Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confedraziun svizra

armasuisse
Wissenschaft und Technologie

Cyber-Defence Campus

Jahresbericht 2021

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

2021 war wie bereits das Jahr zuvor stark von der COVID-19 Pandemie geprägt. Nebst den negativen Auswirkungen wie die Überlastung des Gesundheitssystems und höhere Staatsausgaben hat die Pandemie aber auch zu einer raschen Beschleunigung der Digitalisierung geführt. Cyber-Bedrohungen haben dadurch deutlich an Bedeutung und Komplexität gewonnen und wirken sich zunehmend kritisch für die Sicherheit unserer Gesellschaft aus.

Unsere Mitarbeitenden und Partner des Cyber-Defence (CYD) Campus leisten tagtäglich einen wichtigen Beitrag zur Cybersicherheit der Schweiz, indem sie sich in der Forschung, der Innovation, der Wissensvermittlung oder der Talentausbildung einsetzen. Seit der Gründung vor drei Jahren sind beim CYD Campus mehrere strategische Ziele des Aktionsplans Cyberdefence, der Strategie Cyber VBS und der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) umgesetzt worden. Im Jahr 2021 wurden insbesondere in den nachfolgenden Bereichen bedeutende Fortschritte und Ergebnisse erzielt.

Das systematische Scouting von neuen Technologien und Startups wurde auf sechs weitere Länder ausgeweitet. Ergänzend zum bereits etablierten Technologie- und Marktmonitoring in der Schweiz, den USA und Singapur werden nun auch Cyber-Entwicklungen und Trends in Grossbritannien, Deutschland, Österreich, Frankreich, Israel und Estland aktiv mit einem internationalen Partnernetzwerk verfolgt. Die neuesten Entwicklungen aus diesen Regionen werden nun frühzeitig analysiert und im Rahmen von Studien und Proof-of-Concepts mit den relevanten Stellen beim Bund untersucht. Allein im letzten Jahr wurden so ein Dutzend Proof-of-Concepts mit Bedarfsträgern realisiert. So wurde zum Beispiel am ersten Pilotprojekt der vordienstlichen Cyber-Ausbildung der Armee eine innovative Software eines Startups vom CYD Campus eingesetzt.

Die Forschungszusammenarbeit mit Hochschulen wie der ETH Zürich, EPF Lausanne, der ZHAW oder der Universität Lausanne wurden weiterentwickelt und entlang des Bedarfs der Verteidigung auf neue Technologiefelder wie die Post-Quanten-Kryptographie, die Bekämpfung von Desinformation oder den Schutz von kritischen Infrastrukturen ausgeweitet. Zudem konnte die Schweizer Cyberdefence Community dank unseren Veranstaltungen wie den Lunch Seminars, den Hackathons, den Konferenzen oder der diesjährigen Cyber Startup Challenge gepflegt und weiter ausgebaut werden. Es freut mich sehr, dass dieses Jahr zehn Studierende von Schweizer Universitäten ihre Forschungsarbeit als CYD Fellow durchführen konnten und weitere 35 Studierende ein Hochschulpraktikum oder eine Masterarbeit im Rahmen der Talentförderung beim CYD Campus absolviert haben.

Der vorliegende Jahresbericht gibt Auskunft über die öffentlichen, nicht klassifizierten Aktivitäten des CYD Campus im Jahr 2021. Ich wünsche Ihnen eine spannende Lektüre.

Thun, 31. Dezember 2021

Dr. Vincent Lenders
Leiter Cyber-Defence Campus

1 Über den Cyber-Defence Campus

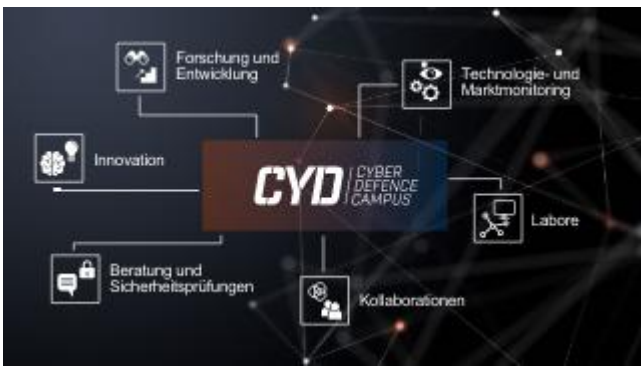
1.1 Strategieeinbettung und Schlüsselaufgaben

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 drei 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), an der EPF Lausanne und an der ETH Zürich. Dies erlaubt es ihm effizient Know-how aufzubauen und Cyber-Expertise bereitzustellen, gemäss den Bedürfnissen der Schweizerischen Eidgenossenschaft. Der CYD Campus wirkt dementsprechend als Bindeglied zwischen dem Privatsektor, 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:



Kernkompetenzen des Cyber-Defence Campus

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 Cyber-Risiken 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.

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, Einblicke in die Umsetzung der oben genannten Aufgaben im Jahr 2021 des Cyber-Defence Campus zu gewähren. Dabei wird ein kurzer Überblick über einige Highlights des Jahres 2021 gegeben. Die öffentlichen Tätigkeiten im Rahmen von Forschungsprojekten, Kundenaufträgen und Demonstratoren werden ebenfalls erläutert. Weiter werden die Arbeiten im 2021 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 ein Ausblick auf das Jahr 2022 gewährt.

1.2 Partner

Der CYD Campus ist organisatorisch bei armasuisse Wissenschaft und Technologie (VBS) angesiedelt. Rund 50 weitere inländische und ausländische Organisationen aus Wissenschaft, Industrie und dem öffentlichen Sektor wirken als Partner mit.

Staatliche Partner/Bund

- Schweizer Armee
- Nachrichtendienst des Bundes NDB
- Bundespolizei fedpol
- Bundesamt für Statistik BFS
- Swisstopo
- Nationales Zentrum für Cybersicherheit NCSC
- Bundesamt für Zivilluftfahrt BAZL
- NATO CCDCoE
- US Air Force Research Lab
- US Army Research Lab
- Luxemburgische Armee
- European Defence Agency EDA
- Bundesamt für Sicherheit in der Informationstechnik (BSI), DE
- Swissnex

Hochschulen

- EPF Lausanne
- Center for Digital Trust (C4DT)
- ETH Zurich
- Zurich Information Security and Privacy Center (ZISC)
- Militärakademie an der ETH Zürich
- Universität Freiburg
- Universität Zürich
- Universität Lausanne
- Universität Neuchâtel
- Universität Oxford, UK
- KU Leuven, BEL
- IMDEA, ESP
- Universität Murcia, ESP
- Universität Rey Juan Carlos, ESP
- TU Kaiserslautern, DE
- ZHAW
- FHNW
- IDSIA
- Northeastern University, USA
- HEIG-VD
- Universität Genf
- HEVS
- HEPIA

Industriepartner

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

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

Stefan Engel

Leiter Business Development und

Stellvertretender Leiter des CYD Campus

Dr. Gérôme Bovet

Leiter Forschungsprogramm

und Gruppe Data Science

Dr. Colin Barschel

Leiter Innovation und

Industriekollaborationen

Giorgio Tresoldi

Leiter internationale Beziehungen

und Scouting

Dr. Alain Mermoud

Leiter Technologie und

Marktmonitoring

Monia Khelifi

Führung der Assistenz

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 (Eintritt April 2021)

Dr. **Daniel Moser** ist Experte für die Sicherheit von kritischen Infrastrukturen und drahtloser Kommunikation sowie wissenschaftlicher Projektleiter

Dr. **Miguel Keer** ist wissenschaftlicher Projektleiter

Dr. **Luca Gambazzi** ist Security Auditor und wissenschaftlicher Projektleiter (Austritt August 21)

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. **Gérôme Bovet** ist Leiter der Gruppe Data Science und Forschungsprogrammleiter

Dr. **Etienne Voutaz** ist Data Scientist und wissenschaftlicher Projektleiter

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

Dr. **Albert Blarer** ist Data Scientist und wissenschaftlicher Projektleiter

Dr. **Metin Feridun** ist Big Data Spezialist und wissenschaftlicher Projektleiter

Dr. **Mathias Humbert** ist Machine Learning und Privacy Experte sowie wissenschaftlicher Projektleiter (Austritt November 21)

Dr. **Raphael Meier** ist Experte für Bildverarbeitung und Machine Learning sowie wissenschaftlicher Projektleiter (Eintritt Mai 21)

Thomas Sigrist ist zuständig für Recheninfrastrukturen und technischer Projektleiter (Austritt Dezember 21)

Ivo Stragiotti ist zuständig für Laborinfrastrukturen und technischer Projektleiter (Eintritt Juli 21)

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 2021 konnten 24 Studierende ein Praktikum beim Cyber-Defence Campus absolvieren. Die Praktikantinnen und Praktikanten stammen aus unterschiedlichen Universitäten wie der EPF Lausanne, der ETH Zürich oder der Universität St. Gallen.

Huzar Marin, September 21 - Februar 22, Cyber Sicherheit, Lausanne

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

Benjamin Kilian, September 21 - Februar 22, Cyber Sicherheit, Lausanne

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

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

Michael Tsesmelis, Juni 21 - Mai 22, Technologie- und Marktmonitoring, Lausanne

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

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

William Lacube, März 21 - Dezember 21, Technologie- und Marktmonitoring, Lausanne

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

Eric Jolles, März 21 - Dezember 21, Technologie- und Marktmonitoring, Lausanne

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

Caroline Violot, Februar 21 - Juli 21, Data Science, Lausanne

Anton Santiago Moreno, Februar 21 - Juli 21, Technologie- und Marktmonitoring, Lausanne

Valérian Rey, Oktober 20 - März 21, Data Science, Lausanne

Marc Kaufmann, Oktober 20 - Juni 21, Data Science, Zürich

Stéphanie Lebrun, Oktober 20 - März 21, Data Science, Lausanne

Etienne Bonvin, Oktober 20 - März 21, Data Science, Lausanne

Adrien Prost, Oktober 20 - März 21, Data Science, Lausanne

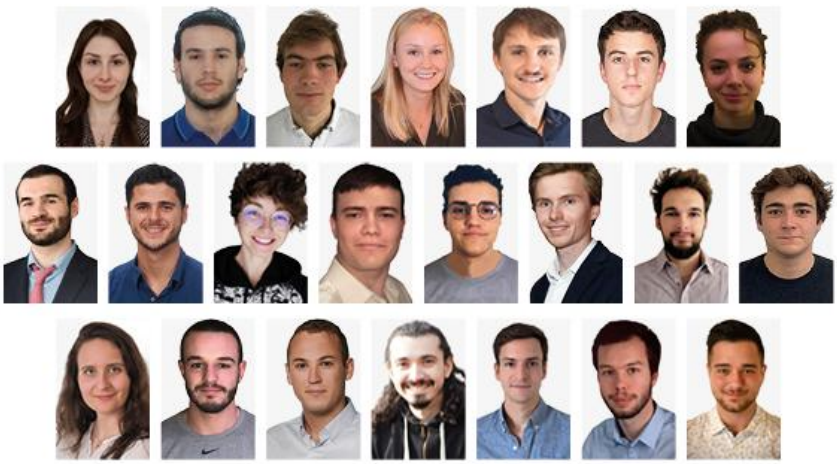
Benno Schneeberger, September 20 - Februar 21, Cyber Sicherheit, Lausanne

Ejub Talovic, September 20 - Februar 21, Technologie- und Marktmonitoring, Lausanne

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

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

Llorenç Roma, April 20 - März 21, Cyber Sicherheit, Thun



CYD Fellows

Im Jahr 2020 hat der CYD Campus zusammen mit der EPF Lausanne ein Cyber-Defence (CYD) Fellowship Programm lanciert, um den Studierenden die Möglichkeit zu geben, sich in Cyberverteidigungsthemen zu vertiefen und die Kompetenzen in der Schweiz im Bereich der Cyberabwehr 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, dass den Studierenden einen CYD Experten / 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 an der EPF Lausanne, der ETH Zürich sowie am Hauptsitz in Thun durch. CYD Fellowships werden mehrmals jährlich für Masterstudierende, Doktoranden sowie Postdocs vergeben und gewähren eine Lebenshaltungskostenvergütung. Im Jahr 2021 waren zehn Fellows aktiv:

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

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

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

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

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

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

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

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 2021 wurden Arbeiten von elf Studierenden durch den CYD Campus begleitet.

Pedro Miguel Sanchez, Universität Murcia, September 21 - Dezember 21, Betreuer: Dr. Gérôme Bovet

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

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

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

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

Philippe Panhaleux, ETHZ, März 21 - August 21, Betreuer: Dr. Martin Strohmeier

Julian Huwyler, ETHZ, März 21 - August 21, Betreuer: Dr. Martin Strohmeier

Leeloo Granger, ETHZ, März 21 - August 21, Betreuer Dr. Martin Strohmeier

Jannik Brun, ETHZ, März 21 - August 21, Betreuer: Dr. Martin Strohmeier

Michael Karpf, ETHZ, März 21 - August 21, Betreuer: Dr. Martin Strohmeier

Georg Baselt, ETHZ, Februar 21 - Juli 21, Betreuer: Dr. Martin Strohmeier

2 Highlights

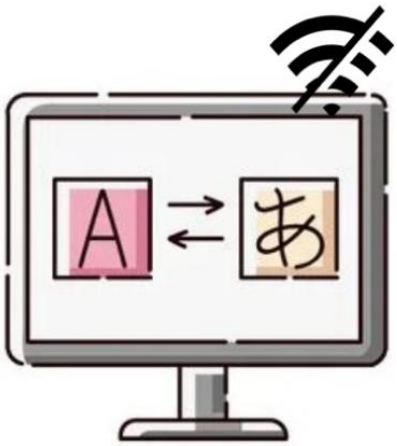
Car Hackathon

Autos werden immer intelligenter. Die neuen Funktionen bringen zwar mehr Komfort und Sicherheit, schaffen aber auch zahlreiche Cyber-Sicherheitslücken. Diese befinden sich nicht nur in potenziell kritischen Systemen wie Bremsen, Motor usw., sondern auch in Komponenten, die von aussen zugänglich sind, z. B. die drahtlosen Schnittstellen des Multimediasystems. Die Gefahrensituation wird durch die Einführung von Elektroautos noch verschärft, da alle Systeme in der Regel an ein einziges Bussystem angeschlossen sind. Die Ladeinfrastruktur dieser Fahrzeuge wirft weitere Fragen zur Zuverlässigkeit und Sicherheit auf (Ausfall Ladestation, Datenaustauch Ladestation-Auto etc.). Die zunehmende Zahl an Sensoren wie z. B. Radar, Lidar, Kameras und deren Abhängigkeit von künstlicher Intelligenz, um die grosse Menge der von ihnen erzeugten Daten zu analysieren, erschaffen ebenfalls neue Schwachstellen.
Um die entsprechende Expertise beim CYD Campus und in der Bundesverwaltung rasch zu erhöhen wurde im Oktober 2021 während fünf Tagen ein Hackathon in Thun durchgeführt. Insgesamt 20 Teilnehmende von der ETH Zürich, der Universität Oxford, fedpol, der Armee und armasuisse haben mit Unterstützung von Experten der japanischen Firma White Motion mögliche Sicherheitsprobleme von sieben verschiedenen Fahrzeuge (unterschiedlicher Hersteller, militärisch / zivil, elektrisch / nicht-elektrisch) aufgedeckt und erste Schritte in diesem Forschungsbereich unternommen. Die Zusammensetzung der Teilnehmer ermöglichte einen interdisziplinären Austausch sowie eine intensive und fruchtbare Arbeit. Zudem konnten mehrere Demonstratoren zusammengestellt werden, die im CYD Campus zum Einsatz kommen werden. Darüber hinaus wurden Daten gesammelt, die in den kommenden Jahren in die gemeinsame CYD Campus Forschung mit den Universitäten einfliessen werden.

Training mit Experten und Schwachstellenüberprüfung während des Car Hackathons in Thun

Offline-Übersetzungsdienst in der Armee

Heutzutage sind zahlreiche automatische Übersetzungsprogramme online verfügbar. Sie bieten die Möglichkeit, zwischen einer Vielzahl von Sprachen zu übersetzen, wobei die Qualität der Übersetzung variiert, was zum einen von dem Tool selbst und zum anderen von den zugrunde liegenden Sprachen abhängt. Allerdings haben Online-Übersetzungsdienste zu zahlreichen Sicherheitsproblemen geführt, da Inhalte mit persönlichen oder vertraulichen Daten nach aussen dringen konnten. Im Rahmen eines Innovationsprojekts wurde ein Proof-of-Concept eines internen, offline arbeitenden maschinellen Übersetzungstools realisiert, das in der Lage ist, verständliche bidirektionale Übersetzungen zwischen Englisch und sechs anderen Sprachen zu liefern. Mit Deutsch, Französisch, Italienisch, Russisch, Arabisch und Chinesisch als Ausgangs- und Zielsprachen wurde die Machbarkeit dieses Tools für den Einsatz in Systemen der Armee bewiesen, unabhängig von der zugrunde liegenden Sprachkomplexität oder dem Schriftsystem.



Dr. Mathias Humbert wird Professor für Cybersicherheit an der Universität Lausanne

Dr. Mathias Humbert, ein wissenschaftlicher Mitarbeiter des CYD Campus, wurde im November 2021 zum Professor an der Universität Lausanne befördert. Während seiner zweijährigen Tätigkeit beim CYD Campus hat Mathias Humbert zahlreiche Studierendenprojekte betreuen können, und somit wichtige Erfahrungen für diese neue Herausforderung gesammelt. Als Professor an der Universität Lausanne wird er die langfristige Zusammenarbeit zwischen dem CYD Campus und seinem Departement auf dem Gebiet der Cybersicherheit und des Datenschutzes weiter vorantreiben. Für den CYD Campus ist es ein zentrales strategisches Ziel, Cyber-Talente mit Blick auf die Sicherheit der Schweiz zu fördern.

Sicherheitslücken in VPN Software gefunden

Im Rahmen des Vulnerability Research Programms wurden VPN Software Lösungen von unterschiedlichen Herstellern auf Schwachstellen untersucht. Von einem CYD Campus Forscher wurde unter anderem eine schwerwiegende Sicherheitslücke im VPN Client der amerikanischen Firma F5 entdeckt. Die bis dahin unbekannte Schwachstelle konnte von unberechtigten Benutzenden ausgenutzt werden, um Administratorenrechte auf denjenigen Windows Client-Systemen zu erhalten, auf denen die VPN Software installiert wurde. Die VPN Software wird von zahlreichen Schweizer Unternehmen eingesetzt, um Mitarbeitenden den Fernzugriff auf das eigene Firmennetzwerk zu ermöglichen. Durch die Covid-19 Pandemie und die damit verbundene Home-Office-Pflicht wurde die Verwendung von VPN Clients zu einer gängigen Praxis. Dank des frühzeitigen Hinweises des CYD Campus an den Hersteller im Februar 2021, konnte die Lücke geschlossen werden. Am 1. Juni 2021 wurde das entsprechende Sicherheitsupdate veröffentlicht. Dieses Highlight veranschaulicht die Relevanz und Wirksamkeit der Schwachstellenforschung des CYD Campus für die Sicherheit der Schweiz.

CYD Campus Konferenz und CRITIS

Am 28. September 2021 fand im EPFL SwissTech Convention Center in Lausanne die CYD Campus Konferenz statt und wurde angesichts der anhaltenden Pandemie gleichzeitig online übertragen. Die Konferenz begrüsste vor Ort 130 Teilnehmende und weitere 80 Partizipierende folgten der Veranstaltung online. Experten und Expertinnen aus Akademie, Verwaltung und Wirtschaft hielten an der Konferenz Vorträge zu Schlüsselthemen der Sicherheit kritischer Informationsinfrastrukturen. Die Veranstaltung bot eine Plattform für den Austausch über die aktuellen und künftigen Herausforderungen und Treiber im Cyberspace. Am Nachmittag wurde im Anschluss an die Pitches der drei Finalisten der Cyber Startup Challenge, das Zürcher Unternehmen Decentriq zum Gewinner-Startup gekürt. Die Konferenz fand in Kollaboration mit der 16. Internationalen Konferenz zur Sicherheit kritischer Informationsinfrastrukturen (CRITIS 2021) statt, die am 27. und 29. September am selben Ort veranstaltet wurde.

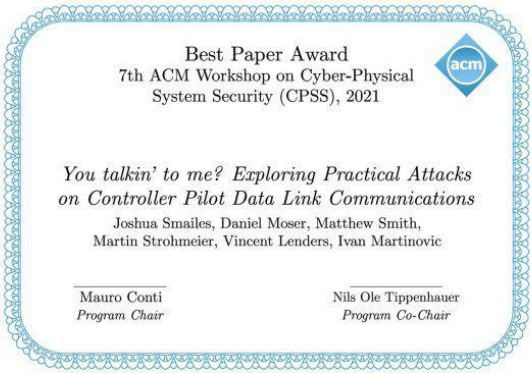
Teilnehmende der CYD Campus Konferenz & CRITIS 2021 in Lausanne

Konferenzprogramm – CRITIS 2021

CYD Campus Awards

Best Paper Award am Cyber-Physical System Security Workshop

Drei Wissenschaftler/innen des CYD Campus erhielten zusammen mit Forschenden der Oxford Universität den Best Paper Award des 7. ACM Cyber-Physical System Security (CPSS) Workshops. In der Forschungsarbeit demonstrieren die Wissenschaftler/innen, dass ein Angreifer durch das Kapern der Verbindung zwischen Fluglots/innen und der Besatzung der Flugzeuge vorgeben kann, ein legitimer Fluglotse zu sein, um anschliessend dem Zielflugzeug falsche Anweisungen zu geben. Die Schwachstelle soll ein signifikantes Sicherheitsrisiko für Flugzeugen bergen. Weiter erarbeiteten sie drei Gegenmassnahmen, um diese Sicherheitsrisiken im Luftraum zu bewältigen. Diese reichen von Plausibilitätsprüfungen und Alarmierung bis hin zur Verwendung von Nachrichten-Signaturen oder Verschlüsselung.
Zur Publikation


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

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

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

Mauro Conti, *Program Chair*
Nils Ole Tippenhauer, *Program Co-Chair*

Auszeichnung zum erhaltenen Best Paper Award von ACM

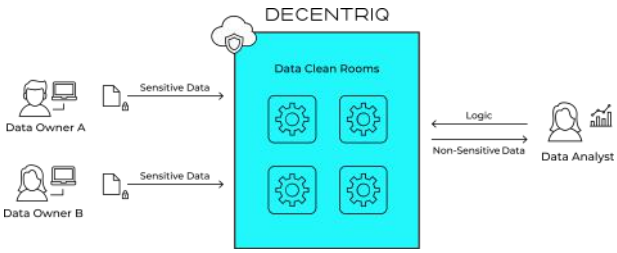
Stéphanie Lebrun präsentiert Ihre Arbeit an der CRITIS 2021, welche mit dem Young CRITIS Award geehrt wurde

Young CRITIS Awards

Im Rahmen der CRITIS 2021 wurde der Young CRITS Award verliehen um junge Wissenschaftler und Wissenschaftlerinnen, die im Bereich des Schutzes kritischer Infrastrukturen forschen, zu fördern und zu unterstützen. Die CRITIS 2021 zeichnete die besten Arbeiten von drei jungen Wissenschaftlern aus. Santiago Anton Moreno und Stéphanie Lebrun, beide CYD Campus Hochschulpraktikanten, wurden zweit-, respektive, drittplatziert und erhielten für ihre Beiträge insgesamt 1500 Franken. Santiago Anton Moreno entwickelte Modelle, wie der Markt und die Technologien für Cybersicherheit bewertet werden können, um Investitionsentscheidungen zur Gewährleistung der Sicherheit von kritischen Infrastrukturen zu erleichtern. Stéphanie Lebrun hat sich in ihrer Arbeit mit der Sicherheit von GNSS Infrastrukturen auseinandergesetzt.

Cyber Startup Challenge

Die Cyber Startup Challenge 2021 hatte das Ziel, die Startup-Technologie-Landschaft rund um das Thema «Stärken Sie Ihr Information Sharing and Analysis Center (ISAC)» zu entdecken und suchte nach innovativen Lösungen im Bereich der Cyber-Bedrohungsaufklärung mit Fokus auf den Schutz kritischer Infrastrukturen. 38 Startups aus Europa, den USA und Asien nahmen an der Challenge teil. Die Jury, bestehend aus Cyber-Expertinnen und Cyber-Experten des VBS und von armasuisse W + T, wählte die drei Finalisten Decentriq, Constella Intelligence und Pandora Intelligence aus, die am 28. September 2021 einen Pitch an der CYD Campus Konferenz hielten. Das Zürcher Startup Decentriq überzeugte schliesslich die Jury mit seiner innovativen Software-as-a-Service (SaaS)-Plattform, die «Data Clean Rooms» für Unternehmen anbietet. Die Technologie ermöglicht es internen und externen Akteuren der kritischen Infrastrukturen, sicher Cyber-Daten auszutauschen und aggregierte und anonyme Einsichten zu erhalten. Dies erhöht ihre Cybersicherheit, ohne den Datenschutz zu beeinträchtigen. Decentriq wird nun im 2022 zusammen mit dem CYD Campus ein Proof-of-Concept seiner Technologie in einer realen Umgebung des VBS integrieren.



Lösungsansatz von DECENTRIQ, Gewinner der Cyber Startup Challenge 2021

3 CYD 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 auch 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 Zürich, Lausanne und Thun an. Darüber hinaus werden studentische Projekte auf Bachelor-, Master- und PhD-Stufe definiert und von CYD Campus Forschenden betreut. Diese Studierenden sind an einer beliebigen Schweizer 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 2021 wurden 24 Hochschulpraktikant/innen beschäftigt und elf studentische Arbeiten durch CYD Campus Wissenschaftler/innen betreut. Zudem waren zehn 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.

Einige CYD Fellows in Lausanne

Hochschulpraktikantin bei Ihrer Cyber-Ausbildung im CYD Campus Lausanne

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 Cyberdefence. 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 Cyberdefence-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 Cyber Sicherheit

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.

Künstliche Intelligenz für Cyberdefence: Blue Team Automation

Durch die hohe Komplexität und Geschwindigkeit von Angriffen wird es immer anspruchsvoller, kritische Anlagen und Prozesse zu schützen. Als Reaktion darauf wird im Rahmen des Projekts Fast-Blue das kognitive Modell eines Cybersicherheitsteams entwickelt. Das Projekt zielt darauf ab, eine automatisierte Methodik aufzubauen, die in der Lage ist, Ströme von cyber-relevanten Daten zu korrelieren und zu analysieren und tiefgreifende Bedrohungsuntersuchungen und Präventionsmassnahmen zu ermöglichen. Angetrieben wird dieses Modell durch automatisierte Workflows und eine Untersuchungswerkbank, um Reaktions- und Schutzmassnahmen vorzuschlagen und zu empfehlen. Das Blue Team muss die Umgebung erkunden, die Systeme härten, Aktivitäten des Red Teams erkennen und darauf reagieren. Dieses vollautomatische Cyber-Abwehrsystem würde keine menschliche Unterstützung mehr benötigen, um Angriffe in einer komplexen Infrastruktur zu erkennen und zu bekämpfen. Die im Jahr 2021 durchgeführte Arbeit fokussierte sich auf Erkennungsmechanismen und die Korrelation von Betriebssystems-Ereignissen. Die Korrelation mithilfe von Graphen ermöglicht es, diese Ereignisse bis zu ihrem Ursprung zurückzuverfolgen und somit als potenzielle Attacken zu identifizieren. Die Verknüpfung wurde auf Windows ausgeweitet und kann auch Querbewegungen zwischen Linux und Windows erkennen. Die Erkennungen basieren auf vordefinierten Angriffsszenarien, wobei es das Ziel ist, dass das System in Zukunft in der Lage ist, Attacken selbständig zu erkennen.

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 vergangen 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 hier 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 entsprechenden 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.

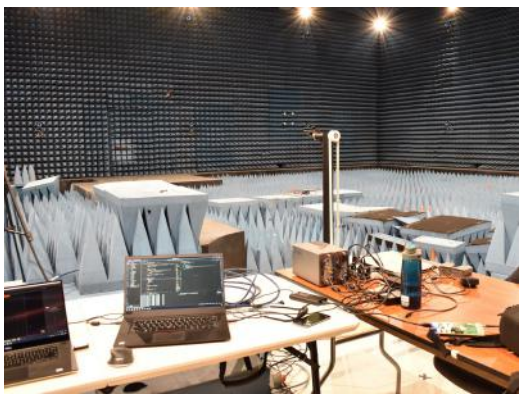
Aufklärungsplattformen für Cyber-Bedrohungen

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 Adaptierung bieten würde. Als Reaktion auf diesen Zielkonflikt entwickeln Forschende des CYD Campus eine Plattform, die technologische Garantien bietet, dass autorisierte Nutzer/innen nur auf die globalen Erkenntnisse (Cyber-Bedrohungsmodelle) zugreifen können, die auf den Daten des gesamten Netzwerks basieren. Jede Institution behält dabei die volle Kontrolle über ihre Datensätze. Ermöglicht wird dies einerseits durch die Entwicklung einer Malware Information Sharing Platform (MISP)-kompatiblen 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 Bedrohungsanalysen und -vorhersagen führt.

Quantensichere Kryptographie

Die voranschreitende Forschung zu Quantencomputern birgt kryptologische Herausforderungen. Bisher eingesetzte digitale Signaturverfahren (Digital Signature Schemes – DSS), sowie asymmetrische Kryptosysteme (Public Key Encryption – PKE) und Schlüsselverkapselungsmechanismen (Key Encapsulation Mechanism – KEM), welche in Bezug auf existierende «Standardcomputer» sicher sind, können mit Quantencomputern gebrochen werden. Daher hat das National Institute of Standards and Technology (NIST) damit begonnen, quantensichere Nachfolger für klassische Public-Key-Verfahren auszuwählen und zu standardisieren. Im Juli 2020 wurde die dritte Bewertungsrunde eingeleitet. Dabei wurden aus den Kandidaten der vorhergehenden Runden sieben Finalisten und acht alternative Kandidaten ausgewählt. In diesem Forschungsprojekt werden die Kandidaten der letzten Evaluationsrunde untersucht, die codebasiert sind (Finalist «Classic McEliece» und Alternate Candidates «BIKE» und «HQC») oder auf multivariaten Polynomen (Finalist «Rainbow» und Alternate Candidate «GemSS») beruhen. Darüber hinaus werden Möglichkeiten zur Erweiterung und Anpassung der vorgeschlagenen Verfahren entwickelt und untersucht.

Hacking Micro Drones



Versuchsaufbau im Labor um Drohnen über GPS Spoofing kontrolliert zu übernehmen

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 Fokus auf der Möglichkeit, die Kontrolle über Mini-UAVs über den GPS-Kanal zu gewinnen. Die GPS-Übernahme konnte im Labor erfolgreich demonstriert werden.

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 und vertrauenswürdige 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 Testbed demonstriert, welche die CYD Campus Standorte in Thun, Lausanne und Zürich verbindet.

Sicherheit von elektrischen Fahrzeugen und Ladeinfrastrukturen

Im Zuge der Umstellung des VBS auf elektrische Fahrzeuge soll die Sicherheit der vorhandenen Ladeinfrastrukturen überprüft werden. Dazu wurden bereits Vorarbeiten geleistet, die aufzeigten, dass für bestimmte Systeme, welche die sogenannte Power Line Communication (PLC) verwenden, der Datenfluss aus der Ferne drahtlos abgehört werden kann. Dies kann verschiedene Auswirkungen auf die Sicherheit und den Datenschutz von Autos und Infrastruktur haben. Während des CYD Campus Car Hackathons in Thun im Oktober 2021 wurde ein aktiver Angriff auf ein Ladesystem entwickelt, bei dem ein unauffälliger, sogenannter Denial-of-Service (DoS)-Angriff den Ladevorgang drahtlos unterbricht und beendet. Die Analyse solcher Angriffe und möglicher Gegenmassnahmen wird im weiteren Verlauf dieses Projekts durchgeführt.

Untersuchung von Sicherheitsschwachstellen bei elektrischen Fahrzeugen und Ladeinfrastrukturen in Thun

Cyber in der Luft- und Raumfahrt

Die Cybersicherheit in der Luft- und Raumfahrt ist seit der Gründung des CYD Campus ein zentrales Forschungsthema. Im Aerospace gibt es viele fundamentale Gemeinsamkeiten, einschließlich im Bereich der Cybersicherheit. So werden viele Legacy-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 grundlegenden Sicherheitsproblemen, da die Inhalte weder verschlüsselt noch authentifiziert werden. Aber auch dort, wo Inhalte verschlüsselt werden, geschieht dies oft nicht mit offenen, sicheren Standards, sondern mit schwachen proprietären Systemen, die dem Kerkhoff'schen Prinzip über sichere Kryptosysteme widersprechen. Der CYD Campus hat dieses Jahr im Rahmen seiner Arbeiten im Avionik-Datenlink ACARS (Aircraft Communication Addressing and Reporting System) verschiedene solcher Verfahren identifiziert, die in einem weiteren Forschungsprojekt nun automatisiert detektiert werden können.

Schutz von unsicheren Avionik-Systemen

Das Forschungsprojekt befasst sich mit der Analyse von Schwachstellen in der Avionik-Hardware und den damit verwendeten drahtlosen Protokollen. Im 2021 wurde hier u.a. ein praktischer Angriff auf FLARM demonstriert, der mit geringem Ressourcenaufwand durchgeführt werden kann. FLARM ist ein in Leichtflugzeugen und Drohnen eingesetztes Kollisionswarngerät, das in der Schweiz entwickelt wurde und weltweite Beachtung und Verbreitung erfuhr. Die Anzeige des FLARMs zeigt umliegende Flugzeuge nach der Priorität der gefährlichsten Annäherung an und unterstützt damit die Luftraumbeobachtung. Darüber hinaus wurden mit Hilfe des Avionik-Labors Analysen von kommerziellen Avionik-Systemen durchgeführt. Auf der theoretischen Seite wurde das Controller-Pilot-Data-Link-Kommunikation (CPDLC)-Protokoll untersucht, wobei Schwachstellen identifiziert und Möglichkeiten zur Verbesserung ermittelt wurden. CPDLC ist eine Methode, mit der Fluglots/innen mit Pilot/innen über ein Datalink-System kommunizieren können.

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 Raspberry-Pi-Geräte nicht über eine fälschungssichere Kennung, so dass sie leicht imitiert werden können. Durch die Betrachtung von Hardwareunterschieden, wie z. B. der Taktdrift, werden Modelle für maschinelles Lernen trainiert, 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 werden Software-Fingerabdrücke erstellt, die das normale Verhalten eines IoT-Geräts modellieren. Modelle des maschinellen Lernens werden trainiert, 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 gemeinsam genutzte Ressource und gleichzeitig für viele 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 tauschten sich im Jahr 2021 mehrfach 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 (Internet of Things, IoT) sowie dem dezentralen maschinellen Lernen.
Die Arbeitsgruppe ist 2020 im Rahmen einer Vereinbarung über die Forschung, Entwicklung, Erprobung und Bewertung entstanden. Diese Vereinbarung wurde im April 2019 zwischen dem US-Verteidigungsministerium (DoD) und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) unterzeichnet.

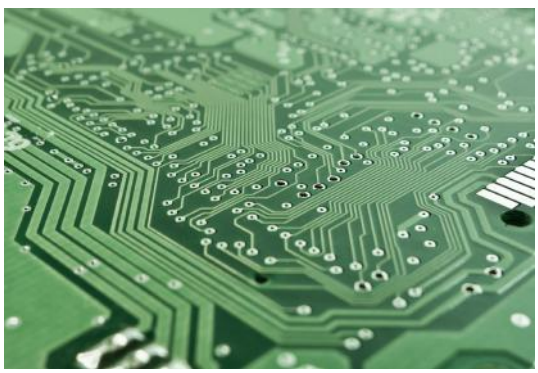
Informationsbeschaffung Cyberspace: Stratosphäre

Um Daten analysieren zu können, muss man sie erst einmal beschaffen. Der Cyberspace ist zwar de facto eine Datenquelle, wurde aber bisher nur als virtuelle Umgebung der Informations- und Kommunikationstechnologien betrachtet. Cyber-Risiken können sich heutzutage jedoch auch auf den Luft- und Weltraum auswirken, etwa auf Flugzeuge und Satelliten. Daher ist es wichtig, den Cyberspace als eine mehrdimensionale 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, Daten von Up- und Downlinks zu sammeln. 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 abfangen und Sender auf der Erde oder im Weltraum orten kann.

Datenschutz bei tragbaren Geräten: Ermittlung von Persönlichkeitsmerkmalen

Vernetzte Uhren machen inzwischen einen grossen Teil des Uhrenmarktes aus. Sie bieten verschiedene Funktionen wie das Zählen von Schritten und Herzschlägen und sind mit Sensoren zur Erfassung von Bewegungen ausgestattet. Obwohl diese Uhren von vielen Besitzenden als nützlich angesehen werden, sind sie sich der potenziellen Datenschutzprobleme nicht bewusst. Die von den Uhren erzeugten Daten werden Drittanbieter-Apps zur Verfügung gestellt, die sie für unterschiedliche Zwecke weiterverwenden können. Im Rahmen dieses Projekts wird die Fähigkeit untersucht, die Persönlichkeitsmerkmale von FitBit-Besitzern zu ermitteln, indem ihre Offenheit, Pflichtbewusstsein, Extraversion, Anpassungsfähigkeit und Neurotizismus ausgewertet wird. Durch das Trainieren von Machine-Learning-Modellen mit den gesammelten Daten dieser Uhren konnte die aktuelle Baseline übertroffen sowie gezeigt werden, dass die Persönlichkeit tatsächlich bestimmt werden kann. Darüber hinaus ermöglichen die Daten auch eine Kategorisierung der Besitzenden nach Geschlecht und Religion, was zu Diskriminierungsproblemen führen könnte.

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 werden 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.

Datenschutz bei tragbaren Geräten: COVID Contact Tracing

Viele Länder haben als Reaktion auf den COVID-19-Ausbruch eine App zur Ermittlung von Kontaktpersonen eingeführt. Diese Apps wurden als Mittel zur Identifizierung von Personen eingesetzt, die möglicherweise mit infizierten Personen in Kontakt standen. Zu diesem Zweck sendet die jeweilige App auf dem Smartphone regelmässig ein Signal über Bluetooth. In diesem Projekt untersuchen CYD Campus Mitarbeitende den Datenschutz einiger Contact Tracing Apps, um beispielsweise herauszufinden, ob es möglich ist, einzelne Nutzende zu identifizieren. Deshalb wurden mehrere Datenerfassungskampagnen in den wichtigsten Schweizer Bahnhöfen organisiert. Durch die Analyse der von den Telefonen gesendeten Identifikatoren konnte gezeigt werden, was die Risiken der Contact Tracing Apps sind.

Erkennung von Fakes in sozialen Medien: Identifizierung von Radikalisierung

Verdächtiges Verhalten in den sozialen Medien wird unter verschiedenen Bezeichnungen wie Fake News, Desinformation, kompromittierte Konten, Identitätstäuschung, Propaganda, Hassreden oder Radikalisierung dargestellt. Alle aufgeführten Verhaltensweisen haben ein gemeinsames Merkmal: Sie spalten die Gesellschaft. Anhand des Anwendungsfalls der Radikalisierung werden in diesem Projekt Zeitpunkte in der Social-Media-Timeline eines Nutzenden identifiziert, die auf eine Änderung der Einstellung in Bezug auf extremistische Ansichten hinweisen. Anhand eines solchen Punktes werden mit Hilfe von mit Daten trainierten Sprachmodellen die Einflüsse modelliert, denen der Nutzende ausgesetzt war und die zu dieser Verhaltensänderung geführt haben könnten. Die Erkennung der einflussreichsten Merkmale im Informationsfluss ermöglicht es, frühzeitige Warnsignale zu geben, wenn eine Radikalisierungsabsicht identifiziert werden kann.

Tweets Verbreitungsbaum

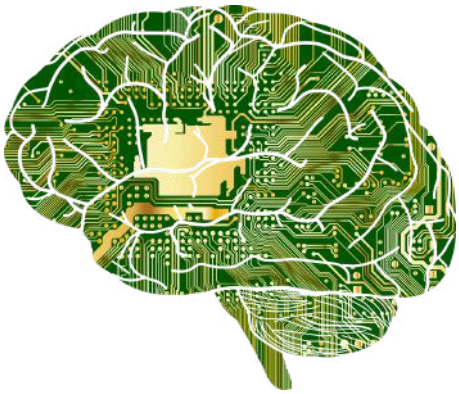
von Fake News | von echten Nachrichten

- 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.

Erkennung von Fakes in sozialen Medien: COVID Fehlinformation

Im Falle einer sich rasch ausbreitenden Pandemie ist es notwendig, schnell relevante Erkenntnisse über die Krankheit zu erhalten. Twitter ist ein beliebtes Medium, um sich in Echtzeit über weltweite Ereignisse zu informieren. Das Netzwerk dient aber auch zur Verbreitung von Fehlinformationen. Die Bildung von Filterblasen, mangelnde Kontrolle und fehlende Überprüfung oder Verifizierung von Informationen sind zentrale Probleme der sozialen Medien. Im Zeitalter der Infodemie ist es von entscheidender Bedeutung, die Reaktionen der Menschen auf Massnahmen des öffentlichen Gesundheitswesens zu erfassen und ihre Bedenken zu verstehen. Dieses Projekt konzentriert sich auf die Identifizierung von Beiträgen in sozialen Medien, die mit einer bestimmten Fehlannahme in Zusammenhang stehen (Identifizierung der Zugehörigkeit), indem klassische Machine-Learning-Modelle wie logistische Regression oder Support Vector Machine (SVM) sowie semantische Textähnlichkeit verwendet werden. Die Beiträge, die sich auf eine Fehlannahme beziehen, werden dann im Hinblick auf die darin enthaltenen Fehlinformationen klassifiziert. Ausserdem kann anhand der Fehlannahme als Diskussionsthema und der Nutzerkommentare herausgefunden, ob der Autor bzw. die Autorin für oder gegen das Thema ist (Erkennung von Haltungen).

Maschinelles Übersetzen: Identifizierung von Dialekten



Die Identifizierung von Sprachdialekten ist aus Sicht der Linguistik und der algorithmischen Verarbeitung von natürlicher Sprache eine sehr anspruchsvolle Aufgabe. Statt sich nur auf die Klassifizierung von Sprachen oder Dialekten zu konzentrieren, wird im Rahmen dieses Forschungsprojektes versucht, die Sprache zu erkennen, bevor die gesamte Äusserung oder der gesamte Text als Input gegeben wird. Mit anderen Worten: Der Schwerpunkt liegt auf einer zuverlässigen Aussage über die Klassifizierung zu einem früheren Zeitpunkt. Das Ziel des Projekts ist es, Kriterien für die Verkürzung der Eingabedaten zu finden, die die Vorhersage des Dialekts in Abhängigkeit von der Eingabeprobe und dem Modell bestimmen und erleichtern. Im Idealfall sollte die Gesamtvorhersagegenauigkeit des vorgeschlagenen Ansatzes die ursprüngliche Leistung übertreffen oder zumindest erreichen. In diesem Projekt befassen sich der CYD Campus mit der herausfordernden Aufgabe der Dialektklassifikation und fokussieren sich dabei auf zwei Sprachen: Schweizerdeutsch und Indoarisch. Die experimentelle Analyse zeigt, dass es in den meisten Fällen einen früheren Zeitpunkt gibt, zu dem die Vorhersage durchgeführt werden kann. Dies erfolgt anhand der Eingabekürzungskriterien, die auf kalibrierten Wahrscheinlichkeiten und Label-Konsistenzen aufbauen.

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 zu Bildverarbeitung wurden Angriffe in der Literatur zu NLP und neuronalen maschinellen Übersetzungssystemen (NMT) bisher nur wenig untersucht. Da NMT-Systeme in hochsensiblen Anwendungen eingesetzt werden, ist die Erforschung gegnerischer Angriffe, insbesondere von UAPs, von entscheidender Bedeutung für das NMT-Modell. Durch die Entwicklung eines Algorithmus zur Erzeugung 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 befasst sich mit universellen Angriffen 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 zielgerichteter sind. Ein Black-Box-Angriff simuliert realitätsnahe den Angriff eines typischen Internet-Hackers. White-Box-Angriffe bezeichnet einen Angriff mit bestimmten Detailkenntnissen über die innere Funktionsweise des Systems. White-Box-Angriffe decken meist mehr Schwachstellen des NMT-Modells auf, da sie auf die Modellparameter zugreifen können.

Maschinelles Übersetzen: Familien von Sprachen und Dialekten

Die maschinelle Übersetzung hat seit der Einführung von neuronalen Netzwerkmodellen erhebliche Fortschritte gemacht, und sogenannte Transformers sind derzeit Standard für Sprachpaare mit vielen parallelen Übersetzungsdaten, sogenannte ressourcenreiche Sprachpaare. Für Sprachpaare mit schwachen Ressourcen oder im Falle gänzlich fehlender paralleler Übersetzungsdaten ist zusätzlicher Aufwand erforderlich. In diesem Projekt liegt das Augenmerk auf Lösungen für den Umgang mit einer ressourcenarmen Sprache, wenn ressourcenreichere Sprachen aus derselben Familie verfügbar sind. Für das Training der anfänglichen Übersetzungsmodelle wurde Transfer-Learning unter Verwendung verschiedener ressourcenreiche Sprachen genutzt, die von den Forschenden für die gegebene ressourcenarme Sprache feinabgestimmt wurde. Darüber hinaus wird die Rückübersetzung als Technik zur Erweiterung der parallelen Übersetzungsdaten verwendet, wenn nur einsprachige Quellen zur Verfügung stehen. Alle diese Techniken haben die Qualität der Übersetzung in ressourcenarmen Umgebungen nachweislich verbessert.

Datenwissenschaftliche Methoden zur Technologie- und Marktbeobachtung

Um die Technologie- und Marktentwicklung verfolgen zu können, muss man in der Lage sein, Technologien zu erkennen, sie auseinanderzuhalten und deren Beziehungen untereinander zu verstehen. Unter Verwendung der technologiebezogenen Konzepte innerhalb des Wikipedia-Graphen wird vom CYD Campus eine Methode zur Identifizierung der realen Position eines neuen Konzepts innerhalb einer bestehenden Taxonomie vorgeschlagen, die sich auf semantische und relevante Ähnlichkeiten stützt. Darüber hinaus wird ein Rahmen für die Erkennung des technologiebezogenen Konzepts in unstrukturiertem Text aufgebaut, indem der Ansatz des Concept Tagging verwendet wird, der nicht die Extraktion der Oberflächenform aus dem rohen Text umfasst. Auf diese Weise wird es möglich, sich auf den semantischen Inhalt eines Dokuments anstatt auf seine Textform zu konzentrieren und Konzepte zu erkennen, die nicht explizit im Text erwähnt werden.

Frühwarnsignale in OSINT: Antizipation von Konflikten

Die Antizipation von Konflikten ist eine zentrale Aufgabe für die Regierungen und Streitkräfte. Das Wissen um potenzielle Konflikte oder Instabilitäten kann die geopolitische Strategie weitgehend beeinflussen und eine bessere Vorbereitung ermöglichen. In jüngster Zeit haben mehrere offene Quellen damit begonnen, Daten zu sammeln, die für die Konfliktvorhersage von grosser 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. Mit Hilfe statistischer Methoden können Mitarbeitende des CYD Campus sogenannte Tipping Points identifizieren und vorhersagen, die einen Richtungswechsel anzeigen. Richtungswechsel können ein Putsch oder eine andere grössere politische Veränderung sein. Durch die Analyse von Daten aus Indien und Irak waren sie in der Lage, die Dynamik von Instabilitäten in diesen Ländern zu modellieren und somit die entsprechenden Frühwarnsignale zu identifizieren.

Kausal-Analysen

In der Statistik werden Korrelationen häufig als Mittel verwendet, um einen Zusammenhang zwischen zwei Variablen aufzuzeigen. Korrelationen geben jedoch keine Auskunft darüber, ob ein kausaler Zusammenhang zwischen den beiden Variablen besteht oder nicht. Der Zweck der Kausalanalyse besteht darin, die Grundursache eines Problems zu finden, anstatt nur die Symptome zu untersuchen. Diese Technik hilft dabei, die Fakten aufzudecken, die zu einer bestimmten Situation führen. In den letzten Jahren wurden viele fortschrittliche Ansätze und Methoden für den Kausalschluss entwickelt, insbesondere in der Statistik. Das Ziel dieses Forschungsprojekts ist es, einen Überblick über moderne Methoden zur Interpretation, Identifizierung und Schätzung von Kausalwirkungen von Beobachtungsdaten zu geben. Die Kausalität könnte beispielsweise bei der Konfliktbeobachtung und -vorhersage angewandt werden, wo solche Methoden Aufschluss über den Grund für eine Veränderung der geopolitischen Stabilität geben könnten.

5 Kunden und Aufwandsverteilung

Das Cyber Dispositiv des Bundes ist in drei Bereiche eingeteilt: Cybersicherheit (EFD), Cyberdefence (VBS) und Cyberstrafverfolgung (EJPD). Der CYD Campus erbringt primär Leistungen für den Bereich Cyberdefence. 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 2021 Leistungen zu Gunsten der Beschaffung, Verteidigung und Verwaltung.

Im Detail wurden Aufträge für nachfolgende Organisationen geleistet:

- armasuisse – Kompetenzbereich Führung und Aufklärung
- Armeestab
- Führungsunterstützungsbasis der Armee
  - Cybersicherheitsorganisationen
  - Verteidigung Kommando Operationen
- Nachrichtendienst des Bundes
- Eidgenössisches Finanz Departement – Nationales Zentrum für Cybersicherheit NCSC
- Bundesamt für Polizei fedpol

Auftragsleistungen	Verteilung 2021
Sicherheitsanalysen, Pentesting, Sicherheits-Beratung	29 %
Sicherheitsanalysen & Pentesting	16 %
Sicherheitskonzepte & Beratung	13 %
Vulnerability Research	2 %
Vulnerability Research	2 %
Beratung, Technologie Transformationen	21 %
Beratungsunterstützung Data Science	3 %
Technologie Transformation	18 %
Demonstratoren	29 %
Aufbau Technologie-Demonstratoren	5 %
Aufbau Innovations-Demonstratoren	24 %
Erstellung & Mitarbeit in Studien	19 %
Erstellen von Fähigkeitsstudien	2 %
Erstellen von Grundlagenstudien	2 %
Mitarbeit Grundlagenstudien	11 %
Erstellen von Technologiestudien	4 %

Tabelle 1: CYD Campus Auftragsverteilung 2021

Die Gesamtleistung des CYD Campus aufgeteilt nach Bereichen ist in Abbildung 1 dargestellt. Dabei lagen die primären Kernleistungen im Bereich der Forschung, der Innovationsbeträge und der Beschaffungsunterstützung. Eine detailliertere Auflistung in Tabelle 1 zeigt die Verteilung der Aufträge, welche im Jahr 2021 bearbeitet wurden.

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

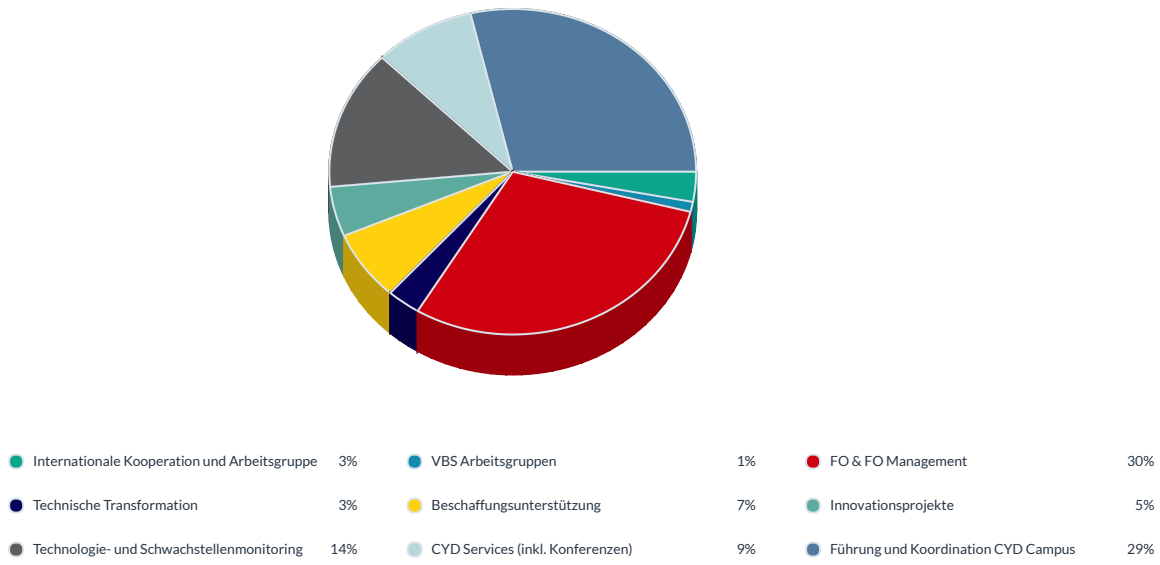


Abbildung 1: CYD Campus Gesamtleistung 2021

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.

Im 2021 wurden Innovationsrapporte für folgende Organisationen durchgeführt:

- Führungsunterstützungsbasis FUB
- Bundesamt für Polizei fedpol
- Nachrichtendienst des Bundes – MELANI

Die Innovationsrapporte wurden mehrheitlich in einem ganztägigen Workshop vor Ort in Thun durchgeführt. Aufgrund der geltenden COVID-19 Restriktionen, musste auf die vollständige Anwesenheit aller Teilnehmer und Teilnehmerinnen verzichtet werden, stattdessen wurden die Veranstaltungen unter Einhaltung der Informationssicherheit hybrid – mit Unterstützung des Videoconferencing – durchgeführt.

6.1 Resultate der Innovationsprojekte

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

Anwendung künstlicher Intelligenz auf aktuelle Problemstellungen

Systeme zur Erkennung von Netzwerkeinbrüchen (Network Intrusion Detection-NIDS) sind wichtige Komponenten moderner sicherer Netzwerke, die dazu beitragen, Anzeichen von Cyberangriffen in einem Netzwerk zu erkennen. Solche Angriffe werden zunehmend komplexer und zielen auf die wachsende Anzahl verbundener Geräte ab, darunter auch Objekte des Internets der Dinge (IoT). Die heutigen IoT-Systeme generieren bereits einen Grossteil des Internetverkehrs, aber die IT-Sicherheit der Geräte ist nach wie vor schwach, was zu einer hohen Zahl erfolgreicher Angriffe führt. Die Einführung innovativer Systeme zur Erkennung von Netzwerkangriffen soll durch neue Techniken des maschinellen Lernens (ML) verbessert werden. Im Innovationsprojekt wurden auf verschiedene IoT-Netzwerkdatensätzen die Leistung neuer ML-Modelle für die NIDS untersucht sowie neue Techniken für die Netzwerkmerkmalsextraktoren im Einsatz verifiziert.

Einführung von Methoden um die Privatsphäre zu schützen

In diesem Projekt wurde untersucht, wie Protokolle zur Wahrung der Privatsphäre wie Private Set Intersection (PSI) oder Private Membership Test (PMT) genutzt werden können, um unrechtmässige Anmeldungen von Remote eingeloggten Mitarbeitenden zu verhindern. Dabei wurden verschiedene kryptografische Primitiven, wie homomorphe Verschlüsselung (HE), oblivious pseudorandom functions (OPRF) und garbled Bloom filters (GBF) verwendet. Die Ergebnisse zeigen, dass die Berechnungen des OPRF PSI-Protokolls bei 4'000 Mitarbeitenden weniger als 200 ms benötigen, während die Datenübertragungskosten unter 1 MB liegen. Bei Verwendung des OPRF-Ansatzes für PMT dauern die Berechnungen 14 ms, und das Protokoll erfordert von den Parteien die Übermittlung von weniger als 20kB.

Wissenstransfer im Bereich Data Science

Der Wissenstransfer aus der akademischen Welt an die Kunden des CYD Campus erfolgt auf mehreren Ebenen. Mit Lehrgängen und Kursen im Bereich Datenwissenschaften vermitteln Mitarbeitende Grundlagen aus Statistik und Mathematik für verschiedene Organisationen des VBS. Die transferierten Lerninhalte sind auf die jeweiligen Fach-Domänen der Kunden angepasst und sind zugeschnitten auf aktuelle Analysen.

Exploratives Arbeiten

Neben wissenschaftlicher Expertise werden auch technische Innovationen an die CYD Campus Kunden weitergereicht. Ein Beispiel für diesen technologischen Wissenstransfer ist die Vermittlung von Know-how zur Verwaltung und Pflege von Daten in sogenannten Data-Lake-Architekturen.

Begleitung bei der Einführung von Datenstrukturen und Verarbeitung grosser Datenmengen, Big Data and Data Lakes

Big Data hat in den vergangenen Jahren die Entwicklung vielfältiger Technologien vorangetrieben. Beispiele für solche Big-Data-Technologien sind neue Speichertechnologien für grosse Datenmengen und verschiedenste Datenformate (z. B. strukturierte und unstrukturierte Datenformate), die Verarbeitung von Datenströmen in Echtzeit oder das Rechnen in verteilten Systemen. Der CYD Campus berät und unterstützt Kunden aus dem VBS beim Aufbau von Systemen mit Data-Lake-Architekturen, die Big-Data-Technologien prominent einsetzen.
Ein wesentlicher Teil des CYD Campus Know-hows stammt aus dem Aufbau des Data Science Lab, einer Plattform, welche eigens für die Speicherung und Verarbeitung von Big Data entwickelt und betrieben wird.

Einführung einer neuartigen Plattform für die Cyber-Bedrohungs-Lageverfolgung inklusive Datenaustausch

Das Verständnis von und der Schutz vor Cyber-Bedrohungen wird immer komplexer, da sich die Angriffstaktiken, -techniken und -verfahren rasch weiterentwickeln. Das Ziel des Projekts Cyberbedrohung-Lageverfolgung (CBL-) ist die Entwicklung eines Proof-of-Concept für eine Threat Intelligence Plattform (TIP). Die entwickelte Plattform nutzt bestehende Open-Source-Elemente wie MISP, OpenCTI und TheHive, wobei jedes Tool eine besondere Funktion hat.
Die Plattform wurde ausgiebig getestet und mit spezifischen Funktionen wie der Dokumentenanalyse (Parsen) verbessert. Darüber hinaus wurden die Architektur und die entwickelte Einrichtung dokumentiert. Verschiedene mögliche Ansätze zur Lösung des Problems, wie beispielsweise andere verfügbare Tools, zukünftige Verfügbarkeit und Flexibilität wurden ebenfalls berücksichtigt. Ausserdem wurde im Rahmen der Studie eine ideale Endarchitektur beschrieben. Ziel ist es, den bestmöglichen produktiven Aufbau unter Berücksichtigung von Kosten, Risiken und langfristigem Betrieb vorzustellen.

Einführung einer Plattform für die Offline-Maschinelle Übersetzung für taktisch operative Einsätze

Im Projekt wurde nachgewiesen, dass es im Falle von allgemeinen Texten möglich ist, Modelle zu trainieren, die eine umfassende Übersetzung unabhängig von der Ausgangs- oder Zielsprache liefern. Allerdings hat sich gezeigt, dass die für das Training verwendeten Daten einen erheblichen Einfluss auf die Qualität der Übersetzung haben können. Vielfältige und aus unterschiedlichen Quellen stammende Daten ermöglichen eine hohe Zuverlässigkeit des erlernten Sprach- und Übersetzungsmodells gegenüber Sprachvariationen. Darüber hinaus können die Modelle, die für eine allgemeine Übersetzung trainiert wurden, an internen Datenbeständen optimiert werden, um spezifischere Anwendungsfälle abzudecken. Diese Datenkorpora, die für das interne Training herangezogen werden, können auch aus klassifizierten Quellen stammen.

Design einer Architektur für sichere mobile Betriebssysteme

Bei Open-Source- oder kommerziellen Projekten mangelt es an einer umfassenden Sicherheitsarchitektur für ein mobiles Betriebssystem. Die Sicherheitsarchitektur sollte nämlich Risiken in Kompartimenten einschliessen um vertrauliche Daten und die Kommunikation vor Angriffen oder unbefugtem Zugriff zu schützen. Darüber hinaus sollte es Benutzern und Benutzerinnen möglich sein, auf einem Gerät unsichere Anwendungen neben vertrauenswürdigen Anwendungen auszuführen und gleichzeitig mit vertraulichen Informationen zu arbeiten. Mit dem Ziel, eine solche Sicherheitsarchitektur aufzubauen, wurden zwei Architekturen entwickelt. Das zugrundeliegende System basiert auf einem Hypervisor-Konzept für die Ausführung mehrerer Kernel und Android-Instanzen. Die Treiber sind ebenfalls virtualisiert, wobei die Kernel keinen direkten Zugriff auf die Hardware haben.

Automatisierter Austausch von Sicherheitsschwachstellen

Der CYD Campus arbeitet erstmalig im Jahr 2021 mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) im Bereich der Innovation zusammen. Die Zusammenarbeit beinhaltet die Bereitstellung von Open-Source Softwareanwendungen, die es ermöglichen, Sicherheitsempfehlungen in einem für Maschinen verwertbaren Format zu erstellen und zu verwalten. Dadurch können Informationen zu Sicherheitsschwachstellen einfacher ausgetauscht werden, was die Cybersicherheit verbessert.

6.2 Cyber Startup Challenges

2020: Aufklärung von Cyberbedrohungen

Startups haben oft innovative und bahnbrechende Ideen und können Technologien anbieten, die einen technologischen Vorteil gegenüber Angreifern bieten. Aus diesem Grund hat der CYD Campus die Cyber Startup Challenge im Jahr 2020 ins Leben gerufen.

Das Startup-Unternehmen CounterCraft konnte 2020 die Jury von seiner neuartigen Lösung im Bereich der Aufklärung von Cyber-Bedrohungen überzeugen. Die Firma setzte im Jahr 2021 ein massgeschneidertes Proof-of-Concept um.

Das Täuschungsszenario beschreibt ein kleines industrielles Steuerungsnetzwerk mit einer geringen Anzahl aktiver Programmable Logic Controllers (PLC). Dabei kann es sich um eine kleine abgelegene Anlage handeln, wie z. B. ein Umspannwerk oder eine Wasserpumpstation. Das Netzwerk wird über eine Mensch-Maschine-Schnittstelle (Human-Machine-Interface - HMI) gesteuert, wobei die Steuerungsdaten in einer vernetzten Datenbank gespeichert werden. Die Anlage wird von einem Kontrollzentrum aus gesteuert.

Der Proof-of-Concept wurde 2021 aus der Sicht des Angreifers und des Verteidigers mit den operativen Einheiten der Armee getestet. Es war möglich, die generierten Taktiken, Techniken und Verfahren (tactics, techniques, and procedures- TTP) mit der Reaktion der Plattform zu vergleichen.

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

Die Cyber Startup Challenge 2021 zielte darauf ab, unter dem Motto «Stärken Sie Ihr Information Sharing and Analysis Center (ISAC)» die Startup-Technologielandschaft zu entdecken und suchte nach innovativen Lösungen im Bereich der Cyber-Bedrohungsaufklärung mit Schwerpunkt auf dem Schutz kritischer Infrastrukturen.

Insgesamt 38 Startups aus Europa, den USA und Asien sind dem Aufruf gefolgt. Die aus Cyber-Experten des VBS und der armasuisse W + T gebildete Jury wählte die drei Finalisten Decentriq, Constella Intelligence und Pandora Intelligence aus, welche im Rahmen der CYD Campus Konferenz am 28. September 2021 einen Pitch hielten. Mit seiner innovativen Software-as-a-Service (SaaS)-Plattform, die «Data Clean Rooms» für Unternehmen anbietet, überzeugte das Zürcher Startup Decentriq die Jury. «Data Clean Rooms» sind sichere, geschützte Umgebungen, in denen personenbezogene Daten bereinigt und verarbeitet werden, damit sie für vielfältige Datenanalysezwecke genutzt werden können. Die Plattform ermöglicht es dementsprechend internen und externen Akteuren kritischer Infrastrukturen, Cyber-Daten sicher zu teilen und aggregierte und anonyme Erkenntnisse zu gewinnen. Auf diese Weise wird die Cybersicherheit verbessert, ohne den Datenschutz zu gefährden.

Decentriq wird im Jahr 2022 gemeinsam mit dem CYD Campus an der Integration eines Proof-of-Concept seiner Technologie in eine reale VBS Umgebung arbeiten.

7 Sicherheitsanalysen, Pentesting und Sicherheitsberatung

Im Jahr 2021 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, Pentestings 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.*

8 Demonstratoren

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.)

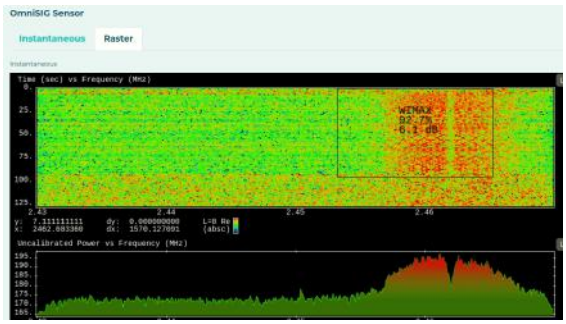
Demonstrator gemischte Realität für die Ausbildungssimulation

Die Verwendung der Technologie birgt gewisse Risiken, 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 Doktrine, 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.

Demonstrator Signal Klassifikation



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

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 Elektromagnetisches-Spektrum klassifizieren zu können. Heute gibt es mehrere Forschungsansätze, die Deep-Learning-Techniken zur Klassifizierung von Spektrumsdaten verwenden. Es wurde von CYD Mitarbeitenden ein vielversprechendes US-amerikanisches Startup identifiziert, das unter Verwendung von Magnituden- und Phasensignaldaten mittels Deep-Learning-Methoden, Signale klassifizieren kann. Die Software bietet eine einfache Benutzeroberfläche sowie fortschrittliche Optionen und basiert auf modernster und sich ständig weiterentwickelnder Technologie. Sie kann ebenfalls mit kostengünstiger, handelsüblicher Computerhardware betrieben werden. Die Sensoren, welche die Inferenz ausführen, benötigen nur eine begrenzte Rechenleistung und können auf einer kleinen, eingebetteten Plattform mit einer grafischen Verarbeitungseinheit laufen. Dieser Demonstrator zeigt die Bedeutung und das Potenzial dieser Technologie, die erst am Anfang steht.

Demonstrator GPS Drone Spoofing

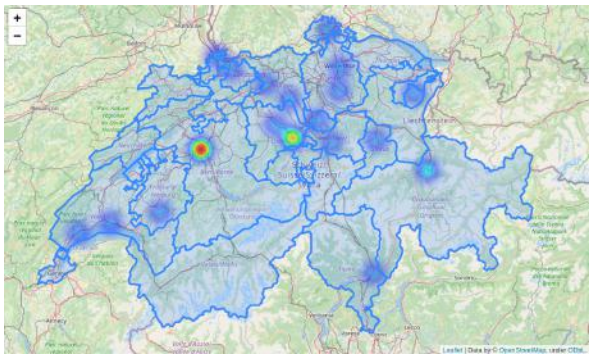
GPS-Spoofing ist ein Angriff, bei dem ein Funksender in der Nähe des Ziels verwendet wird, um ein legitimes GPS-Signal vorzutäuschen. Da Drohnen zur Bestimmung ihres Standorts auf GPS-Signale angewiesen sind, sind auch sie von solchen Angriffen betroffen. Es konnte bereits gezeigt werden, wie eine Drohne den gefälschten Standort an den Piloten bzw. an die Pilotin zurückmeldet. Die Untersuchung konzentriert sich nun darauf, wie eine Drohne mithilfe dieses Angriffs 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 Angreifer bzw. die Angreiferin die volle Kontrolle über die Bewegung der Drohne hat. GPS-Spoofing könnte demnach von einem Angreifer / einer Angreiferin dazu genutzt werden, kommerzielle Drohnen von Privatpersonen zu kapern, um unbemerkt böswillige Handlungen durchzuführen, wie z. B. die Drohne gegen ein bestimmtes Ziel abstürzen zu lassen oder die Drohne zu stehlen, um an persönliche Daten zu gelangen.

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.

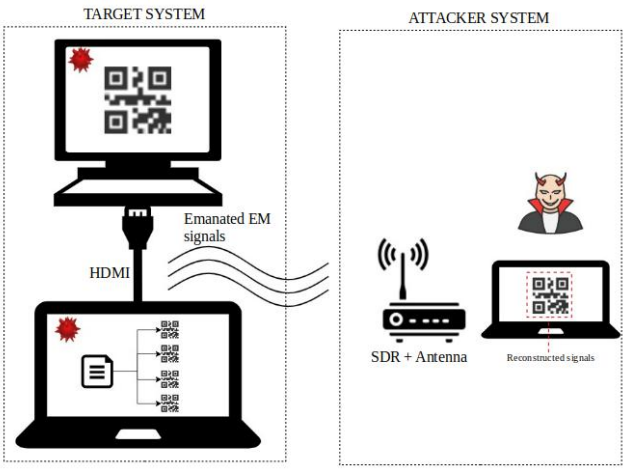
Evaluation der Augmented Reality für die bessere Verteidigung gegen Phishing anhand des Demonstrators

Demonstrator Social Media-Lagebild



Heatmap der Anzahl Tweets, welche in Zusammenhang mit der COVID19-Pandemie Ortschaften referenzieren

Kommunikation im 21. Jahrhundert wird durch die drei Technologien Internet, Mobilgeräte und Social Media geprägt. Es ist daher nicht überraschend, dass diese Infrastruktur von bestimmten Akteuren, wie z.B. ausländischen Nachrichtendiensten für die gezielte Verbreitung von Falschinformationen benutzt werden. Im Aufbau befindet sich daher ein Demonstrator für die automatisierte Analyse von Inhalten aus Twitter-Konten. Dabei werden über die offizielle Twitter API sämtliche vom Zielkonto verfassten Beiträge heruntergeladen. Anschliessend kann eine Analyse von darin enthaltenen Text-, Bild- und Videodaten durchgeführt werden. Durch den Einsatz von regulären Ausdrücken können Datums- und Zeitangaben, verbunden mit den genannten Ortschaften, aus den Tweets extrahiert werden. Damit können Inhalte in einen zeitlichen und örtlichen Kontext gesetzt werden, was die Generierung eines Lagebildes erlaubt. Der textuelle Inhalt der Tweets wird dann weiter auf Wortfrequenzen und die Frequenzen von genannten Ortschaften untersucht. Damit kann ein erster Eindruck über dominante Narrative eines Twitter-Kontos und dessen Bezug zu örtlich und zeitlich definierten Ereignissen gewonnen werden. Weiter werden Bilddaten mittels moderner Deep Learning-Methoden (Convolutional Neural Networks) analysiert, wodurch Bild-mit-Text Memes von anderen Bilddaten unterschieden werden können. Bild-mit-Text Memes sind ein effektives Instrument zur Verbreitung von Ideen und Kontrolle von Onlinenarrativen, was sie als Mittel für Desinformationskampagnen attraktiv macht.



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

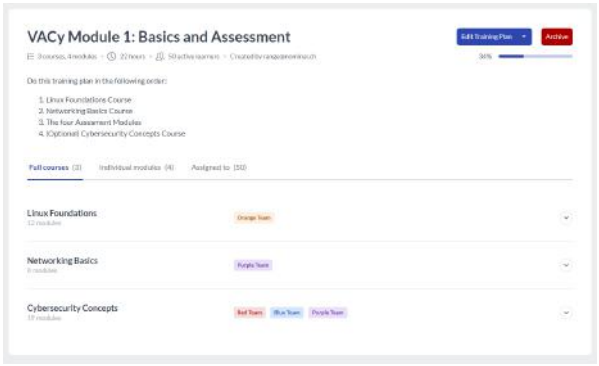
Demonstrator TEMPEST Datenabfluss

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.

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.



Softwareumgebung des Demonstrators für die vordienstliche Cyber-Ausbildung der Armee

Die fünfzig jungen Menschen, die Teil des ersten Pilotprojekts der Vordienstlichen Ausbildung Cyber sind (Beginn im November 2021), konnten die innovative Software eines der ausgesuchten Startups nutzen.

Demonstration der Ausnutzung von Sicherheitslücken von Elektrofahrzeugen um die Kommunikation abzuhören

Demonstrator Car Hacking

Während des Car Hackathons in Thun, welcher im Kapitel Highlights beschrieben wurde, haben die Teilnehmenden mehrere Demonstrationen von Angriffen entwickelt, die gegen Autos durchgeführt werden können. In einem Fall konnte durch den Anschluss einer Schnittstelle an den CAN-Bus (Kommunikationsschnittstelle) eines Elektroautos unbeabsichtigtes Verhalten wie blinkende Lichter, das Öffnen und Schliessen der Fenster ausgelöst oder die Servolenkung beeinflusst werden. In Anbetracht des starken Trends zu Elektromobilität konnte ebenfalls aufgezeigt werden, dass der Ladevorgang von Elektrofahrzeugen aus der Ferne gestört und unterbrochen werden kann.

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 2021 erfolgreich in einer Live-Fire-Cyber-Übung der Schweizer Armee getestet. Sie wird nächstes Jahr weiterentwickelt, indem sie an echte speicherprogrammierbare Steuerungen (SPS) angeschlossen und in eine realistische SCADA-Umgebung (Supervisory Control and Data Acquisition) integriert wird, die für Forschung und Übungen genutzt werden kann.

Visualisierung von Cyberangriffen auf einem Militärflugplatz

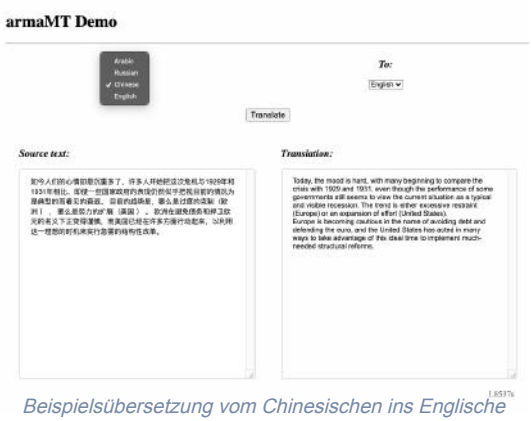
Demonstrator Hybrid Cyber Range

Cyber Ranges sind Infrastrukturen, die aus mehreren Computern und Netzwerken bestehen und für die Forschung oder Übungen genutzt werden können. In der Regel ist der größte Teil der Infrastruktur virtualisiert, d.h. es gibt keine echten Workstations, sondern diese laufen auf Servern in einem Rechenzentrum. Reale Netzwerke bestehen jedoch nicht nur aus Servern und Workstations, sondern umfassen auch physische Komponenten, die zur Überwachung und Steuerung technischer Prozesse eingesetzt werden. Es wurden Komponenten getestet, die es den CYD Campus Mitarbeitenden ermöglicht haben, echte industrielle Überwachungssysteme (SCADA) in einen Cyber-Range zu integrieren. Diese wurden erfolgreich in Übungen und anderen Versuchen eingesetzt.

Industrielles Steuerungssystem mit Visualisierungsanzeige (oben) und mobilem Cyberbereich (unten)

Demonstrator Offline-Übersetzung

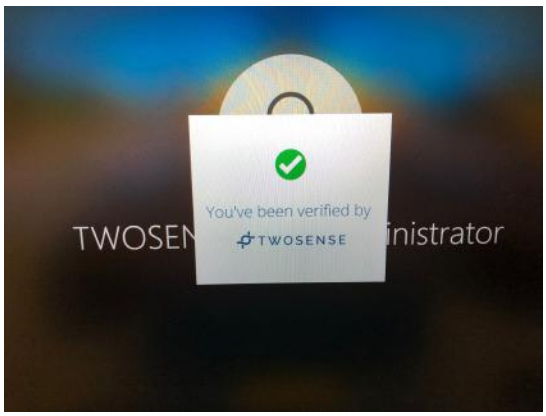
Der Austausch von Informationen in verschiedenen Sprachen ist zu einer Notwendigkeit geworden. Maschinelle Übersetzungswerkzeuge haben sich ebenfalls zu einem festen Bestandteil unseres Berufsalltags entwickelt. Allerdings bergen diese Online-Übersetzungs-Tools auch erhebliche Risiken für die Privatsphäre, insbesondere bei sensiblen Informationen. Daher ist es dringend erforderlich, dass die automatische Übersetzung genutzt werden kann, ohne dass die Informationen der Aussenwelt preisgegeben 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

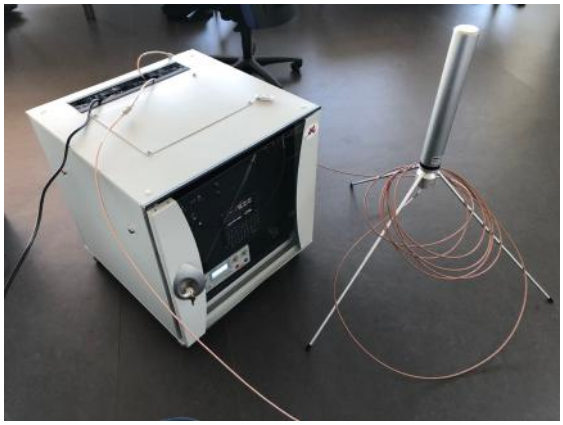
Passwortabfragen oder einmalige biometrische Prüfungen wie Fingerabdruck- oder Iris-Sensoren gewähren Nutzer/innen den Zugang nach erfolgreicher Authentifizierung und prüfen nicht regelmässig auf böswilliges Verhalten oder einen Wechsel des Nutzers. Diese Methoden ermöglichen z. B. sogenannte Mittagsangriffe, 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

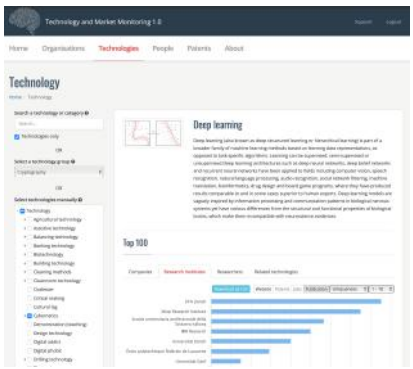
In den 2010er Jahren haben Wissenschaftler/innen und Hacker/innen zahlreiche Schwachstellen in den von Flugzeugen und Fluglotsen bzw. Fluglotsinnen genutzten drahtlosen Technologien nachgewiesen. Bislang wurde solches Spoofing mit geringen Mitteln wie Software-Defined Radios ausschliesslich am Computer mit simulierter Hard- und Software demonstriert.
Dieser Demonstrator verwendet eine realitätsnahe Abbildung realistischer 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 Technologie- und Marktmonitoring

Der Demonstrator bietet den Nutzenden auf der Basis von Open-Source-Daten eine Liste relevanter Unternehmen in der Schweiz, die dem gesuchten Technologie-Cluster entsprechen. Zudem sind im Demonstrator Informationen über offene Stellen, Anzahl Patente und Anzahl Publikationen verfügbar sowie Unternehmen mit ihren Informationen wie angebotene Produkte, Dienstleistungen und Technologien auffindbar. Dadurch werden Unternehmen sowohl als potentielle (Unter-) Lieferanten als auch als mögliche Offsetpartner bei Beschaffungen sichtbar.



Ausschnitt TMM Tool zu Deep-Learning-Technologien

9 Technologie- und Marktmonitoring

Der CYD Campus wirkt als Antizipationsplattform von Cyber-Entwicklungen und Trends. Mit diesem Aufgabenbereich will das VBS in der Lage sein, technische Entwicklungen zu entdecken sowie ihre Chancen und Risiken frühzeitig zu verstehen. Um die neusten Trends auf dem Markt aufzuspüren, setzt der CYD Campus auf ein quantitatives und qualitatives Technologie- und Marktmonitoring (TMM). Auf der einen Seite werden unter Verwendung der TMM-Plattform aufkommende Cyber-Technologien und Clusters mittels quantitativer Auswertung von öffentlich zugänglichen Daten entdeckt, auf der anderen Seite werden vielversprechende Startups mittels einem qualitativen Scouting, einem internationalen Technologiebeobachtungsprogramm, aufgespürt.

Cybersicherheitstechnologien

Um relevante Cybersicherheitstechnologien auf dem Markt zu entdecken, ist es unabdingbar, Zugang zu Datenquellen mit aktuellen und zuverlässigen Informationen über die auf dem Markt angebotenen Technologien zu haben. Der CYD Campus verwendet dazu die eigene Plattform Technology and Market Monitoring (TMM) sowie weitere Quellen.
Dieses Jahr wurde von Forschenden des CYD Campus ein Bericht verfasst, der einen Überblick über Trends und Aktivitäten in der Schweiz und im Ausland im Bereich der Cybersicherheitstechnologien gibt. Die Erkenntnisse wurden am 2. Dezember 2021 am CYD Campus EPFL Standort in Lausanne vorgestellt.

Darstellung Schweizerisches Cybersicherheitsökosystem

Eine Studie im Rahmen von TMM wurde in Zusammenarbeit mit der MILAK an der ETH Zürich durchgeführt. Dabei ging es darum, die öffentlichen, privaten und akademischen Ökosysteme im Zusammenhang mit dem Cyber-Bereich in der Schweiz zu modellieren. Es wurden mehrere Netzwerkkarten und eine geografische Darstellung der wichtigsten Akteure entwickelt. Ein Teil dieses Projekts wurde auf der NCSC-Website veröffentlicht, indem eine Liste der in der Schweiz verfügbaren akademischen Ausbildungen im Bereich der Cybersicherheit zur Verfügung gestellt wurde.
Link zur Swiss Cyber Map:

Scouting

Durch das qualitative Scouting spürt der CYD Campus interessante Startups und Partner im In- und Ausland auf, die den Anforderungen des VBS gerecht werden. Das Programm richtet sich hauptsächlich an aufstrebende Unternehmen, gelegentlich aber auch an etablierte Unternehmen, die innovative Produkte anbieten können. Ein Netzwerk mit verschiedenen Partnern wie Swissnex, Swisscom, PlugandPlay, verschiedenen Startup Accelerators und Venture Capital Firmen sowie mit Botschaften und anderen institutionellen Akteuren wurde bereits etabliert, um wichtige Märkte systematisch auf neue Trends im Bereich Cyber-Technologien zu scannen. In geografischer Hinsicht liegt der Schwerpunkt auf Regionen mit leistungsstarken Startups.

Darunter sind:

- Schweiz: Trust Valley, Crypto Valley und Inno-Raum Zürich.
- USA: Ballungszentren um Silicon Valley, Washington DC, Boston, New York, Seattle und Austin.
- Israel: Armeeeinheit bringt 8200 Spitzentalente für Cybersicherheit hervor.
- Vereinigtes Königreich: Renommierte Universitäten und ein grosser Verteidigungshaushalt tragen zur Startup-Szene bei.
- Frankreich: Der Cyberpol in Rennes fördert die Arbeit im Bereich der Cybersicherheit.
- Deutschland: Förderung durch Organisationen wie das Institut für Cyber Defence der Universität der Bundeswehr München.
- Estland: Standort des CCDCOE der NATO sowie Staat mit einem hohen Digitalisierungsgrad.
- Singapur: Der Staat verfügt über eine der höchsten Pro-Kopf-Verteidigungsausgaben der Welt.

Allgemeines Vorgehen

Im Rahmen des Scoutings werden die Ressourcen jedes Unternehmens, das jeweilige Problem, das es zu lösen versucht, sowie die Lösung des Unternehmens, analysiert. Zudem wird untersucht, für welche Stakeholder (armasuisse, andere Bundesbehörden innerhalb und ausserhalb des VBS) das Unternehmen und seine Lösung interessant sein könnte. Die entsprechende Stelle der Bundesverwaltung kann auch eine konkrete Anfrage stellen und der CYD Campus wird versuchen, mit Hilfe seines Netzwerks die innovativsten und am besten geeignetsten Unternehmen zu finden, um eine bestimmte Herausforderung zu bewältigen. Bei Bedarf wird eine tiefergehende Evaluation oder ein Proof-of-Concept gestartet.

2021: 300 STARTUPS
davon 60 technische Präsentationen
davon 20 an zuständige Stellen innerhalb BV verwiesen
8 Proof-of-Concepts umgesetzt
12 aktive Scouting-Partner

Aktivitäten in 2021

Vereinigtes Königreich

Im April 2021 führte der CYD Campus ein Scouting zu Cybersicherheitsfirmen im Vereinigten Königreich durch. Der Swiss Business Hub (SBH) in London war massgeblich an der Identifizierung interessanter Unternehmen beteiligt und erstellte mit Hilfe von lokalen Experten und des gesamten Botschaftsteams eine Longlist mit rund 100 britischen Startups und Firmen. Im Vereinigten Königreich traf sich das Scouting Team mit einer Vielzahl von Unternehmen, die sich grob in die folgenden Kategorien einteilen lassen: Sicherheit der Lieferkette, Datenanalyse, Reaktion auf Netzwerkerkennung, industrielle Kontrollsysteme, Infrastruktur und Bedrohungsanalyse.

Deutschland und Österreich

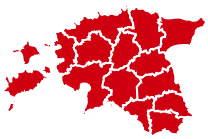
Ein ähnlicher Prozess wie im Vereinigten Königreich wurde Ende 2021 für Deutschland und Österreich durchgeführt, wodurch ebenfalls interessante Unternehmen ermittelt werden konnten.

Frankreich

Ausserdem nahm der CYD Campus am Forum International de la Cybersecurité in Lille, Frankreich, sowie an der European Cyber Week in Rennes teil, im Rahmen derer mehrere neue Kontakte geknüpft werden konnten.

Estland

Ein Besuch in Tallinn, Estland, wurde unternommen, um erste Einblicke in das dortige Cyber-Sicherheitsökosystem zu gewinnen. Es gibt einige sehr interessante Unternehmen, insbesondere im Bereich der Cyber-Ausbildung. Das lokale Ökosystem zur Unterstützung von Startups mit Wissen, Finanzmitteln und Humankapital ist gut entwickelt, allerdings ist die absolute Zahl der disruptiven und reifen Startups gering.



USA

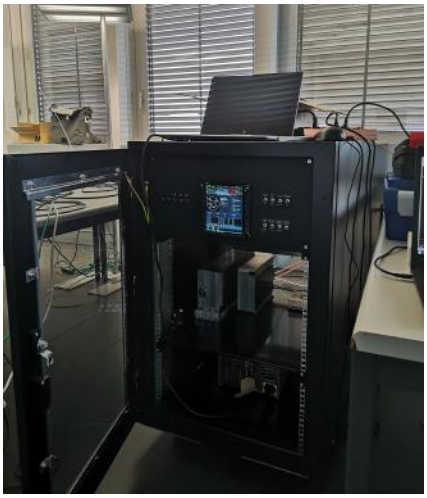
In den Jahren 2019 und 2020 wurde das Cybersicherheitspanorama der Vereinigten Staaten gründlich nach interessanten Technologien untersucht. Angesichts der schnellen Entwicklungen und des grossen Marktes wurde im August 2021 eine Reise in die USA durchgeführt, die es ermöglichte, mehrere zusätzliche Unternehmen zu treffen und Informationen mit wichtigen Partnern auszutauschen.

10 Laborinfrastrukturen

Die Laboreinrichtungen des CYD Campus sind für den kollektiven Wissensaufbau eingerichtet. Zusätzlich zum bestehenden Cybersecurity Lab wurde 2021 an der Weiterentwicklung der Laborinfrastrukturen gearbeitet, auf die in den folgenden Abschnitten näher eingegangen wird.

Erweitertes Cyber Avionik Labor

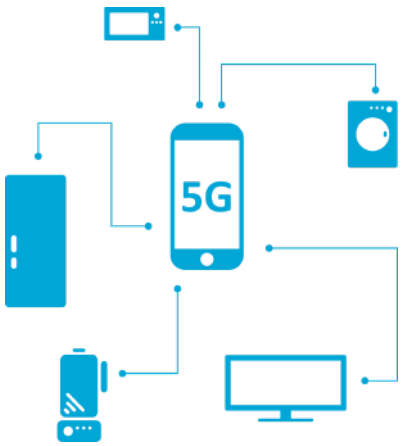
Das Avionik Labor des CYD Campus hat bereits erfolgreich die Erprobung und Sicherheitsüberprüfung von Flugzeugtechnologien unterstützt und Ergebnisse wurden unter anderem im Aviation Village der Hackerkonferenz DEFCON publiziert. Nun wird das Lab um die Pilot Datalink Communication (CPDLC) Technologie erweitert. CPDLC ist ein Datenlink über den sicherheitskritische Instruktionen zwischen Flugzeug und Fluglotsenden ausgetauscht werden. Forschungsarbeiten des CYD Campus haben bereits aufgezeigt, dass CPDLC ohne Authentifizierung nicht sicher ist und zum Beispiel sogenannte Man-in-the-Middle Angriffe möglich sind. Nun soll dies in der Praxis in einer Laborumgebung mit zertifizierter Hardware erprobt werden.



Erweiterung Cyber Avionik Lab um Pilot Datalink Communication (CPDLC)

5G-Labor im Aufbau

Das Fachwissen und die Kompetenz im Bereich der 5G-Technologie sind in der Schweiz gering, insbesondere im Bereich der Sicherheit und des Core-Netzwerks. Die meisten Betreiber lagern den Aufbau und sogar den Betrieb der Infrastruktur aus, und akademische Einrichtungen haben keinen Zugang zu Forschungslabors, um Studierende auszubilden. Ein 5G-Forschungslabor in der Schweiz ist für das VBS und die FUB von grosser Bedeutung. Kritische Infrastrukturen werden in Zukunft vermehrt 5G-Technologie einsetzen. Das 5G-Forschungslabor wird das fehlende Wissen in die verschiedenen Organisationen des VBS bringen und das breite Spektrum der Sicherheitsaspekte erforschen.



Satcom Labor

Um die bisherigen improvisierten Experimentierplattformen mit kleinen Satellitenantennen zu ergänzen, wird ein Satcom Labor aufgebaut. Im Zentrum dieses Labors steht eine Satellitenschüssel von 2.5 Metern Durchmesser, welche auf einer motorisierten Plattform montiert ist. Sie erlaubt es den CYD Campus Mitarbeitenden, die Schüssel über eine Konfigurationsplattform auf die Satelliten auszurichten und, im Falle von nicht geostationären Satelliten, ihrer Bahn zu folgen. Der Empfänger der Schlüssel ist darauf ausgelegt, eine Vielzahl von Frequenzen zu empfangen, was es den Forschenden ermöglicht, mehrere Frequenzbänder gleichzeitig zu nutzen. Die Fertigstellung des Labors ist für den Sommer 2023 geplant.

Satcom Cyber Security Lab in Zürich

Data Science Lab

Deep-Learning-Algorithmen benötigen eine hohe Rechenkapazität. Grafikprozessoren (GPUs) sind für die Art der mathematischen Operationen, die von diesen Algorithmen ausgeführt werden, besonders optimiert. Um den Forschenden des CYD Campus ausreichende Rechenressourcen zur Verfügung zu stellen, wurde im Data Science Lab ein GPU-Cluster eingerichtet. Dieser umfasst etwa 30 GPUs, die dynamisch zur Verfügung gestellt werden können. Die Nutzer/innen müssen nur ihre Aufgabe (Code) einreichen, die automatisch auf einem freien Grafikprozessor ausgeführt wird. So ist es möglich, mehrere Aufgaben gleichzeitig einzureichen. Der Grafikprozessor-Controller verwaltet die Zuweisung der Aufgaben auf den verschiedenen Grafikprozessoren. Diese Infrastruktur erleichtert es Nutzern und Nutzerinnen, Grafikprozessoren zu verwenden und gemeinsam zu nutzen, z. B. für maschinelle Übersetzungen, zur Erkennung von Fakes oder zur Vorhersage von Zeitreihen. Zudem wurde dieses Jahr ein FPGA Server als Ergänzung zu den GPUs und CPUs im Lab eingerichtet.

Scion

Um das Potenzial neuer Netzwerktechnologien zur Sicherung des Datenverkehrs über Wide-Area Networks (WANs) zu demonstrieren, wird ein Netzwerklabor zwischen den drei CYD Campus Standorten (Thun, Lausanne und Zürich) aufgebaut. Die Standorte werden über die neue Scion-Technologie der ETH Zürich verbunden, um ein sicheres und kontrollierbares Routing zu ermöglichen. Zudem bieten programmierbare Switches an den Standorten die Möglichkeit, neue Verschleierungsmethoden für den Datenverkehr im Netzwerk zu implementieren und auf ihre Effizienz zu untersuchen. Diese Laborinfrastruktur wird von Forschenden und Partnern des CYD Campus für Forschungs- und Innovationsprojekte genutzt.

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

11 Anlässe

Konferenzen

16.-18. November 21 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.

27.-29. September 21 CYD Konferenz & CRITIS
Am 28. September 2021 fand im EPFL SwissTech Convention Center in Lausanne (remote war ebenfalls möglich) die CYD Campus Konferenz statt. Kernthema der Konferenz war die Sicherheit kritischer Informationsinfrastrukturen. Die Konferenz fand in Kollaboration mit der 16. Internationalen Konferenz zur Sicherheit kritischer Informationsinfrastrukturen (CRITIS 2021) statt, die am 27. und 29. September veranstaltet wurde.

7.-9. September 21 Forum International de Cybersécurité, Lille, Frankreich
Das Forum ist eine der grössten jährlichen europäischen Veranstaltungen zum Thema Cybersicherheit und bietet Stakeholdern die Möglichkeit, sich im europäischen Cybersicherheitsökosystem zu vernetzen. Im Jahr 2021 war die Schweiz zum ersten Mal mit dem CYD Campus und einem Dutzend weiterer Unternehmen vertreten. Das Hauptziel der Teilnahme des CYD Campus war es, Unternehmen mit innovativen Ideen im Bereich Cybersicherheit zu finden.

10.-11. März 21 Swiss Cyber Security Days
Dr. Vincent Lenders, Dr. Luca Gambazzi und Giorgio Tresoldi stellten ein Video zum Thema Locked Shields her, welches im Rahmen der Konferenz gezeigt wurde.

Challenges & Hackathons

11.-15. Oktober 21 Car Hackathon
Am Car Hackathon nahmen ca. 20 Personen von armasuisse, der Industrie, Hochschulen, FUB, und fedpol teil. Es wurden diverse Fahrzeuge auf ihre Cybersicherheit untersucht und Exploits für bestimmte Schwachstellen getestet. Getestet wurden E-Cars, klassische Benzin-Autos und ein Duro.

28. September 21 Cyber Startup Challenge
Startups konnten unter dem diesjährigen Motto «Stärken Sie Ihr Information Sharing and Analysis Center (ISAC)» ihre innovativen Technologielösungen im Bereich der Aufklärung von Cyber-Bedrohungen mit dem Fokus auf den Schutz kritischer Infrastrukturen einreichen. Das Zürcher Sieger-Unternehmen Decentriq wurde an der CYD Campus Konferenz am 28. September 2021 gekürt.

Data Science Challenges

8. November 21:	Meme Classification
24. September 21:	Dialect Identification + GPU cluster
21. Juni 21:	FitBit Data
10. Mai 21:	IoT Device Fingerprints
29. März 21:	Tipping Points
15. Januar 21:	Early Warning Signals

Eröffnungsrede des Leiters CYD Campus an der CYD Konferenz in Lausanne


Car Hackathon Thun


Forum International de Cybersécurité in Lille

Lunchseminare

Aufgrund der anhaltenden Pandemie mussten dieses Jahr viele Seminare abgesagt werden. An diesen Informationsanlässen werden Vorträge von jeweils ausgewählten Referent/innen zu spezifischen CYD Fachthemen für Kunden der Verteidigung und der Bundesverwaltung organisiert.

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

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

19. Mai 21: Tutorial: Running programs at terabits per second in network switches (P4 and Intel Tofino), Referent: Roland Meier, ETH Zürich

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

Referenten:

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

Retreats

28. Juni - 2. Juli 21: Cyber Alp Retreat

CYD Campus Forschende und ausgewählte Forschungspartner hielten Vorträge zu Schlüsselthemen der Cybersicherheit und der Datenwissenschaften. Die Veranstaltung brachte Akteure aus dem VBS, der Industrie und der Wissenschaft zusammen, um sich über die aktuellen und zukünftigen Herausforderungen und Treiber im Cyberspace auszutauschen.

Forschungsrapporte

Die Jahresrapporte dienen dazu, über laufenden 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.

3. Juni 21: Forschungsrapport 3a Cyberspace

10. August 21: Forschungsrapport 3b Data Science

Lunchseminar zu Quantum-Resistent Edge in Thun

Forschungsrapport Data Science in Thun

Cyber-Alp Retreat 2021 in Gstaad

Besuche

16. November 21:	Besuch Military Aviation Authority, Thun
10. November 21:	Besuch Chef der Armee, Thun
1. November 21:	Besuch Cyber-Lehrgang 2021, Thun
15. Oktober 21:	Vorstellung Data Science an Studenten ETH
8. September 21:	Besuch Hochschulen Luzern und ICT Warriors, Thun

TMM Anlass

2. Dezember 21:	Cybersicherheitstechnologien, CYD Campus Lausanne

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

8. Oktober 21 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:

5. August 21

26. Januar 21

Besuch Cyber-Lehrgang der Armee

TMM Anlass zu Cybersicherheitstechnologien in Lausanne

Studentischer Fachaustausch in Thun

12 Referate

- 9. November 21 — *Collaboration EPFL-CYD Campus: Manager's Lunch*, EPFL Innovation Park, Lausanne, Dr. Vincent Lenders
- 25. Oktober 21 — *Panel discussion*, *Workshop on Systems Challenges in Reliable and Secure Federated Learning, ACM SOSP*, Dr. Gérôme Bovet
- 15. Oktober 21 — *Panel on the future of digital trust*, Digital Trust 2025, Genf, Dr. Vincent Lenders
- 8. Oktober 21 — *EPFL Forum*, Karrieremesse, Lausanne, Dr. Mathias Humbert
- 30. September 21 — *Security and Privacy in Wireless Communication Systems*, Abschlusssitzung Expertengruppe Cybersecurity VBS, Dr. Daniel Moser
- 3. September 21 — *Cyberbedrohungen verstehen*, DSC Security Week, Dr. Daniel Moser
- 27. August 21 — *Deep Fake Video Bundesrätin Viola Amherd*, Kadertag VBS, Dr. Gérôme Bovet
- 26. August 21 — *Fusion von OSINT und SAR-IMINT - NATO/PfP Research Program SET-279*, Informationsveranstaltung zu Radarsatelliten, armasuisse, Thun, Dr. Albert Blarer
- 7. Juli 21 — *Présentation du CYD Campus*, visites des secrétaires généraux de la Confédération à l'EPFL», Dr. Vincent Lenders
- 9. Juni 21 — *Digitale NRW-Ministerreise in die Schweiz - Roundtable: Cyber Security*, Dr. Vincent Lenders
- 1. Juni 21 — *Machine Learning for Intrusion Detection Systems: Challenges and Opportunities*, FUB TechTalk, Dr. Mathias Humbert
- 30. April 21 — Vorstellung *CYD Campus*, Bundeshaus, Besuch Verteidigungsministerin, Österreich, Dr. Vincent Lenders
- 21. April 21 — *Analyzing Cybersecurity Risks with and in Machine Learning*, SDSC (ETH/EPFL) & ZISC (ETH), Dr. Mathias Humbert
- 7. April 21 — *Fake News in Social Media: How to fight them?* , Kdo Op - armasuisse W+T, Dr. Ljiljana Dolamic und Dr. Vincent Lenders
- 25. März 21 — *Wireless Security in Critical Infrastructures: Legacy Debt and Opportunities*, ZISC (ETH), Dr. Martin Strohmeier
- 18. März 21 — *Secure and Fast Satellite Broadband*, CySat, Davos, Dr. Vincent Lenders
- 10. März 21 — *The role of AI in Cyberdefence*, Swiss Cyber Security Days, Fribourg, Dr. Vincent Lenders
- 25. Februar 21 — *Cyber-Defence Campus: Bilanz nach 2 Jahren*, Subkommission EDA/VBS des Ständerats, Bundehaus Bern, Dr. Vincent Lenders
- 17. Februar 21 — *Cyberdefence Research and Innovation: The Swiss Approach*, UK-Swiss Cyber Seminar, Bern, Dr. Vincent Lenders
- 10. Februar 21 — *Research on Aviation Cyber Security*, BAZL, Dr. Martin Strohmeier
- 21. Januar 21 — *How (not) to do wireless security*, Eurocontrol, Dr. Martin Strohmeier
- 20. Januar 21 — *Deception technologies*, FUB TechTalk, Dr. Luca Gambazzi

13 Wissenschaftliche Publikationen

13.1 Papers

Dezember

Classi-Fly: Inferring Aircraft Categories from Open Data

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

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

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

Adaptive Uplink Data Compression in Spectrum Crowdsensing Systems

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

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

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

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

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

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

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

November

Federated Learning for Malware Detection in IoT Devices

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

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

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

When Machine Unlearning Jeopardizes Privacy

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

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

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

September

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

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

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

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

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

August

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

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

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

Juni

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

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

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

Mai

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

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

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

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

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

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

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

April

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

März

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

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

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

Februar

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

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

Crowdsourced Air Traffic Data from the OpenSky Network 2019–20

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

13.2 Studentische Arbeiten

CYD Fellows

Postdoc

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

PhD

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

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

Studierende und Praktikant/innen

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

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

14 Kommunikation

@Cyber-Defence Campus

@cydcampus

Webmitteilungen

- 20.12.2021, Erfolgreiche Zusammenarbeit zwischen dem Cyber-Defence Campus und dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI)
- 02.11.2021, Wissenschaftlicher Mitarbeiter des CYD Campus erhält Professur an der Universität Lausanne
- 06.10.2021, Automatische Erkennung von Fake News durch Künstliche Intelligenz?
- 30.09.2021, Treffen Sie die Finalisten der Cyber Startup Challenge 2021
- 08.09.2021, Cyber-Defence Campus Konferenz 2021
- 27.07.2021, CYD Campus demonstriert neue Angriffsformen gegen kritische Infrastrukturen
- 23.07.2021, Cyber-Defence Campus Wissenschaftler/innen erhalten Best Paper Award
- 23.06.2021, Der Cyber-Defence Campus findet kritische Sicherheitslücke in VPN Software
- 10.06.2021, Aufruf Cyber Startup Challenge 2021
- 25.05.2021, Der Cyber-Defence Campus an der NATO CyCon Konferenz in Tallinn, Estland
- 21.05.2021, Cyber-Defence Campus als treibende Innovationskraft

Medienmitteilungen

- 20.12.2021, Erfolgreiche Zusammenarbeit zwischen dem Cyber-Defence Campus und dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI)
- 30.09.2021, «Cyber Startup Challenge 2021»: Schweizer Startup Decentriq überzeugt Jury
- 25.05.2021, Forschungsprojekte des Cyber-Defence Campus VBS an der NATO Cyber Conflict Konferenz
- 22.03.2021, Neues Team beim Cyber-Defence Campus VBS zur Detektion von Software-Schwachstellen

Armafolio

- Dezember Ausgabe, Künstliche Intelligenz im Einsatz gegen Desinformation in sozialen Netzwerken

Medien

- 15.10.2021, Der Schlüssel für eine effektive Cyber Defence liegt im Teamwork, Smart Media, Distributionskanal Tagesanzeiger

15 Ausblick 2022

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 2022 gemäss Strategie Cyber VBS umgesetzt werden sollen:

- Anhebung des CYD Campus auf das Niveau des nationalen technischen Kompetenznetzwerks für Cyberdefence mit Hochschulen und Industrie. Insbesondere soll die Unterstützung auf die im Cyberbereich tätigen Stellen des Bundes ausserhalb des VBS wie die Betreiber kritischer Infrastrukturen erweitert werden.
- Unterstützung beim Aufbau des Cyber Kommandos. Besonders bei den Vorhaben Cyber Training Center (CTC), Mobile Cyber Mittel (MCM), vordienstliche Ausbildung und dem Cyber Lehrgang.
- Weiterentwicklung eines automatisierten Technologie-Radars (TMM 2.0), 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 verwalten.
- Erweiterung des CYD Campus Antennenstandortes Zürich. Aus Platzgründen muss der CYD Campus an der ETH Zürich im Sommer 2022 in grössere Räumlichkeiten umziehen. Der neue Standort wird Arbeitsplätze bereitstellen sowie die Möglichkeit bieten, Seminare und Workshops durchzuführen.
- Im 2022 soll ein neues Kommunikationskonzept umgesetzt werden. Insbesondere soll die Webseite des CYD Campus komplett neu ausgestaltet werden mit mehr Inhalten und aktuellen News für die Cyberdefence Community.
- Die Laborinfrastrukturen des CYD Campus sollen weiter ausgebaut werden, vor allem für die Projekte im Bereich der 5G-Sicherheit, der SATCOM-Sicherheit, der Sicherheit von E-Fahrzeugen und des Future Internets.
- Weiterentwicklung des CYD Fellowship Programms, um wissenschaftliche Cyber-Talente möglichst früh zu erkennen und zu fördern. Ein neues Fellowship für Proof-of-Concepts soll die Innovationskraft von jungen Talenten fördern und sie in die Innovationsprozesse des VBS besser einbinden.
- Entsendung einer Person zum CCDCoE nach Tallinn (Estland). Ein Mitarbeiter des CYD Campus wird ab 2022 permanent in Tallinn beim CCDCoE stationiert sein, um die Zusammenarbeit mit der NATO im Bereich Technologie und Forschung gezielt zu fördern.

Kontakt

Cyber-Defence Campus

Feuerwerkerstrasse 39

CH-3602 Thun

Auf der Mauer 17

CH-8001 Zürich

EPFL Innovation Park, Bâtiment I

CH-1015 Lausanne

cydcampus@armasuisse.ch

+41 58 480 59 34

Mehr Informationen:

https://cydcampus.ch