angriffe im Laufe der Übung immer raffinierter wurden, war die WAF in der Lage, auch mit exotischeren Fällen Schritt zu halten. Ein solcher Fall war ein Angriff auf das Content Delivery Network (CDN), das in der Übung bereitgestellt wurde. Der CDN-Anbieter verteilte über das CDN Schadsoftware statt legitimer Software, was zu Defacements, Cross-Site-Angriffen und Angriffen auf legitime Nutzer führte. In diesem Fall wurde die Airlock WAF eingesetzt, um die Adressen der Malware-Ressourcen in legitime und sichere Inhalte umzuschreiben und so den Angriff erfolgreich zu blockieren.
Zusammenfassend lässt sich sagen, dass das Schweizer Blue Team die Technologie erfolgreich einsetzen und schnell auf wechselnde Angriffe reagieren konnte, was ein gutes Beispiel für die gelungene Zusammenarbeit zwischen dem CYD Campus, der Schweizer Industrie und der Schweizer Armee ist.

Ein Content Delivery Network (CDN)	Ein Content Delivery Network verbessert die Verfügbarkeit und Skalierung in der Bereitstellung von Online-Inhalten wie Websites, Videos und Anwendungen. Wenn eine grosse Anzahl Benutzer Inhalte anfordern, werden diese mithilfe lokal verteilter Content Server schneller zur Verfügung gestellt. CDNs tragen auch dazu bei, die Last auf dem Ursprungsserver gering zu halten, wenn die Anzahl der Nutzer und Bereitstellung der Inhalte ansteigt (Skalierbarkeit).
Web-Shell	Eine Web-Shell ist eine Art von Hintertür oder Schadsoftware, die es Angreifern ermöglicht, einen Webserver aus der Ferne zu steuern. Web-Shells sind in der Regel in legitimen Webseiten versteckt oder werden über Schwachstellen in Webanwendungen auf den Server hochgeladen. Sobald die Web-Shell auf dem Server installiert ist, kann der Angreifer mit ihr beliebige Befehle ausführen, Dateien hoch- oder herunterladen und andere Aktionen auf dem Server durchführen.
OWASP 10	Die OWASP Top 10 ist ein Standarddokument für die Sensibilisierung von Entwicklern und die Sicherheit von Webanwendungen. Es stellt einen breiten Konsens über die wichtigsten Sicherheitsrisiken für Webanwendungen dar.

Cyber-Lagebild

Die bestehenden staatlichen «Information Sharing and Analysis Centers» (ISAC) beschaffen, analysieren und tauschen Informationen aus, um die kritischen Infrastrukturen der Schweiz zu schützen. Dies ist wichtig, um die wachsende Zahl von Cyber-Bedrohungen abzuwehren, und muss kontinuierlich weiterentwickelt werden, um mit neuen Bedrohungen Schritt halten zu können. ISAC sammelt Informationen von Partnern wie Fedpol, Govcert, Betreibern kritischer Infrastrukturen und privaten Einrichtungen, um ein Lagebild vergangener und aktueller Bedrohungen zu erstellen. Mit einem Proof of Concept (PoC) wurde die Realisierbarkeit einer zentralen Plattform getestet, die verschiedene Tools integriert und Querverweise von Ereignissen ermöglicht. Für den PoC wurden drei Open-Source-Tools untersucht: MISP, TheHive/Cortex, sowie OpenCTI. Der PoC wurde mit einer Microservice-Architektur aufgebaut und stützte sich hauptsächlich auf Docker. Die Plattform wurde laufend von Partnern getestet, um die Anforderungen an ein Endprodukt zu verstehen. Die vorgeschlagene Lösung empfiehlt die Weiterentwicklung von TheHive und Cortex durch eine benutzerdefinierte, intern entwickelte Plattform zu ersetzen, die eine zentrale Datenbank zur Datenspeicherung nutzt und sich auf einen Kubernetes-Cluster oder einen einzelnen leistungsstarken Server stützt.

Cyber-Ausbildung- Simulation Cybervorfallbewältigung

Die Bewältigung eines Cybervorfalls verlangt die Zusammenarbeit und Kommunikation zwischen dem Cyber-Response-Team, der Geschäftsleitung, den Mitarbeitern und häufig auch mit der Öffentlichkeit. Die Geschwindigkeit, mit der sich ein Cybervorfall entfalten kann, in Kombination mit der damit verbundenen Ungewissheit macht die Handhabung einer solchen Krise besonders schwierig. Zur besseren Bewältigung derartiger Ereignisse ist es neben soliden Szenario-basierten Ablaufplänen auch erforderlich, die Reaktionen zu testen und zu trainieren. Dies geschieht meist in Form von Table-Top-Übungen. Mit der zunehmenden Digitalisierung ist es jedoch sinnvoll, computergestützte Hilfsmittel einzusetzen, zumal der Grossteil der Kommunikation online oder über online-basierte Kanäle wie E-Mails, Websites und soziale Medien erfolgt. Der Cyber-Defence Campus hat zusammen mit dem Kommando Operationen und der Führungsunterstützungsbasis der Schweizer Armee eine Krisensimulationsplattform des Unternehmens Conducttr getestet, um sich effektiv auf zukünftige Cyberkrisen vorzubereiten. Unter Beteiligung von zivilen Experten, Militär- und Milizeinheiten wurden mehrere Tests erfolgreich durchgeführt, die es der Schweizer Armee ermöglichten, das Wissen und mögliche Anwendungsfälle dieser Technologie zu erweitern.

6.2 Cyber Startup Challenges

2022: Netzwerkerkennung und IoT-Gerätesicherheit

Die Cyber Startup Challenge 2022 wurde vom Cyber-Defence Campus organisiert, um die Startup-Landschaft im Bereich der Sicherheit von Internet of Things (IoT) Geräten zu erkunden. 36 Startups aus der ganzen Welt nahmen teil und präsentierten innovative Technologien im Bereich der Netzwerkerkennung und IoT-Gerätesicherheit. Die Jury nominierte die drei Finalisten: ONEKEY, Narrowin und Sepio. ONEKEY bietet eine automatisierte Sicherheitsanalyse von IoT-Geräten und operativen Technologien, die den Zeitaufwand für die Identifizierung und Behebung von Schwachstellen reduziert. Der Lightweight Network Explorer von Narrowin ermöglicht die Überwachung und Analyse von Netzwerkstrukturen in Echtzeit und reduziert so Komplexität und Aufwand. Die Plattform für das Asset-Risikomanagement von Sepio erkennt, bewertet und reduziert bekannte und unbekannte Risiken mithilfe eines neuartigen Algorithmus und einer Threat Intelligence-Datenbank.
Das deutsche Startup ONEKEY gewann die Cyber Startup Challenge 2022 und überzeugte die Jury mit seiner innovativen Technologie zur automatisierten Sicherheits- und Compliance-Analyse von IoT-Geräten und operativen Technologien (OT). Die Lösung von ONEKEY nutzt «Software Bill of Materials (SBOM)» und «Digital Twins», um Sicherheitsschwachstellen und Compliance-Verstösse zu erkennen und zu isolieren. Diese Technologie kann in Softwareentwicklungs- und Beschaffungsprozesse integriert werden und wird von führenden internationalen Unternehmen eingesetzt.

2021: Stärken Sie ihr Information Sharing und Analysis Center (ISAC)

Im Jahr 2022 wurde die Arbeit mit Schweizer Jungunternehmen Decentriq, dem Gewinner der Cyber Startup Challenge 2021, fortgesetzt. Der Fokus der Challenge lag auf dem Thema «Boost your Information Sharing and Analysis Center (ISAC)». Decentriq bietet eine Software-as-a-Service (SaaS) Plattform an, die eine sichere und private Datenzusammenarbeit ermöglicht. Decentriq bietet «Data Clean Rooms», die es Finanzinstituten ermöglichen, Ereignisdaten auszutauschen und anonyme Erkenntnisse zu gewinnen, ohne den Datenschutz zu gefährden. Decentriq verwendet eine «Confidential Computing» Technologie, um zu gewährleisten, dass niemand, einschliesslich des Plattformbetreibers, direkten Zugriff auf die Daten hat. Die Plattform bietet somit eine Lösung für den Zielkonflikt zwischen der gemeinsamen Nutzung sensibler Daten und deren Schutz. Im Anwendungsfall dieses Innovationsprojekts tauschen mehrere Banken Phishing-E-Mails aus, um diese zu analysieren und Erkenntnisse zu gewinnen, wodurch sie ihre Cybersicherheit verbessern und ihre Kunden besser schützen können. Ein erfolgreiches Proof of Concept wurde mit drei grossen Schweizer Banken im 2022 umgesetzt.

7 Sicherheitsanalysen, Penetration Testing und Sicherheitsberatung

Im Jahr 2022 untersuchten Mitarbeitende des CYD Campus die Sicherheit von einem Dutzend militärischer Systeme, die im Rahmen von Rüstungs- und IKT-Beschaffungen im VBS bearbeitet werden. Die Prüfungen erfolgten als Sicherheitsanalysen, Penetration Testing oder Sicherheitsberatungen. Auftraggeber waren in den meisten Fällen die Beschaffungsstellen von armasuisse.

Der Fokus lag auf folgenden Bereichen:

- Windows Plattformen
- Linux Plattformen
- Web Anwendungen
- Middlewares
- Computer Netzwerke
- VPN Technologien und Kryptolösungen
- Führungsinformationssysteme
- Drohnen
- Fahrzeuge
- Drahtlose Kommunikationssysteme (Sprache und Daten)
- Aviatik und Satellitenkommunikationssysteme

Die Analysen und Prüfungen haben zu Sicherheitsmassnahmen geführt, welche anschliessend in den Beschaffungsprojekten umgesetzt wurden oder von den Risikoträgern im Rahmen des Informationssicherheits- und Datenschutzkonzeptes (ISDS) als Restrisiko getragen werden.

Hinweis: *Aus Klassifikationsgründen können die Sicherheitsanalysen, Pentesting und Sicherheitsberatungen im Jahresbericht nicht detaillierter beschrieben werden.*

Security Advisories 2022

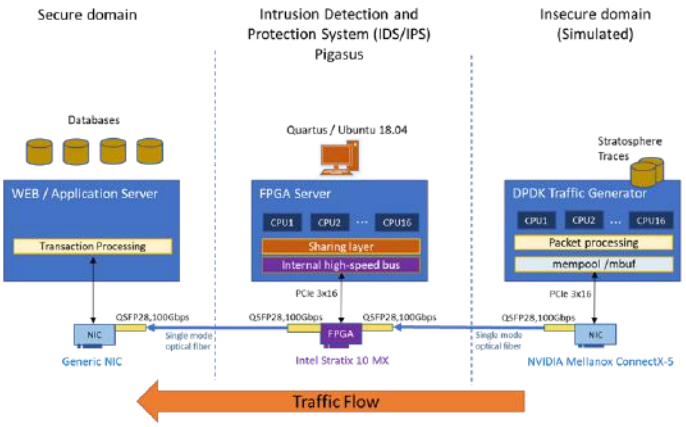
Der CYD Campus findet regelmässig Schwachstellen in Software und Geräten von Herstellern. Diese Schwachstellen werden gemäss eines sogenannten Responsible Disclosure Verfahrens offengelegt. Bei diesem Prozess werden zuerst die Hersteller informiert und erst nach einer angemessenen Frist zur Behebung der Schwachstellen, werden die Schwachstellen an die Betroffenen gemeldet, bzw. veröffentlicht.
Die Schwachstellen werden nach dem Common Vulnerability Scoring System (CVSS) bewertet. CVSS ist ein Industriestandard zur Bewertung des Schweregrades von möglichen oder tatsächlichen Sicherheitslücken in Computer-Systemen. Im CVSS werden Sicherheitslücken nach verschiedenen Kriterien, sogenannten Metrics, bewertet und miteinander verglichen, so dass eine Prioritätenliste für Gegenmassnahmen erstellt werden kann.

Hardware / Software	Datum	CVSS	CVE
Combined Charging System (CCS)	Februar 22	6.5	CVE-2022-0878
CVRF-CSAF-Converter	März 22	5.7	CVE-2022-27193
CSAF Provider	Mai 22	6.2	CVE-2022-43996
e***	September 22	10	
Plantronics Hub	September 22	7.8	
Elvexys StreamX	Dezember 22	6.5	CVE-2022-4778
Elvexys StreamX	Dezember 22	7.5	CVE-2022-4779
Elvexys ISOS	Dezember 22	4.5	CVE-2022-4780

8 Demonstratoren

Demonstrator: Architektur des 100 Gbps Intrusion Prevention Systems

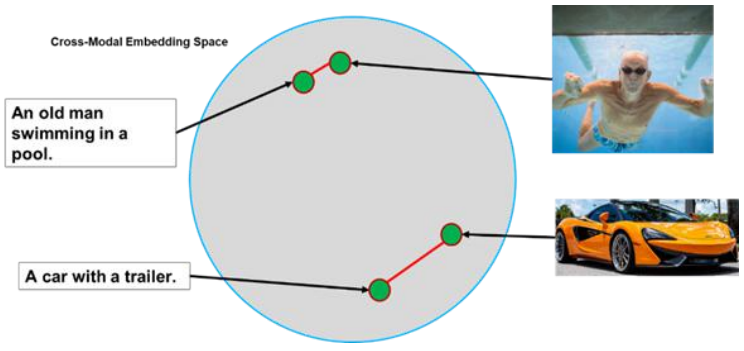
«Intrusion Detection and Prevention Systems» (IDS/IPS) wie SNORT benötigen viel Rechenleistung, wenn sie Datenverkehr mit hohem Durchsatz analysieren. Für die Analyse eines Verkehrsstroms von 100 Gbps sind normalerweise mehrere Server erforderlich. Dieser Demonstrator zeigt, wie ein 100 Gbps «Intrusion Prevention System» mit nur einem einzigen Server implementiert werden kann. Die Idee ist, dass CPU-intensive Aufgaben auf ein FPGA verlagert werden und die Beschleunigungsleistung moderner FPGAs genutzt wird. Der Demonstrator enthält einen Intel Stratix 10 MX FPGA, der mit einer Intel Xeon CPU mit 16 Kernen kombiniert wird, um bis zu 100 Gbps zu verarbeiten.



Architektur eines 100 Gbps «Intrusion Prevention System» mit nur einem einzigen Server.

Demonstrator: Automatische Auswertung von Bilddaten in Desinformationskampagnen

In diesem Demonstrator werden die technischen Möglichkeiten einer kürzlich publizierten Deep Learning Methode, dem sogenannten «Contrastive Language-Image Pre-training» (CLIP), aufgezeigt. Dabei wird auf einen anonymisierten, von Twitter für Forschungszwecke veröffentlichten Datensatz zurückgegriffen. Die Besonderheit von CLIP liegt in dessen Fähigkeiten, Ähnlichkeiten zwischen Text- und Bildinhalten messen zu können (siehe Abbildung 1). Mit dieser Fähigkeit eröffnen sich eine Vielzahl von potenziell sehr interessanten Anwendungen: semantisches Durchsuchen von Bildern (analog Google Image Search aber auf lokalem Server), Klassifikation von Bildern ohne Trainingsvorgang und die Exploration von grossen Mengen an Bildern auf inhaltliche Trends. Der Zweck dieses Demonstrators ist es, diese Anwendungsmöglichkeiten von CLIP zu zeigen und in einem nachrichtendienstlichen Kontext zu illustrieren.



Fähigkeit von «Contrastive Language-Image Pre-training» (CLIP) sowohl Bilddaten wie auch Textdaten in einen Vektorraum abzubilden. Innerhalb dieses Vektorraums können dann Ähnlichkeiten von Bild- und Textinhalten gemessen werden, was eine Vielzahl interessanter Anwendungen ermöglicht.

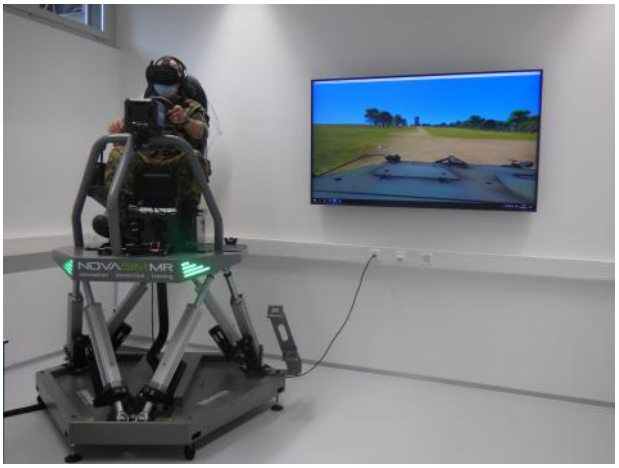
Demonstrator: Gemischte Realität für die Ausbildungssimulation

Die gemischte Realität (engl. Mixed Reality - MR) beschreibt die Vermischung der realen, physischen Welt mit einer virtuellen Realität, d. h. mit einer computergenerierten, interaktiven Umgebung. Um diese gemischte Realität auch für Ausbildungen zu nutzen, wurde ein Demonstrator entwickelt.
Das Ziel des Demonstrators ist es, Innovation in die Ausbildungssimulation zu bringen, die konservativen Behauptungen der Industrie zu prüfen, das Potenzial der gemischten Realität in der Simulationsausbildung aufzuzeigen sowie die Grenzen der Technologie einzuschätzen und zu beurteilen. Simuliert wird das Fahren mit einem Panzer.

Einsatz des Demonstrators für Tests mit Personen

Die Potenziale der MR sind unter anderem:

- Erhöhte physische und operationelle Lageerkennung
- Kostenreduktion in Ausbildung und Training
- Bessere Trainings- und Einsatzvorbereitungen
- Flexibilität und (Teil-)Mobilität in Trainings, Ausbildung und Einsatzvorbereitungen
- Bessere Unterstützung (Wartung, Logistik, Sanitätstruppen, usw.)
- Effektiverer Sensor-Nachrichten-Führungs-Wirkungsverbund
- Schonung Material und der Umwelt
- Durchführung von Szenarien, die in der realen Welt nicht oder schwer realisierbar sind (Notfallszenarien in Fahrzeugen, Durchführung von grossen Übungen, Einsätze in urbanen Gebieten, usw.)



Demonstrator gemischte Realität für die Ausbildungssimulation.

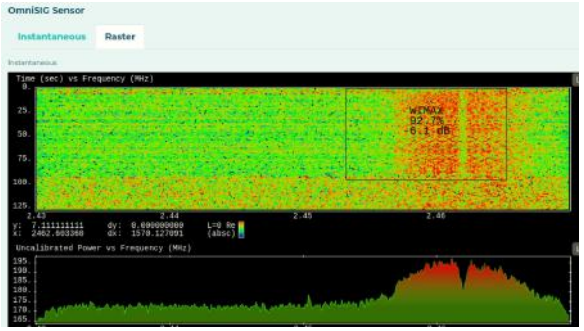
Die Verwendung der Technologie birgt gewisse Probleme, unter anderem:

- VR- oder Simulatorkrankheit
- Daten- und Informationsüberlastung
- Starke Abhängigkeit der MR im Einsatz
- Starke Abhängigkeit von IKT-Diensten
- Sicherheit (Integrität der Systeme, Verfügbarkeit der Dienste, Vertraulichkeit der Daten)
- Mögliche starke Auswirkungen in der Doktrin, insbesondere in der Ausbildung
- Aneinanderreihung von Ausbildung, Training und Einsatz
- Mangelnde Interoperabilität und Frameworks
- Tiefe Marktreife
- Tiefer MR-Reifegrad für militärische Anwendungen

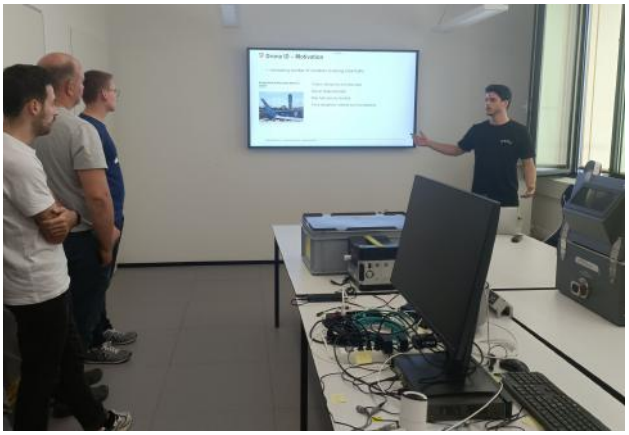
Die ersten Ergebnisse mit dem Demonstrator zeigen, dass ein grosses Potenzial zwar vorliegt, aber die Bündelung der verschiedenen Komponenten und die Überwindung der Risiken herausfordernd ist. Der Demonstrator wurde in einem ersten Schritt als virtueller Demonstrator entwickelt (virtuelle Realität-VR). Der Übergang von der VR zur MR im Jahr 2022 hat sich als besondere Herausforderung erwiesen. Die unterschiedliche Dynamik zwischen reellen und virtuellen Bildern muss noch bewältigt werden.

Demonstrator Signal Klassifikation

Cyber-Kriegsführung und elektromagnetische Kriegsführung wurden meist als getrennte Bereiche betrachtet. Heute sehen wir eine Konvergenz beider Bereiche hin zu einem integrierten Verständnis und Einsatz von Technologien. Dies zeigt sich auch im Zusammenhang mit modernen Operationen der hybriden Kriegsführung. Vor diesem Hintergrund wird es immer wichtiger, mit begrenzter Rechenleistung und mit zunehmender Flexibilität, Signale im elektromagnetischem-Spektrum klassifizieren zu können. Heute gibt es mehrere Forschungsansätze, die Deep Learning Techniken zur Klassifizierung von Spektrumsdaten verwenden. Die im Jahr 2021 begonnene Arbeit wurde erweitert und ermöglicht nun die Demonstration einer breiteren Funktionalität bei der Arbeit mit verschiedenen Wellenformen.



Demonstrator nutzt Maschine-Learning-Modelle um das elektromagnetische Spektrum in Echtzeit zu klassifizieren.



Vorstellung Demonstrator an Studierende der Hochschule Luzern

Demonstrator «Drone Hijacking» über GPS

Der Demonstrator «Drone Hijacking» zeigt eine Methode, bei der ein Funksender in der Nähe der Drohne verwendet wird, um ein authentisches GPS-Signal vorzutäuschen. Drohnen, die zur Bestimmung ihres Standorts auf GPS-Signale angewiesen sind, können davon betroffen sein. Es konnte bereits gezeigt werden, wie eine Drohne den gefälschten Standort an den Piloten bzw. an die Pilotin zurückmeldet. Der Demonstrator konzentriert sich nun darauf, wie eine Drohne mit Hilfe dieses Ansatzes gekapert werden kann. Die Idee besteht darin, ständig Standorte in der Nähe zu fälschen und eine echte Bewegung zu simulieren, so dass sich die Drohne fortbewegt und der vortäuschende Sender die volle Kontrolle über die Bewegung der GPS-Drohne hat. Dieses Verfahren könnte folglich von einem legitimen Akteur genutzt werden, um Drohnen von böswilligen Angreifern zu kapern und sich so vor Drohnenangriffen zu schützen.

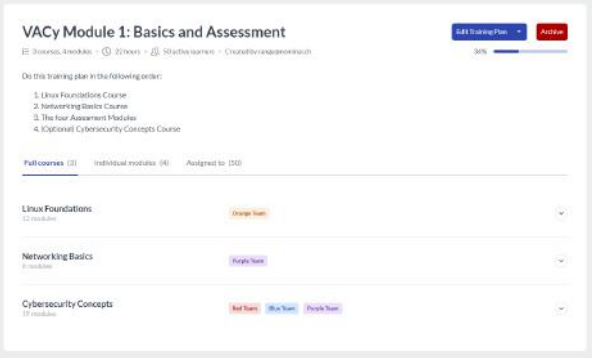
Demonstrator Augmenting Reality for Security

Die erweiterte Realität (engl. Augmented Reality - AR) ermöglicht es einer Person, mit ihrer realen Umgebung zu interagieren, die durch virtuelle Informationen und Objekte erweitert wird. Für diesen Demonstrator wird die Anwendbarkeit von AR als Hilfsmittel für Benutzer/innen zur Abwehr von Cybersicherheitsattacken wie Phishing betrachtet. Eine AR-Brille kann einen Cybersicherheitsexperten simulieren, der dem Nutzenden «über die Schulter schaut» und bei der Abwehr von Attacken unterstützend wirkt. Dieser Ansatz ermöglicht eine wesentlich bessere Verteidigung gegen Phishing und Spear-Phishing im Vergleich zu herkömmlichen Methoden.

Evaluation der Augmented Reality für die bessere Verteidigung gegen Phishing anhand des Demonstrators.

Demonstrator Gamified Cyber Training

Es ist bekannt, dass es einen systematischen Mangel an qualifizierten Arbeitskräften im Bereich der Cybersicherheit gibt; eine mögliche Lösung für dieses Problem besteht darin, mehr Menschen für die Ausbildung in diesem Bereich zu gewinnen. Um junge Menschen wirksam zu erreichen, sollte etwas Attraktives angeboten werden. In diesem Rahmen kann die Gamification in der Cyber-Ausbildung einen wichtigen Beitrag leisten. Gamification bedeutet, dass spieltypische Elemente in einem spielfremden Kontext angewendet werden. Um verschiedene Szenarien und Hypothesen zu testen, haben Mitarbeitende des CYD Campus die Produkte mehrerer Startups angesehen und zwei davon mit einer Gruppe junger Menschen getestet. Mit den Erfahrungen, die in diesem ersten Versuch gesammelt wurden, konnte zu einem umfangreicheren Test übergegangen werden. Die 50 jungen Menschen, die Teil des ersten Pilotprojekts der Vordienstlichen Ausbildung Cyber sind (Abschluss Dezember 2022), konnten die innovative Software eines der ausgesuchten Startups nutzen.



Softwareumgebung des Demonstrators für die vordienstliche Cyber-Ausbildung der Armee

Demonstrator Visualisierung von Angriffen auf kritische Infrastrukturen

Bei der Durchführung von Capture-the-Flag- oder Live-Fire-Übungen ist es für Cybersicherheitsexpertinnen bzw. Cybersicherheitsexperten und Entscheidungsträger/innen oft schwierig, die Auswirkungen von Cyber-Aktionen auf die physische Infrastruktur zu verstehen. Denn im Gegensatz zu Angriffen auf cyber-physische Systeme wie Stromerzeugungsanlagen oder militärische (Waffen-)Systeme ist es vergleichsweise einfach zu erkennen, wenn eine Website nicht lädt, bösartige E-Mails eintreffen oder Ransomware auf einen Computer gelangt. Zur Ermittlung der besten Cyber-Trainingswerkzeuge für die Schweizer Armee wurde ein Demonstrator gebaut, der diese Auswirkungen veranschaulicht. Er besteht aus einem 2.4 x 1.2 Meter grossen Geländemodell, das modular aufgebaut und leicht zu bewegen ist und einen gemischten zivil-militärischen Flughafen sowie kritische Infrastrukturen, Energieproduktion und militärische Systeme zeigt. Diese Anlage wurde in 2022 ausgeweitet. Es wurde eine physikalische Darstellung eines Pumpspeicher-Kraftwerks hinzugefügt, das echte speicherprogrammierbare Steuerung (SPS) sowie Sensoren und Aktuatoren verwendet. Dies kann zur Demonstration, aber auch zur Forschung und Ausbildung in der Betriebstechnik (OT) genutzt werden.

Visualisierung von Cyberangriffen auf einem Militärflugplatz.

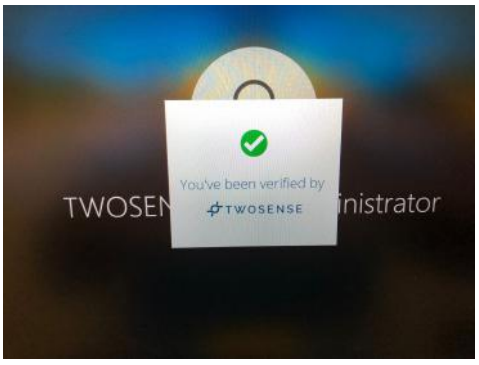
Demonstrator Offline-Übersetzung

Der Austausch von Informationen in verschiedenen Sprachen ist zu einer Notwendigkeit geworden. Maschinelle Übersetzungswerkzeuge haben sich ebenfalls zu einem festen Bestandteil unseres Berufsalltags entwickelt. Allerdings bergen diese Online-Übersetzungs-Tools auch erhebliche Risiken für die Privatsphäre, insbesondere bei sensiblen Informationen. Daher ist es dringend erforderlich, dass die automatische Übersetzung genutzt werden kann, ohne dass die Informationen der Aussenwelt prei gegeben werden. Der Offline Übersetzungs- Demonstrator bietet zu diesem Zweck eine bidirektionale automatische Offline-Übersetzung von Text zwischen Englisch und sechs anderen Sprachen, nämlich Arabisch, Deutsch, Französisch, Italienisch, Russisch und Chinesisch. Um Fehler zu vermeiden, die durch falsche Sprachverwendung verursacht werden, ist auch ein Spracherkennungswerkzeug integriert. Es kann über GUI und REST API genutzt werden.

Beispielsübersetzung vom Chinesischen ins Englische mit einem Offline System.

Demonstrator Continuous Authentication

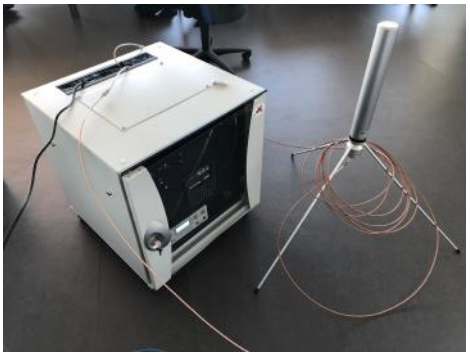
Passwortabfragen oder einmalige biometrische Prüfungen wie Fingerabdruck- oder Iris-Sensoren gewähren Nutzer/innen den Zugang nach erfolgreicher Authentifizierung und prüfen nicht regelmässig auf böswilliges Verhalten oder einen Wechsel des Nutzers. Diese Methoden ermöglichen z. B. sogenannte Mittagsangriffe, bei denen ein Angreifender einen Arbeitsplatz benutzt, an dem ein legitimer Benutzer oder eine legitime Benutzerin noch angemeldet ist. Ebenso können Passwortdaten durch Lecks, Schulter-Surfen oder Phishing-Angriffe gestohlen werden und einem Angreifer / einer Angreiferin freie Hand auf dem Zielsystem geben. Dies steht im Gegensatz zu der Kontinuierlichen Authentifizierung (CA). Es handelt sich um eine Methode, bei der ein/e Nutzende/r über einen längeren Zeitraum beobachtet und die Authentifizierung kontinuierlich gewährt oder gegebenenfalls widerrufen wird. CA authentifiziert das Verhalten des Benutzenden also auch dann, wenn er / sie angemeldet ist, in der Regel mit biometrischen Merkmalen wie Blickverfolgung oder Umgebungsüberwachung wie drahtloser Näherungssensorik. Der Demonstrator automatisiert die Identitätssicherheit durch biometrische Authentifizierung der Benutzer/innen, so dass diese sich nicht mehr manuell authentifizieren müssen. Der Demonstrator ermöglicht es bis zu zehn Nutzenden, sich mit der automatischen Authentifizierungssoftware an zwei verwalteten Computern anzumelden, um die kontinuierliche Authentifizierungsfähigkeit zu demonstrieren.



Verhaltensbasierte Verifizierung des Nutzenden durch den Demonstrator.

Demonstrator Aircraft Communication Spoofing

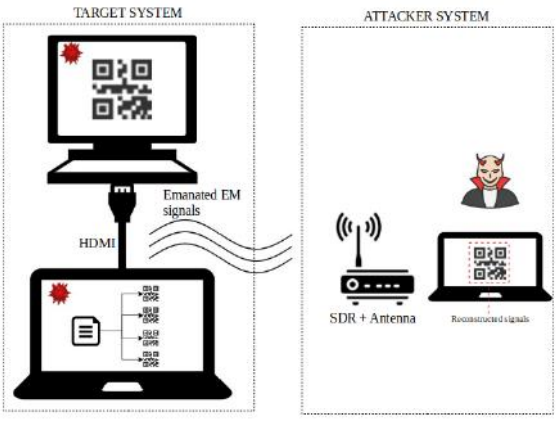
In den 2010er Jahren haben Wissenschaftler/innen und Hacker/innen zahlreiche Schwachstellen in den von Flugzeugen und Fluglotsen bzw. Fluglotsinnen genutzten drahtlosen Technologien nachgewiesen. Bislang wurde solches Spoofing mit geringen Mitteln wie Software Defined Radios ausschliesslich am Computer mit simulierter Hard- und Software demonstriert.
Dieser Demonstrator verwendet eine realitätsnahe Abbildung realisti-scher Avionik-Systeme (Hard- und Software), wie sie tatsächlich in Flugzeugen verbaut sind. Der vollständige Zugriff auf diese Systeme zum Zweck der Penetrationstests ermöglicht es den CYD Campus Forschenden, drahtlose Radiofrequenz (RF)-Attacken auf die GPS, Automatic Dependent Surveillance - Broadcast (ADS-B) und Traffic Alert and Collision Avoidance System (TCAS)-Systeme zu zeigen.



Demonstration von Spoofing im Cyber Avionics Lab.

Demonstrator TEMPEST Datenabfluss

Jedes elektronische Gerät erzeugt elektromagnetische Emissionen. Die erzeugten elektromagnetischen Signale hängen damit zusammen, wie die emittierenden elektronischen Komponenten intern arbeiten. Ein böswilliger Angreifer bzw. eine böswillige Angreiferin kann die ausgestrahlten Signale abhören und sie untersuchen, um Informationen über das sendende Gerät zu erhalten. Die Praxis des Abhörens und des Schutzes gegen das Abhören und ihrer Untersuchung ist in einem Rahmenwerk zusammengefasst, das als TEMPEST bekannt ist. Im Falle von Videomonitoren können die ausgestrahlten Signale dazu verwendet werden, den Inhalt zu rekonstruieren. Es wurde bereits gezeigt, wie ein Angreifer / eine Angreiferin die Signale des Verbindungskabels zwischen einem PC und einem Videomonitor nutzen kann, um interne Informationen aus dem Monitor zu extrahieren. In dieser Demonstration zeigt der CYD Campus, wie ein QR-Code verwendet werden kann, um interne Daten mit Hilfe dieser vom Videomonitor ausgehenden Signale zu exfiltrieren. Da sich zahlreiche Unternehmen auf Computernetzwerke als Kommunikationssystem verlassen, um verschiedene Arten von Informationen zwischen Servern und Workstations zu übertragen, ist zu erwarten, dass solche Netzwerke ein interessantes Ziel für böswillige Angreifer/innen sind, da einige dieser Informationen Geschäftsgeheimnisse enthalten und höchst vertraulich sein können.



Ausnutzung der Abstrahlung von HDMI Videokabeln um sensible Daten aus einem infizierten Computer zu exfiltrieren.

Demonstrator Anti-GPS Jamming

GPS-Jamming, bei dem GPS-Signale nicht mehr empfangen werden können, ist ein zunehmendes Problem und eine Bedrohung sowohl für zivile als auch für militärische Nutzende. Während sich militärische Nutzende auf spezifische Signale verlassen können, die störresistent sind, selbst im Verteidigungssektor verlässt man sich mehr und mehr auf nicht gehärtete Consumer-Hardware. Zusammen mit dem Schweizer Drohnen und Robotik Zentrum (SDRZ) und dem Fachbereich Sensorik von armasuisse W+T hat der CYD Campus ein neuartiges Gerät getestet, das dank eines fortschrittlichen Null-Steering-Algorithmus und einer speziellen Signalfilterungstechnologie gegen GPS-Jamming resistent ist. Das Neue daran ist, dass dieses Gerät einfach nachgerüstet werden kann und wenig Strom verbraucht. Die Wirksamkeit des Geräts wurde bei einem genehmigten GPS-Jamming-Test an einer Drohne im freien Luftraum getestet und demonstriert.

GPS-Jamming-Test an einer Drohne

Demonstrator Car Hacking

Das CYD Campus-Elektroauto Renault Zoe wird als Labor für die Cybersicherheitsforschung genutzt, da es mit verschiedenen Sensoren, Kommunikationsgeräten und Softwaresystemen ausgestattet ist, auf die zugegriffen und die manipuliert werden können. Die Forscher untersuchen die Kommunikationsnetze (z. B. den CAN-Bus), Sensoren und Software des Fahrzeugs auf Schwachstellen und mögliche Cyberangriffe.

Das Auto bietet den Forschenden auch die Möglichkeit, die Sicherheit von Ladesystemen und deren Auswirkungen auf das Stromnetz zu analysieren, was im Hinblick auf die Umstellung auf Elektromobilität in der Schweiz und im VBS sehr wichtig ist. Bis jetzt haben die Mitarbeitenden das Auto genutzt, um die Schwachstelle des Brokenwire-Ladesystems zu demonstrieren und Angriffe auf die Kamerasysteme und die Modelle zur Verkehrszeichenerkennung zu testen.

Demonstration der Ausnutzung von Sicherheitslücken von Elektrofahrzeugen um die Kommunikation abzuhören.

9 Technologie Monitoring

Der CYD Campus ist eine Antizipationsplattform für nationale und internationale Entwicklungen und Trends im Cyber-Bereich. Cyber-Bedrohungen und Cyber-Technologien verändern sich rasant und es ist eine Herausforderung, diese Trends zu überblicken. Mit diesem Aufgabenfeld versucht das VBS, technische Entwicklungen zu identifizieren und deren Chancen und Risiken frühzeitig zu verstehen. Zur Erkennung der jüngsten Marktbewegungen betreibt der CYD Campus ein quantitatives und qualitatives Technologie- und Marktmonitoring, das in Form eines Technologie Monitoring (TM) Portfolios zusammengefasst wird. Einerseits werden aufkommende Cyber-Technologien und -Clusters mit Hilfe einer Technologie- und Marktmonitoring (TMM) Plattform durch eine quantitative Analyse öffentlich verfügbarer Daten entdeckt. Andererseits werden vielversprechende Startups durch ein qualitatives Scouting, einem internationalen Technologiebeobachtungsprogramm, aufgespürt. Die Aufgaben des TM-Portfolios bestehen darin, i) die Trends im Bereich der Cybersicherheitstechnologien innerhalb eines Zeithorizonts von maximal fünf Jahren zu identifizieren, ii) zu beobachten und zu analysieren sowie iii) Prognosen zu erstellen.

Quantitativer und wissenschaftlicher Ansatz

Beim CYD Campus werden die jüngsten Fortschritte in den Bereichen Big Data und künstliche Intelligenz genutzt, um auf der Grundlage öffentlicher Daten und wissenschaftlicher Methoden einen zunehmend quantitativen Ansatz zu verfolgen. Gemeinsam mit verschiedenen Partnern aus der Industrie und der Akademie wird eine TMM Plattform laufend weiterentwickelt und optimiert. Die Plattform durchsucht kontinuierlich zahlreiche freie und nicht-öffentliche Datenquellen, die den Technologieanalysten des CYD Campus aggregierte Erkenntnisse liefern, welche sie mit ihren Erfahrungen aus Forschungs- und Scoutingaktivitäten kombinieren. Mittels prädiktiver Methoden können Trends vorhergesagt werden, was den Beteiligten einen Wissensvorsprung verschafft. Umsetzbare Erkenntnisse werden unterschiedlichen Entscheidungsträgern in den folgenden Tätigkeitsfeldern zur Verfügung gestellt:

- Verteidigung
- Cybersicherheit
- Sicherheitspolitik
- Marktforschung
- Strategisches Management

Die Aktivitäten im Rahmen des TM-Portfolios tragen auf unterschiedlichen Ebenen zu Cyber-Strategien der öffentlichen Verwaltung bei:

i. Bund: Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)
ii. VBS: Strategie Cyber VBS
iii. Schweizer Armee: Gesamtkonzeption Cyber
iv. CYD Campus: Business Architektur

Eine zentrale Aktivität des TM-Portfolios im Jahr 2022 war die Studie «Trends in Datenschutz- und Verschlüsselungstechnologien 2025». Dies ist auch der wichtigste Beitrag zur Massnahme 1 (Technologie Monitoring) der NCS. Die Studie bietet einen Überblick über die sich rasch wandelnde Landschaft der Verschlüsselungs- und Datenschutztechnologien und hat zum Ziel, die voraussichtlichen Entwicklungen bis 2025 zu analysieren sowie die Auswirkungen auf die Bereiche Militär, Zivilgesellschaft und Wirtschaft abzuleiten. Der CYD Campus, der eine interdisziplinäre und internationale Forschungsgemeinschaft zusammenbringt, war ebenfalls massgeblich an der Gründung des Schweizer Technologieobservatoriums 2022 beteiligt.

Webseite
Technologieobservatorium

10 Internationales Scouting und Zusammenarbeit

Im Jahr 2022 konzentrierte sich das Startup-Scouting des CYD Campus auf die Schweiz, die USA, Israel, Deutschland und Frankreich mit einigen wenigen Unternehmen in anderen Ländern. Der Fokus des Scouting liegt auf der Suche nach neuen Technologien in den Bereichen Cybersicherheit und künstliche Intelligenz mit dem Ziel, die wichtigsten Trends und Akteure frühzeitig zu entdecken. Es wurden Gespräche mit über 80 Startups und Unternehmen geführt. Die Ergebnisse dieser Gespräche wurden in strukturierter Form an potenzielle Interessenten in der Verwaltung weitergegeben. Um Zugang zu den interessantesten Startups zu erhalten und auch sogenannte Early-Stage-Unternehmen aufzuspüren, stützt sich der CYD Campus auf ein grosses Netzwerk, das von Venture Capitalists bis zu Accelerators und von Botschaften bis zu Wirtschaftsförderungsorganisationen reicht. Besonders wichtige Partner sind der Swisscom Outpost im Silicon Valley und das Swissnex Network (Boston, Bangalore, Tel Aviv). Ein weiteres wichtiges Instrument für das Scouting ist die Teilnahme an weltweit führenden Konferenzen wie der RSA Conference in San Francisco, Black Hat, Defcon, Usenix Security, Cybertech und Cyberweek in Tel Aviv sowie der European Cyber Week in Rennes. Diese Veranstaltungen bieten die Möglichkeit, in kurzer Zeit eine grosse Zahl von Unternehmen und Partnern zu treffen.

Die im Rahmen der Scouting-Aktivitäten identifizierten Startups führten zu mehreren Proof of Concepts, die im Kapitel «Demonstratoren» detaillierter beschrieben werden. Ausserdem wurden die gewonnenen Informationen genutzt, um den Beschaffungsprozess zu unterstützen und den Cyber Markt besser zu verstehen.

2022: 100 STARTUPS
davon 80 technische Präsentationen
davon 30 an zuständige Stellen innerhalb BV verwiesen
8 Proof of Concepts umgesetzt
15 aktive Scouting-Partner
1 Cyber Startup Challenge

Venture Capitalist	Ein Investor, der in wachstumsstarke Unternehmen investiert. Venture Capitalists unterstützen Unternehmen bei der Wachstumsstrategie. Ähnlich wie der CYD Campus suchen sie nach innovativen Startups.
Accelerator-Programm	Es handelt sich um ein Programm, das Startups durch Zugang zu Ressourcen, Mentoring und Networking unterstützt. Teilnehmende eines Accelerator-Programms arbeiten oft an ihren Geschäftsideen und erhalten Feedback. An diesen Programmen teilnehmende Startups können für den CYD Campus vielversprechend sein.

Internationale Zusammenarbeit

Die Zusammenarbeit mit internationalen Partnern ist im Cyberraum von entscheidender Bedeutung. Da Bedrohungen und böswillige Akteure nicht an Landesgrenzen gebunden sind, ist die Schweiz auf eine enge Zusammenarbeit angewiesen. In diesem Zusammenhang führt der CYD Campus einerseits Forschungsprojekte mit Wissenschaftlerinnen und Wissenschaftlern von weltweit führenden Universitäten wie etwa der Universität Oxford, der Universität Southern California, oder der Ruhr Universität Bochum durch. Andererseits arbeitet der CYD Campus auch mit anderen Regierungen und internationalen Organisationen zusammen. So vertritt er die Schweiz im Rahmen der CapTechs Cyber und Information der European Defence Agency. Je nach Bedarf werden die Diskussionen zu bestimmten Projekten vertieft und es wird mit den CYD Campus Forschenden geprüft, ob ein Beitrag der armasuisse sinnvoll ist. Diese Gremien dienen auch als Plattform für den informellen Austausch unter Fachleuten. So leitet der CYD Campus die schweizerischen Bemühungen für eine mögliche Teilnahme an einem zukünftigen PESCO-Projekt im Bereich der Cyber-Ranges Federation (CRF). Das Ziel von CRF ist es, die Leistungsfähigkeit der europäischen Cyber Ranges (CR) zu verbessern, indem bestehende nationale Cyber Ranges zu einem grösseren Cluster zusammengeschlossen werden.

Die NATO ist ebenfalls ein wichtiger Kooperationspartner. Der CYD Campus trägt wesentlich zu den Aktivitäten des CCDCOE in Tallinn bei, sowohl durch die Mitwirkung des Forschers William Blonay vor Ort als auch durch Forschungsbeiträge zum Arbeitsprogramm des Zentrums. Ausserdem wirkt der Campus gezielt in interessanten Arbeitsgruppen der NATO STO mit. Diese Projekte werden durch das armasuisse-Büro in Brüssel unterstützt.

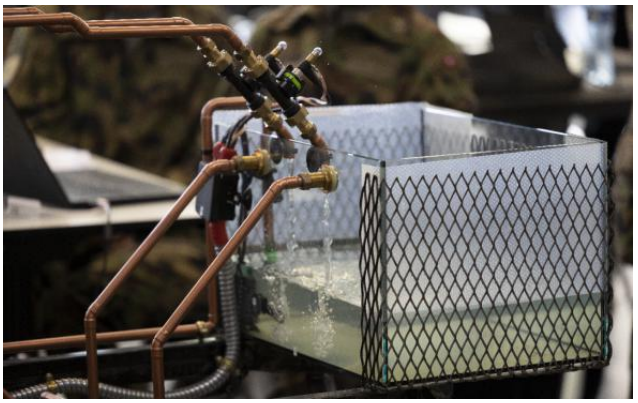
Von grosser Bedeutung ist auch der bilaterale Austausch mit den Partnerorganisationen des VBS in ausgewählten Partnerländern. Je nach Partnerland geht es darum, Forscherinnen und Forscher mit übereinstimmenden Interessen zu finden, um Fachwissen, Methoden und Daten auszutauschen oder in einigen Fällen auch gemeinsame Forschungsarbeiten zu realisieren. Bei diesen Projekten erfolgt die Zusammenarbeit mit dem armasuisse-Büro in Washington, den Schweizer Botschaften und den Verteidigungsattachés weltweit.

CapTechs European Defence Agency	Es handelt sich um Arbeitsgruppen, in denen die Mitglieder gemeinsam an der Forschung und Entwicklung militärischer Fähigkeiten arbeiten.
Permanent Structured Cooperation (PESCO) Projekt	Bezeichnet ein Kooperationsprojekt der EDA im Rahmen der europäischen Verteidigungszusammenarbeit. Ziel ist es, die militärischen Fähigkeiten zu verbessern und eine engere Zusammenarbeit zwischen den Mitgliedsstaaten zu fördern. An ausgewählten PESCO-Projekten sind auch Norwegen, Kanada, das Vereinigte Königreich und die USA beteiligt.
NATO Science and Technology Organization (STO)	Die Organisation konzentriert sich auf die Förderung der wissenschaftlichen und technischen Zusammenarbeit im Bereich der Verteidigung. Die STO unterstützt die Entwicklung von Technologien und Konzepten, die für die militärischen Aufgaben der NATO von Bedeutung sind.

11 Laborinfrastrukturen

ICS Labor Pumpspeicherkraftwerk

Im Jahr 2022 wurde beim CYD Campus in Thun ein neues ICS-Labor in Betrieb genommen. ICS steht für industrielle Kontrollsysteme, welche aus Hardware und Software bestehen, die zur Steuerung, Überwachung und zum Betrieb von Anlagen, Maschinen und Prozessen in industriellen Umgebungen eingesetzt werden. Sie sind häufig in kritischen Infrastrukturen zu finden. Da industrielle Kontrollsysteme teuer sind und einen langen Produktionszyklus haben, braucht es geeignete Labors, um Schwachstellentests durchführen zu können. Das ICS-Labor ist eine Darstellung eines Pumpspeicherkraftwerks. Das industrielle Steuerungssystem kontrolliert Funktionen wie die Messung des Wasserstands oder den Betrieb von Ventilen und Pumpen. Im Rahmen des ICS-Hackathons im September 2022 wurde das Labor genutzt, um gezielte Schwachstellenanalysen durchzuführen, verschiedene Angriffsvektoren zu untersuchen sowie wirksame Gegenmassnahmen zu entwickeln.



Modell eines Pumpspeicherkraftwerks: CYD Campus ICS-Labor in Thun.

Erweitertes «Cyber Avionics Lab»

Das vom CYD Campus während zwei Jahren aufgebaute «Cyber Avionics Lab» wurde am 8. August 2022 auf dem «15th Cyber Security Experimentation and Test (CSET) Workshop» der internationalen Cyber-Community vorgestellt. Das Testen von Cyberangriffen auf Luftfahrtkommunikationssysteme erfordert höchste Sorgfalt, um den Luftverkehr nicht zu stören. In der Schweiz ist der Luftraum Tag und Nacht besetzt, weshalb praktische Tests in der realen Welt kaum durchführbar sind. In Labortests können Cyberangriffe untersucht werden, ohne den Luftverkehr zu behindern.
Im «Cyber Avionics Lab» sind die gleichen zertifizierten Systeme integriert und vernetzt wie in aktuell eingesetzten Flugzeugen. Daher können Aussagen darüber getroffen werden, wie ein echtes Flugzeug auf entsprechende Cyberangriffe reagieren würde. Gegenstand der Tests sind Kommunikationssysteme des zivilen Luftraumes.

Cyber Avionics Lab zur Untersuchung von Cyber-Angriffen im Luftraum..

5G Labor

Das CYD Campus 5G Lab betreibt ein 5G Standalone (5G SA) Kernnetz, das die Open-Source-Software Open5GS einsetzt und derzeit für zwei laufende Forschungsprojekte genutzt wird. Der grösste Teil dieses Labors ist virtualisiert und läuft in unserem Rechenzentrum: Das Kernnetz ist virtualisiert, während das Radio Access Network (RAN) emuliert und teilweise virtualisiert ist. Für die Virtualisierung werden sowohl LXC-Container als auch virtuelle QEMU-Maschinen verwendet. Da dieses Labor wächst, werden zwei echte Antennen (gNB) zum Labor hinzukommen und das Kernnetz wird in Kubernetes verlagert, um eine Service Base Architecture (SBA) zu schaffen, die einem echten 5G-Netzwerk ähnelt.

SATCOM (Starlink)

SATCOM Cyber Security Lab

Als Ergänzung zu den bestehenden nicht permanenten Versuchsplattformen mit kleinen Satellitenantennen wird derzeit ein SATCOM-Labor eingerichtet. Im Zentrum dieses Labors steht eine Satellitenschüssel mit einem Durchmesser von 2,5 Metern, die auf einer motorisierten Plattform angebracht ist. Sie ermöglicht es den Mitarbeitern des CYD Campus, die Schüssel über eine Konfigurationsplattform auf die Satelliten auszurichten und, im Falle von nicht geostationären Satelliten, deren Umlaufbahn zu verfolgen. Der Satellitenempfänger der Schüssel ist für den Empfang verschiedener Frequenzen ausgelegt, so dass die Forschenden mehrere Frequenzbänder gleichzeitig nutzen können. Im Jahr 2022 wurde die Basis für ein konsolidiertes Labor geschaffen, indem ein speziell angefertigter Container auf dem Dach des Georg-Herzog-Hauses in Thun installiert wurde. Zusätzlich wurde eine Starlink-Schüssel installiert, um diese neuartige und hochrelevante Konstellation in der Praxis zu untersuchen.

SCION (Thun-Lausanne-Zürich)

Die drei CYD Campus-Standorte in Thun, Lausanne und Zürich wurden im November 2022 mit SCION-Netzanschlüssen ausgestattet und stehen der Armee und den Sicherheitsbehörden während drei Jahren als nationale Testinfrastruktur zur Verfügung. Die SCION-Technologie ermöglicht ein sicheres und kontrollierbares Routing. Zudem bieten programmierbare Switches an den Standorten die Möglichkeit, neue Verschleierungsmethoden für den Datenverkehr im Netzwerk zu implementieren und auf ihre Effizienz zu untersuchen. Im genannten Zeitraum wird ebenfalls die Resistenz der SCION-Technologie gegenüber verschiedenen Formen von Cyberangriffen wie DDoS-Angriffe oder Route-Hijacking untersucht. Zudem soll die Implementierung der Technologie für die Bedürfnisse der Schweizer Cyberverteidigung anhand konkreter Anwendungsfälle erweitert und getestet werden. Die Sicherheitstests werden von Mitarbeiterinnen und Mitarbeitern des CYD Campus sowie assoziierten Partnerorganisationen aus der Industrie, den Hochschulen und der Armee durchgeführt.

SCION Netzwerk Topologie ermöglicht effizientes Routing nach unterschiedlichen Kriterien (Quelle: anapaya.net).

Internet of Things (IoT) Labor

Das IoT-Cluster besteht aus etwa 50 Einplatinen-Computern, bei denen es sich überwiegend um Raspberry Pis verschiedener Modelle handelt. Dieses Cluster dient verschiedenen Szenarien. Zunächst werden einige Experimente durchgeführt, deren Ziel es ist, Malware zu identifizieren, welche die Geräte infiziert, und den Angriff abzuschwächen. Zudem wird mit den Hardware-Fingerabdrücken dieser Rapsberry Pis experimentiert, um sie als eindeutige Identifikatoren zu verwenden. Darüber hinaus wird dieses Cluster auch dazu genutzt, ein verteiltes Framework für maschinelles Lernen zu testen, das eine reale Umgebung für das Edge-Computing simuliert.

IoT Labor in Thun.

Data Science Lab for Machine Learning Operations

Das Data Science Lab (DSL) erlaubt es den CYD Campus Forschenden, digitale Projekte nach modernen Standards des wissenschaftlichen Arbeitens und der Software-Entwicklung zu realisieren. Hierfür unterhält das DSL Anwendungen zur Versionierung (basierend auf Git) von Anweisungen (Code) und kann je nach Bedarf Rechen- und Speicherkapazität bereitstellen. Um eine optimale Nutzung der vorhandenen Ressourcen zu gewährleisten, wurden im DSL verschiedene Mechanismen implementiert, die typischerweise bei «Cloud» Infrastrukturen zur Anwendung kommen. So verfügt das DSL über Speicherkapazitäten, die flexibel für einzelne Projekte zur Verfügung gestellt und jederzeit an sich verändernde Bedürfnisse angepasst werden können. Generelle Rechenleistung wird den Projekten im DSL auf dynamische Weise zugewiesen. Dies gestattet die Entwicklung und Nutzung zahlreicher Anwendungen, von Web-Applikationen bis hin zur Verarbeitung und Analyse von Daten. Für hoch spezialisierte Analysen, wie z.B. solche, die die Anwendung von Deep-Learning-Algorithmen benötigen, kann ein Verbund von Grafikprozessoren indirekt, über eine zentrale Management Applikation angesprochen werden. Diese auch als Cluster bezeichnete Architektur ermöglicht eine effiziente und faire Nutzung der begrenzten Ressourcen. Mit dieser Konfiguration bietet das DSL die Möglichkeit, Projekte vollständig vom automatisierten Anbinden von Ressourcen über die Analyse bis hin zur Bereitstellung der Ergebnisse in deklarativer Form als Liste von Instruktionen (Code) zu definieren. Somit kann im DSL die ganze Entwicklung in einem Projekt versioniert, die Versionen automatisch getestet und nach Bedarf zur Verfügung gestellt werden. Diese Praxis kombiniert die automatische Ressourcen-Verwaltung, auch «Infrastructure as Code (IaC)» genannt, mit modernen Standards aus dem Bereich der Software-Entwicklung (DevOps) oder des maschinellen Lernens (MLOps).

Data Science Lab in Thun.

12 Anlässe

Konferenzen

28. November– 2. Dezember 22 MILCOM, Washington D.C., USA
An der MILCOM versammeln sich Wissenschaftler rund um die Themen militärischer Kommunikation und Datenanalyse. Gérôme Bovet, Leiter der Gruppe Data Science, war Organisator eines Panels im Rahmen der NATO-Arbeitsgruppe IST-ET-121 und wurde vom US Army Research Lab eingeladen, einen Vortrag zu halten.

15.–17. November 22 Rennes European Cyber Security Week
Mehr als 4000 öffentliche und private Akteure sowie 84 Partner im Bereich der Cybersicherheit trafen sich in Rennes, um künftige technologische Entwicklungen zu erkennen und zu antizipieren. Der CYD Campus nahm Teil um sich mit relevanten Akteuren zu vernetzen.

10.–11. November 22 10th OpenSky Symposium, Delft, Holland
Martin Strohmeier hat über die Gefahr von Open Aviation Datensätze referiert und dabei die neuesten Forschungsergebnisse vorgestellt.

26. Oktober 22 CYD Campus Konferenz
Die CYD Campus Konferenz 2022 fand am 26. Oktober im Kursaal in Bern statt. Im Rahmen der Veranstaltung referierten Expertinnen und Experten aus der öffentlichen Verwaltung, Akademie und Industrie zu Schlüsselthemen im Bereich der Sicherung von zukünftigen digitalen Infrastrukturen. Der CYD Campus durfte mehr als 300 Teilnehmende an dieser Konferenz begrüssen.

14.– 16. September 22 CRITIS, München, Deutschland
CRITIS bringt Forschende, Akademiker, Betreiber kritischer Infrastrukturen, die Industrie sowie Verteidigungs- und Regierungsorganisationen zusammen, die auf dem Gebiet der Sicherheit komplexer Infrastruktur-Systeme arbeiten. Auf der CRITIS 2022 präsentierte Llorenç Romá eine wissenschaftliche Arbeit, die zeigt, wie Informationen aus kritischen Infrastrukturen heimlich und systematisch exfiltriert werden können.

26.– 29. Juni 22 Cyber Week Tel Aviv, Israel
Giorgio Tresoldi stellte auf einer vom israelischen National Cyber Directorate organisierten Podiumsdiskussion Forschungsergebnisse zum Thema Cybersicherheit in der Zivilluftfahrt vor.

6.– 20. Juni 22 RSA Conference, USA
Neben der Teilnahme an der Konferenz und dem Treffen mit zahlreichen Startups hat der CYD Campus zusammen mit Swissnex und dem Swisscom Outpost im Silicon Valley einen Networking-Event im Schweizer Konsulat organisiert.

30. Mai– 2. Juni 22 CyCon, Tallinn, Estland
An der 14. Internationalen Konferenz zu Cyberkonflikten (CyCon) nahm CYD Campus Wissenschaftler Martin Strohmeier an der Podiumsdiskussion «Cyber Security Threats in the Transport Industry» teil und sprach über seine Forschungsarbeit zu Sicherheits- und Datenschutzproblemen der Satellitenkommunikation in der Luftfahrt.

6.– 7. April 22 Swiss Cyber Security Days, Freiburg
Martin Strohmeier, CYD Campus Forscher, hielt während der Konferenz einen Vortrag über die Sicherheit von Elektroautos und Ladeinfrastrukturen.

27.– 28. März 22 Applied Machine Learning Days, Lausanne
- Workshop über visuelle Desinformation von CYD Campus Mitarbeiter Raphael Meier.
- Organisation eines Artificial Intelligence & Cyber Security Track durch Martin Strohmeier zusammen mit C4DT.
- Vortrag von Vincent Lenders über die Rolle von Artificial Intelligence in der Cyberverteidigung.

Kaffeepause an der CYD Campus Konferenz 2022

Challenges & Hackathons

3.– 7. Oktober 22 Hackathon ElectroSense
Der diesjährige Hackathon konzentrierte sich auf das LoRa-Protokoll. Drei Teams arbeiteten an der Lokalisierung von LoRa-Sendern, der Erstellung von Fingerabdrücken und der Entwicklung einer OSINT LoRa-Plattform. Während verschiedener Veranstaltungen im Jahr 2022 hatten die Teilnehmenden die Möglichkeit, ihre Aktivitäten vorzubereiten, so dass sie beim Hackathon direkt mit der Datenanalyse beginnen konnten.

19.– 23. September 22 ICS Hackathon
Der CYD Campus organisierte zusammen mit dem Cyber Bataillon 42 einen Hackathon rund um industrielle Kontrollsysteme (ICS) und operative Technologien (OT). Die 30 Teilnehmenden führten Schwachstellenanalysen durch, untersuchten verschiedene Angriffsvektoren und entwickelten geeignete Gegenmassnahmen. Weitere Informationen finden Sie im Kapitel Highlights.

5.– 7. September 22 Satcom Hackathon
Der CYD Campus organisierte einen Hackathon zum Thema Satelliten und Satellitenkommunikation. Die 10 Teilnehmenden kamen aus dem Bereich der universitären Kollaborationen und von anderen Stellen im Bereich des Bundes. Ziel war es Bodenstationen, CubeSats und Kommunikation zwischen Satelliten unter die Lupe zu nehmen, zu verstehen und mögliche Angriffsvektoren zu finden.

Data Science Challenges

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

Security Challenges

05. Dezember 22	Hack the Box
03. Oktober 22	Scavenger Hunt
29. August 22	WebApp/Linux Hacking
13. Juni 22	Android Application Hacking
04. April 22	Static Reverse Engineering

Neueröffnung Standort Zürich

24. November 22
Im Jahr 2022 feierte der CYD Campus zusammen mit ausgewählten Forschungspartnern die Neueröffnung seiner Räumlichkeiten an der Zollstrasse 62 in Zürich. Gleichzeitig wurden die drei CYD Campus-Standorte (Thun, Lausanne, Zürich) mit SCION-Netzwerkanschlüssen verbunden. Die Technologie ersetzt das unsichere Internet-Routing-Protokoll durch ein sichereres und effizienteres Protokoll.

Lunchseminare

Im Rahmen dieser Informationsveranstaltungen werden von ausgewählten Referentinnen und Referenten Vorträge zu spezifischen CYD Fachthemen für Kunden der Verteidigung und der Bundesverwaltung organisiert.

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

Forschungsrapporte

Die Jahresrapporte dienen dazu, über laufende Forschungsthemen zu Gunsten der Auftraggeber und interessierten Stellen zu berichten. Die Rapporte fanden in hybrider Form statt, wobei jeweils ca. 80 Gäste begrüsst werden konnten. Davon waren einige Teilnehmende aus dem Armee Stab, FUB, GS VBS, NDB.

2. September 22	Forschungsrapport 3b Data Science
6. Juli 22	Forschungsrapport 3a Cyberspace

Retreats

4.– 8. Juli 22 Cyber Alp Retreat in Sachseln
In Sachseln (Obwalden) trafen sich Forschende des CYD Campus und ausgewählte Forschungspartner und referierten zu zentralen Themen wie Internet der Dinge, Verkehrssicherheit, Desinformation in sozialen Medien sowie Technologie- und Marktmonitoring. Die Veranstaltung brachte 120 Teilnehmende aus dem VBS, der Industrie und der Akademie zusammen, um sich über mehrere Tage zu aktuellen und zukünftigen Herausforderungen und Treibern im Cyberspace auszutauschen.


Lunchseminar zu Post-Quantum Cryptography


Cyber-Alp Retreat 2022 in Sachseln


Cyber Security Jam Session in Zürich

Besuche

20. Dezember 22	Österreich Arbeitsbesuch, Zürich
20. Dezember 22	Besuch Kdt LVb Pz / Art
28. November 22	Besuch Rüstungschef mit Vertreter/innen aus Norwegen
23.– 24. November 22	Besuch Königliche Technische Hochschule (KTH) Schweden, Thun/Zürich
22. November 22	Besuch Nachrichtendienst des Bundes, Thun
22. November 22	Besuch Eidgenössische Finanzkontrolle, Thun
10. November 22	Besuch Sicherheitspolitische Kommission des Ständerates, Thun
11. November 22	Besuch Advanced Course in Engineering (ACE), Thun
8. November 22	Besuch Technischer Lehrgang Cyber, Zürich
8. November 22	Besuch Fachstab Cyber der Armee, Zürich
2. November 22	Besuch Arbeitsgruppe Informationssicherheit (AIS), Thun
31. Oktober 22	Besuch Cyber-Lehrgang 22, Thun
22. September 22	Besuch Luftwaffe
7. September 22	Besuch Hochschule Luzern, Zürich
24. Mai 22	Besuch der GL Swisstopo, Thun
23. Mai 22	Besuch Delegation Rüstungschef Schweden, Thun
16. Mai 22	Besuch Cyber-Lehrgang 22, Thun

Technologie- und Marktmonitoring Anlässe

31. Mai 22 Startup Jam Session in Zürich

Der CYD Campus veranstaltete seine erste Cyber Security Startup Jam Session in Zürich und brachte Fachleute von armasuisse W + T, Swisscom, dem ETH Entrepreneur Club und mehreren studentischen Risikokapitalfonds mit UnternehmerInnen, Studierenden und Cybersicherheits-ExpertInnen zusammen. Ziel der Initiative ist es, die Zusammenarbeit mit dem Startup-Ökosystem in der Schweiz zu fördern und die Entwicklung von innovativen Technologielösungen voranzutreiben.

Studentischer Fachaustausch

Dienstags im Zweiwochentakt berichten CYD Studierende und Praktikanten und Praktikantinnen über Ergebnisse ihrer Forschungsprojekte. In diesem Rahmen treffen sich alle Mitarbeitenden der jeweiligen Standorte online um über die Forschungsarbeiten und Erkenntnisse zu diskutieren.

Rekrutierungsplattform Studierende

7. Oktober 22 EPFL Forum:

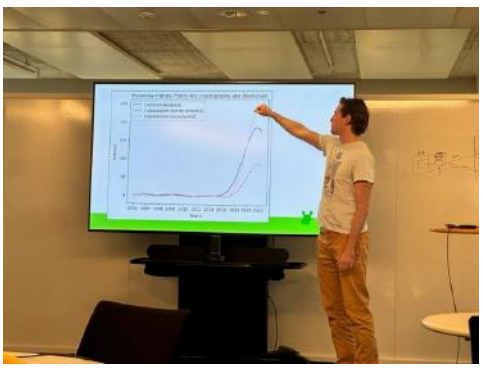
Am diesjährigen EPFL Forum war der CYD Campus vertreten, um mit Studierenden in Kontakt zu treten und ihnen Einblicke in die Tätigkeiten des CYD Campus zu gewähren sowie über die diversen Möglichkeiten zu berichten, die der CYD Campus bietet, um praktische Erfahrungen zu sammeln.

CYD Fellowship Workshop für Bewerbende:

29. Juni 22

25. Januar 22

Besuch Fachstab Cyber beim CYD Campus in Zürich



Studentischer Austausch in Lausanne

13 Referate

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

Vortrag von Raphael Meier über Desinformation an der CYD Campus Konferenz in Bern.

Martin Strohmeier hält einen Vortrag zu Cybersicherheit in der Satelliten-Kommunikation.

Vortrag von Vincent Lenders über den CYD Campus.

14 Wissenschaftliche Arbeiten

14.1 Publikationen

Dezember

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

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

Robust and Explainable Identification of Logical Fallacies in Natural Language Arguments
Zhivar Sourati, Vishnu Priya Prasanna Venkatesh, Darshan Deshpande, Himanshu Rawlani, Filip Ilievski, Hông-Ân Sandlin, Alain Mermoud. arXiv preprint arXiv:2212.07425.

November

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

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

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

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

Oktober

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

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

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

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

September

RITUAL: A Platform Quantifying the Trustworthiness of Supervised Machine Learning

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

High Data Throughput Exfiltration through Video Cable Emanations,

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

A Secure Framework for Distributed Privacy-Preserving Threat Intelligence Sharing

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

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

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

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

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

Building collaborative cybersecurity for critical infrastructure protection

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

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

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

August

SAFEAMC: Adversarial Training for Robust Modulation Classification Models

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

Aggregate-based Congestion Control for Pulse-Wave DDoS Defense

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

Building an Avionics Laboratory for Cybersecurity Testing

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

An Experimental Study of GPS Spoofing and Takeover Attacks on UAVs

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

Juli

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

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

Communicating via Markov Decision Processes

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

Juni

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

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

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

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

Efficient Collective Action for Tackling Time-Critical Cybersecurity Threats

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

On the Security of the FLARM Collision Warning System

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

Security and Privacy Issues of Satellite Communication in the Aviation Domain

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

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

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

Mai

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

Étienne Voutaz & Albert Blarer, Computing and Informatics.

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

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

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

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

April

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

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

März

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

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

Februar

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

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

Januar

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

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

14.2 Studentische Arbeiten

CYD Fellows

Postdoc

Dr. **Lucianna Kiffer**	*Security and Usability of Blockchain Networks*	ETH Zürich
Dr. **Andrei Kucharavy**	*Evolutionary Dynamics for Improved GAN Detection*	EPF Lausanne
Dr. **Dimitri Percia David**	*Technology Forecasting and Market Monitoring for Cyber-Defence*	Universität Genf

PhD

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

Master

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

Studierende und Praktikant/innen

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

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

15 Kommunikation

@Cyber-Defence Campus

@cydcampus

Webmitteilungen

- 11.11.2022, VBS testet das SCION Netzwerk für die Schweizer Cyberabwehr
- 26.10.2022, Treffen Sie die Finalisten der Cyber Startup Challenge 2022
- 30.09.2022, CYD Campus Hackathon zu industriellen Kontrollsystemen
- 29.09.2022, Maschinelles Lernen für mehr Sicherheit in Stromnetzten
- 01.09.2022, Stärkung der kollektiven Cyber-Resilienz
- 02.08.2022, Neues Cyber Avionics Labor
- 23.06.2022, Erste Startup Jam Session beim Cyber-Defence Campus
- 20.06.2022, Aufruf für die Cyber Startup Challenge 2022
- 07.02.2022, Der Cyber-Defence Campus veröffentlicht seinen Jahresbericht 2021

Medienmitteilungen

- 26.10.2022, «Cyber Startup Challenge 2022»: Startup ONEKEY überzeugt das VBS

armasuisse Print

- Dezember Ausgabe, Vertretung des Cyber-Defence Campus am Cooperative Cyber Defence Centre of Excellence in Estland stärkt die Zusammenarbeit zwischen der Schweiz und der NATO
- Ausgabe 2022, Forschungsbroschüre armasuisse Wissenschaft und Technologie

Videos

- 22.06.2022, EPFL/Cyber-Defence Campus Zusammenarbeit
- Digitalisierung, Innovation & Sicherheit im VBS, Fokus armasuisse

16 Ausblick 2023

Im kommenden Jahr soll die Zusammenarbeit des CYD Campus mit Hochschulen und der Wirtschaft weiter ausgebaut werden, insbesondere in den Bereichen der Digitalisierung, der künstlichen Intelligenz und der Innovation. In diesen drei Bereichen steht das VBS, aber auch die gesamte Bundesverwaltung, vor grossen technologischen Herausforderungen. Weiterhin erwähnenswert sind nachfolgende Entwicklungsschritte und geplante Tätigkeiten des CYD Campus, welche im Jahr 2023 gemäss Strategie Cyber VBS umgesetzt werden sollen:

Der Zusatzbericht zum sicherheitspolitischen Bericht, der 2022 veröffentlicht wurde, erläutert, warum die internationale Zusammenarbeit durch den Krieg in der Ukraine für die Schweiz noch dringlicher geworden ist. Der CYD Campus wird auch 2023 einen wesentlichen Beitrag zur verstärkten internationalen Kooperation im Bereich der Cyberverteidigung leisten und die Beziehungen unter anderem mit der NATO weiter ausbauen.

Ein neues CYD Fellowship für Proof of Concepts soll ab 2023 die Innovationskraft von jungen Cyber-Talenten in der Schweiz fördern und sie besser in die Innovationsprozesse des VBS einbinden. Es dient auch der Entwicklung von unternehmerischem Denken und Handeln.

Wie jedes Jahr planen wir eine CYD Campus Konferenz und weitere Cyber-Anlässe durchzuführen. Die CYD Campus Konferenz 2023 wird am 26. Oktober 2023 im Kursaal in Bern stattfinden. Wir freuen uns darauf, über 300 Cyber-Expertinnen und Experten sowie Interessierte an dieser Veranstaltung begrüssen zu dürfen. Hackathons zu der Sicherheit von Autos und kritischen Infrastrukturen sind ebenfalls geplant.

Als Massnahme der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS2) soll die Weiterentwicklung eines automatisierten Technologie-Radars (TMM 2.0) vorangetrieben werden, welcher bestehende Datenbanken, Websites und Verzeichnisse nutzt, um Trends und Technologien frühzeitig zu erkennen und deren Bedeutung für die Schweiz einzuschätzen. Dieses Instrument soll dazu dienen, die Scouting- und Monitoring Tätigkeiten des CYD Campus zu unterstützen, aber auch die sicherheitsrelevante Technologie- und Industrie Basis (STIB) der Schweiz besser zu verfolgen.

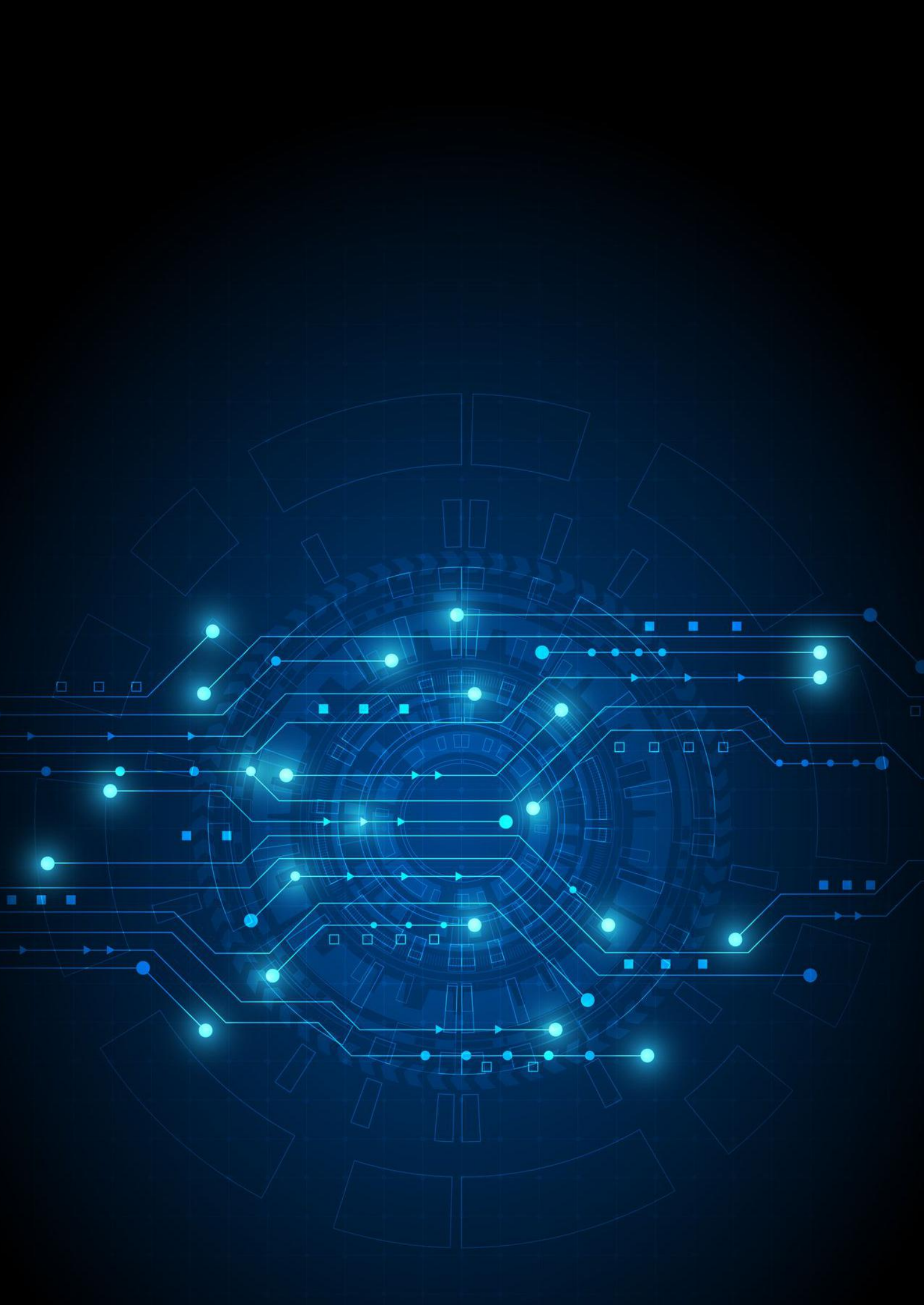
Mit dem Space Campus wird eine neue Plattform für die Space Community geschaffen, die Forschungsprojekte und Talente in diesem Bereich sowie unternehmerische Möglichkeiten fördert. Der CYD Campus wird dabei den Space Campus in Lausanne beherbergen und die Schweizer Innovation im Weltraum stärken.

Im 2023 streben wir an die Zusammenarbeit mit dem Cyber Bataillon 42 zu vertiefen. Das Bataillon hat Anfang 2022 seinen Dienst aufgenommen und besteht aus Angehörigen der Armee, die aufgrund ihrer zivilen Tätigkeit über wichtiges Know-how im IT- und Cybersicherheitsbereich verfügen. Es wird ein wichtiger Bestandteil des im Aufbau befindlichen Cyber Kommandos, das aus der heutigen Führungsunterstützungsbasis (FUB) hervorgehen wird. Durch die Einbindung dieser Fachleute in spezifische Projekte profitieren sowohl der CYD Campus als auch das Cyber Bat 42 von wertvollen Synergien.

Mit zentralen Projekten in Brennpunktthemen wie der Robustheit von künstlicher Intelligenz und der Sicherheit von 5G und oder IoT Sicherheit wollen wir auch im Jahr 2023 einen bedeutenden Mehrwert für die Schweizer und internationale Cyber-Defence Landschaft generieren.

Im Frühjahr 2023 wird der Release einer neuen Website erfolgen, die der Cyber-Defence-Community mehr Inhalte und aktuelle Nachrichten, z. B. über unsere Forschungsprojekte und Veranstaltungen, bieten wird. Dadurch können wir angesichts der sich stets wandelnden Technologie- und Bedrohungslandschaft agiler mit der Cyber-Community interagieren und kommunizieren.

Zudem werden wir laufend prüfen wie wir spezifisch unsere Angebote für das anstehende Cyber Kommando und das neue Bundesamt für Cybersicherheit erweitern wollen, beispielsweise in den Bereichen der Innovation und des Cyber-Trainings.



Kontakt
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