Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung
Bevölkerungsschutz und Sport
armasuisse
Wissenschaft und Technologie

CYD
CYBER
DEFENCE
CAMPUS

Cyber-Defence Campus

Jahresbericht 2023

Editorial

Liebe Leserin, lieber Leser

2023 war ein bewegtes Jahr für die Schweiz im Cyberraum. Die Anzahl gemeldeter Cybervorfälle ist dieses Jahr auf fast 50'000 Meldungen angestiegen. Schweizer Organisationen und Behörden waren im Sommer über zwei Wochen Zielscheibe eines koordinierten DDoS Angriffes. Hackerinnen und Hacker konnten heikle Daten von Sicherheitsbehörden über die Schweizer IT-Dienstleisterin Xplain AG und Concevis stehlen. Bund und Kantone beschlossen eine neue nationale Cyberstrategie (NCS) und die Armee hat ihre Gesamtkonzeption Cyber als wichtigen Meilenstein zur Entwicklung ihres Cyber Kommandos verabschiedet.

Diese Ereignisse verdeutlichen die Wichtigkeit unserer Mission beim Cyber-Defence Campus, die Cybersicherheit in der Schweiz zu stärken und die voranschreitende Digitalisierung unseres Landes mitzugestalten. Insbesondere sind wir mehr denn je gefordert die technologischen Entwicklungen im Cyberbereich zu antizipieren, voranzutreiben, und mit unserem Wissen die Cyber Resilienz in der Schweiz zu stärken.

Dies ist uns dieses Jahr in einigen Bereichen gelungen. Dank zahlreichen durchgeführten Veranstaltungen trugen wir zum Beispiel zu einem aktiven Austausch und zu einer Vernetzung der Schweizer Cyber Community bei. Einer unserer Höhepunkte war unsere Konferenz am 26. Oktober, bei der wir über 350 Teilnehmende aus Industrie, Armee, Wirtschaft, Verwaltung und Forschung im Kursaal in Bern begrüssen durften, um den Diskurs zu der Rolle der Künstlichen Intelligenz in der Sicherheit voranzutreiben. Im Herbst konnten wir ebenfalls mehrtägige Cyber Trainings zu hochaktuellen Themen, wie der Sicherheit des Energiesektors und der Cybersicherheit von Autos, anbieten. Diese Trainings waren begleitet von Hackathons, an denen Vertreterinnen und Vertreter aus Industrie, Betreibende von kritischen Infrastrukturen, Hochschulen und Armee teilgenommen haben und wertvolle Erfahrungen in diesen kritischen Bereichen sammeln konnten.

Auch dieses Jahr konnten sich zahlreiche innovative Startups und talentierte Studierende bei uns bewerben und sich über unsere Challenges und Studentenprogramme aktiv an der Schweizer Cyber-Defence beteiligen. Das Thema der diesjährigen Cyber Startup Challenge war die Sicherheit von Smartphones und die Firma Ostorlab konnte sich am Schluss im Final an der CYD Campus Konferenz durchsetzen. Über 60 Studierende erhielten im Rahmen ihrer Studienarbeit oder eines Praktikums beim Cyber-Defence Campus die Möglichkeit auf einen mehrmonatigen Forschungsaufenthalt und sammelten erste praktische Erfahrungen zum Thema Cyber.

Um die nationale Cyberstrategie (NCS) umzusetzen, haben wir dieses Jahr ein neues Team gebildet, welches sich ausschliesslich mit dem Technologie Monitoring im Cyberbereich auseinandersetzt. Unter Federführung dieses neuen Teams wurde zum Beispiel zusammen mit über 50 Fachleuten aus Hochschulen und Industrie eine ausführliche Trendanalyse über die Technologien zur Verschlüsselung und zum Schutz der Daten im digitalen Zeitalter durchgeführt, welche dieses Jahr als Buch ("Trends in Data Protection and Encryption Technologies") erschienen ist. Weitere Technologie- und Trendanalysen im Bereich der Künstlichen Intelligenz und der Quantum Technologien sind bereits am Laufen.

Unsere Forschungsprogramme, welche die Kompetenzen der Hochschulen und Industrie einbinden, haben dieses Jahr geholfen, neue Cyberbedrohungen und deren Auswirkungen im Bereich Cybersicherheit und Datenwissenschaften frühzeitig zu erkennen sowie Lösungsansätze zu entwickeln. Der Cyber-Defence Campus veröffentlichte 2023 zusammen mit seinen Partnerinnen und Partnern über 80 wissenschaftliche Publikationen in verschiedenen disruptiven Technologiebereichen wie zum Beispiel Künstliche Intelligenz, generative LLM (Large Language Models), 5G Sicherheit, die Cybersicherheit von Weltraumtechnologien, oder die Sicherheit von zukünftigen Netzwerktechnologien. Auch zahlreiche Sicherheitsschwachstellen in Software und Geräten wurden gefunden und an die betroffenen Stellen zurückgemeldet.

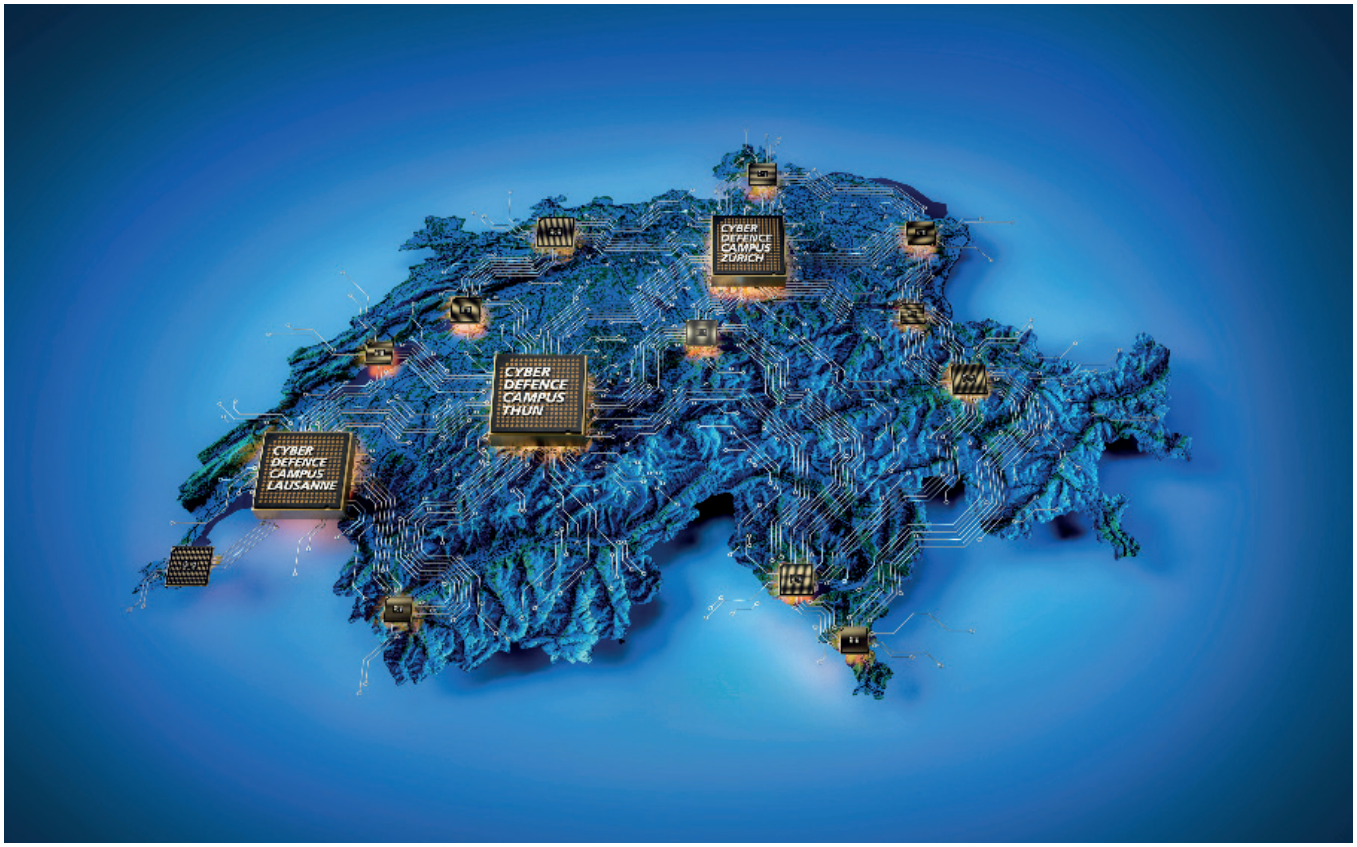
In diesem Jahr haben wir eine neue Website in frischem Design unter cydcampus.admin.ch liveschalten können. So können wir zeitnaher und transparenter über unsere Aktivitäten und Resultate informieren.

Ich freue mich, Ihnen spannende Einblicke aus unserem Alltag und aus unseren Projekten zu zeigen und wünsche Ihnen viel Spass beim Lesen und beim Entdecken des Cyber-Defence Campus.

Thun, Dezember 2023

Dr. Vincent Lenders
Leiter Cyber-Defence Campus

Inhaltsverzeichnis



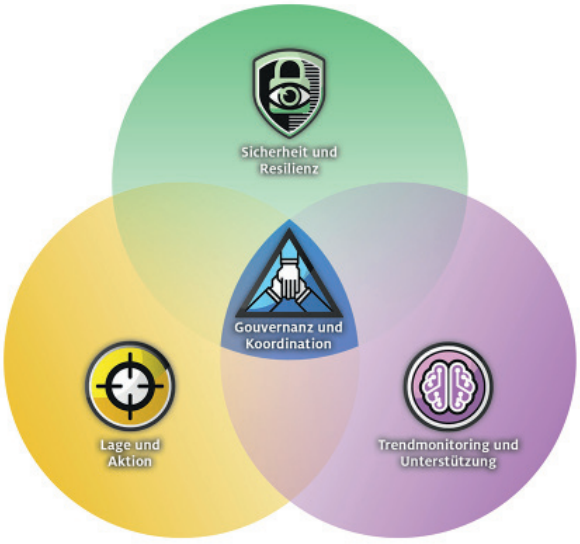
1. Über den Cyber-Defence Campus

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 Eidgenössische 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 Cyber-Defence (APCD). Angesichts der rasanten Weiterentwicklung der Cyber-Bedrohungslage in den letzten 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 Cyberstrategie NCS abgestimmt.

Als Teil dieser Strategien wird im VBS seit fünf Jahren der Cyber-Defence (CYD) Campus entwickelt und betrieben. Er ist beim Bundesamt für Rüstung (armasuisse Wissenschaft und Technologie) angesiedelt. Der CYD Campus bietet dem VBS eine Antizipations- und Wissensplattform zur Identifikation und Bewertung technologischer, wirtschaftlicher und gesellschaftlicher Cyber-Trends. Um möglichst eng mit den Hochschulen, dem VBS und der Industrie zusammenarbeiten zu können, ist der CYD Campus an drei Standorten vertreten: Am Hauptstandort Thun (armasuisse Wissenschaft und Technologie), im Innovationspark an der EPFL in Lausanne und in der Nähe der ETH in Zürich. Dies erlaubt es ihm, gemäss den Bedürfnissen der Schweizerischen Eidgenossenschaft, effizient Know-how aufzubauen und Cyber-Expertise bereitzustellen.

Der CYD Campus wirkt als Bindeglied zwischen der Industrie, der öffentlichen 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.



Strategie Cyber VBS 2021 - 2024

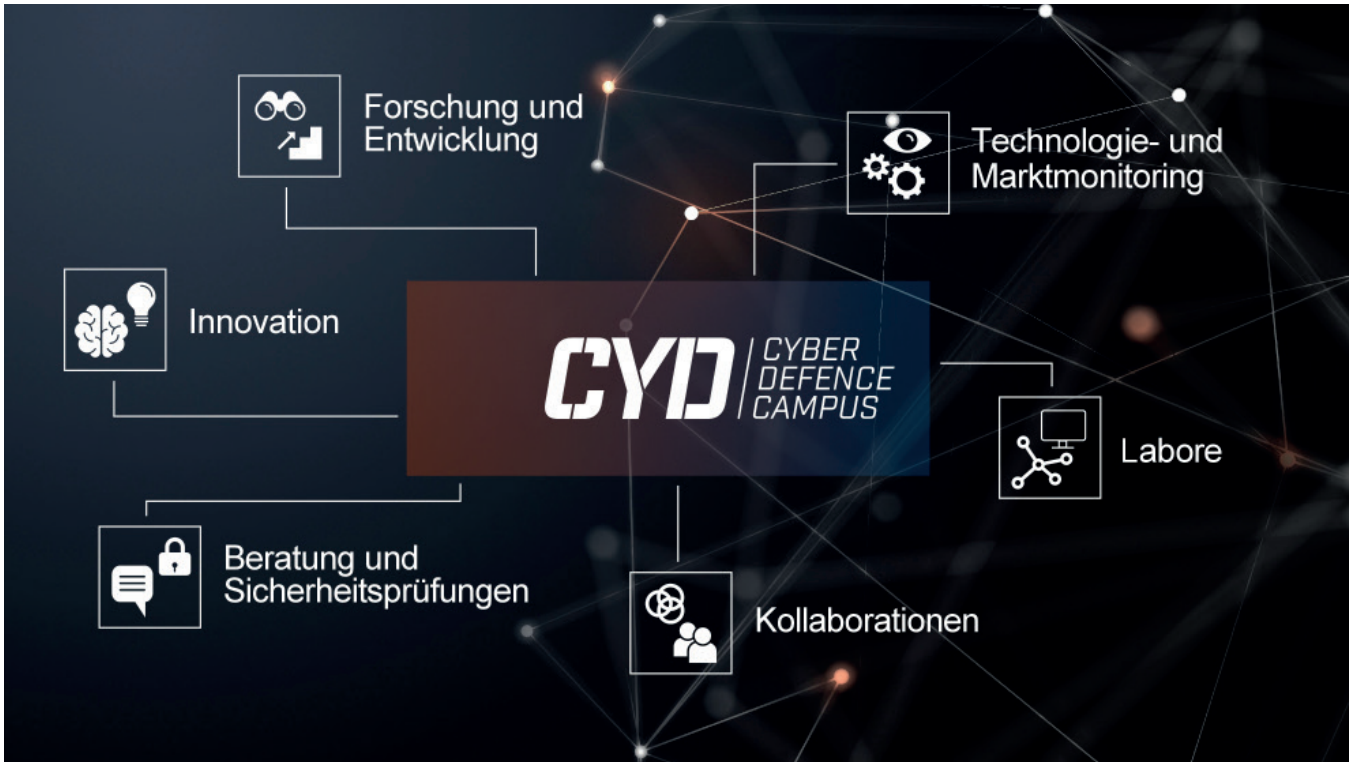
Der CYD Campus hat heute folgende drei Schlüsselaufgaben:

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

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

Ausbildung von Cyberfachleuten: Beim CYD Campus werden Talente auf Master-, PhD- und Postdoc-Stufe sowie Hochschulpraktikantinnen und -praktikanten für zukünftige Herausforderungen ausgebildet. Zudem werden gemeinsame Cyber Trainings (z.B. Hackathons) angeboten.

Das Ziel dieses Jahresberichts ist es, Einblicke in die Umsetzung der oben genannten Schlüsselaufgaben im Jahr 2023 des CYD Campus zu gewähren. Dabei wird ein kurzer Überblick über das CYD Campus Team sowie über einige Highlights des Jahres 2023 gegeben. Die öffentlichen Tätigkeiten im Rahmen von Forschungsprojekten, Kundenaufträgen und Demonstratoren werden ebenfalls erläutert. Weiter werden die Arbeiten im Jahr 2023 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 2024 gewährt.



Kernkompetenzen des Cyber-Defence Campus

Unsere Partner

National		
Bund und Kantone	Hochschulen	Industriepartner/-innen
Bundespolizei fedpol Bundesamt für Statistik Bundesamt für Zivilluftfahrt BAZL Bundesamt für Sport BASPO Eidgenössisches Departement für auswärtige Angelegenheiten EDA Nachrichtendienst des Bundes NDB Nationales Zentrum für Cybersicherheit NCSC Schweizer Armee Swisstopo Swissnex Kantonspolizei Zürich	Berner Fachhochschule (BFH) École polytechnique fédérale de Lausanne (EPFL) • Center for Digital Trust (C4DT) Eidgenössische Technische Hochschule Zürich (ETHZ) • Militärakademie an der ETH Zürich (MILAK) • Zurich Information Security and Privacy Center (ZISC) Fachhochschule Nordwestschweiz (FHNW) Haute École du Paysage, d'Ingénierie et d'Architecture de Genève (HEPIA) Haute école spécialisée de Suisse occidentale (HES-SO) Haute école de gestion de Genève (HEG Genève) • Secrétariat du Centre de recherche appliquée en gestion (CRAG) Hochschule Luzern (HSLU) Haute École d'Ingénierie et de Gestion du Canton de Vaud (HEIG-VD) Ostschweizer Fachhochschule (OST) Scuola universitaria professionale della Svizzera italiana (SUPSI) Universität Freiburg Université de Genève Université de Lausanne Université de Neuchâtel Universität St. Gallen Universität Zürich Zürcher Hochschule für Angewandte Wissenschaften (ZHAW)	Adnovum Anapaya Astrocast Brunner Elektronik AG CYSEC Decentriq Effixis FLARM Tehnology IBM Research Kudelski Security Modulos Nationales Testzentrum für Cybersicherheit Noser Engineering Nozomi Networks RUAG SBB Swisscom Tune Insight
International		
Öffentliche Organisationen	Hochschulen	Industriepartner/-innen
Bundesamt für Sicherheit in der Informationstechnik (BSI), DEU European Defence Agency EDA KRITIS Luxemburgische Armee, LUX NATO CCDCOE US Department of Defense, USA	IMDEA Networks, ESP KTH Royal Institute of Technology, SWE KU Leuven, BEL Northeastern University, USA Portland State University, USA Ruhr Universität Bochum, DEU RPTU Kaiserslautern-Landau, DEU Universidad de Murcia, ESP Universidad Rey Juan Carlos, ESP Universita di Genova, ITA Universität Luxemburg, LUX University of Oxford, UK University of Southern California (USC), USA	Countercraft, USA, ENG, ESP CybExer Technologies, EST Onekey, DEU Plug and Play Quarkslab, FRA SeRo Systems, DEU

Gesichter hinter dem CYD Campus

CYD Campus Leitung

Von links nach rechts

Dr. Colin Barschel
Leiter Innovationen und Industriekollaborationen

Giorgio Tresoldi
Leiter Internationale Beziehungen

Dr. Vincent Lenders
Leiter des CYD Campus

Dr. Bernhard Tellenbach
Leiter Cybersicherheit

Dr. Gérôme Bovet
Leiter Data Science

Dr. Alain Mermoud
Leiter Technologie Monitoring

Stefan Engel
Leiter Business Development und Stellvertretender Leiter des CYD Campus

Projektmanager/-innen und Experten/-innen

Cédric Aeschlimann
Cyber Training

Dr. Albert Blarer
Data Science

William Blonay
Cyber Security

Dr. Martin Burkhart
Cyber Security

Lucas Crijns
Innovation

Dr. Ljiljana Dolamic
Data Science

Daniel Hulliger
Cyber Security

Dr. Julian Jang-Jaccard
Technologie Monitoring

Dr. Miguel Keer
Cyber Security

Dr. Jonas Liechti
Data Science

Dr. Raphael Meier
Data Science

Dr. Roland Meier
Cyber Security

Dr. Daniel Moser
Cyber Security

Valentin Mulder
Technologie Monitoring

Damian Pfammatter
Cyber Security

Llorenç Roma
Cyber Security

Dr. Hông Ân Sandlin
Data Science

Ivo Stragiotti
Data Science

Dr. Martin Strohmeier
Cyber Security

Dr. Etienne Voutaz
Data Science

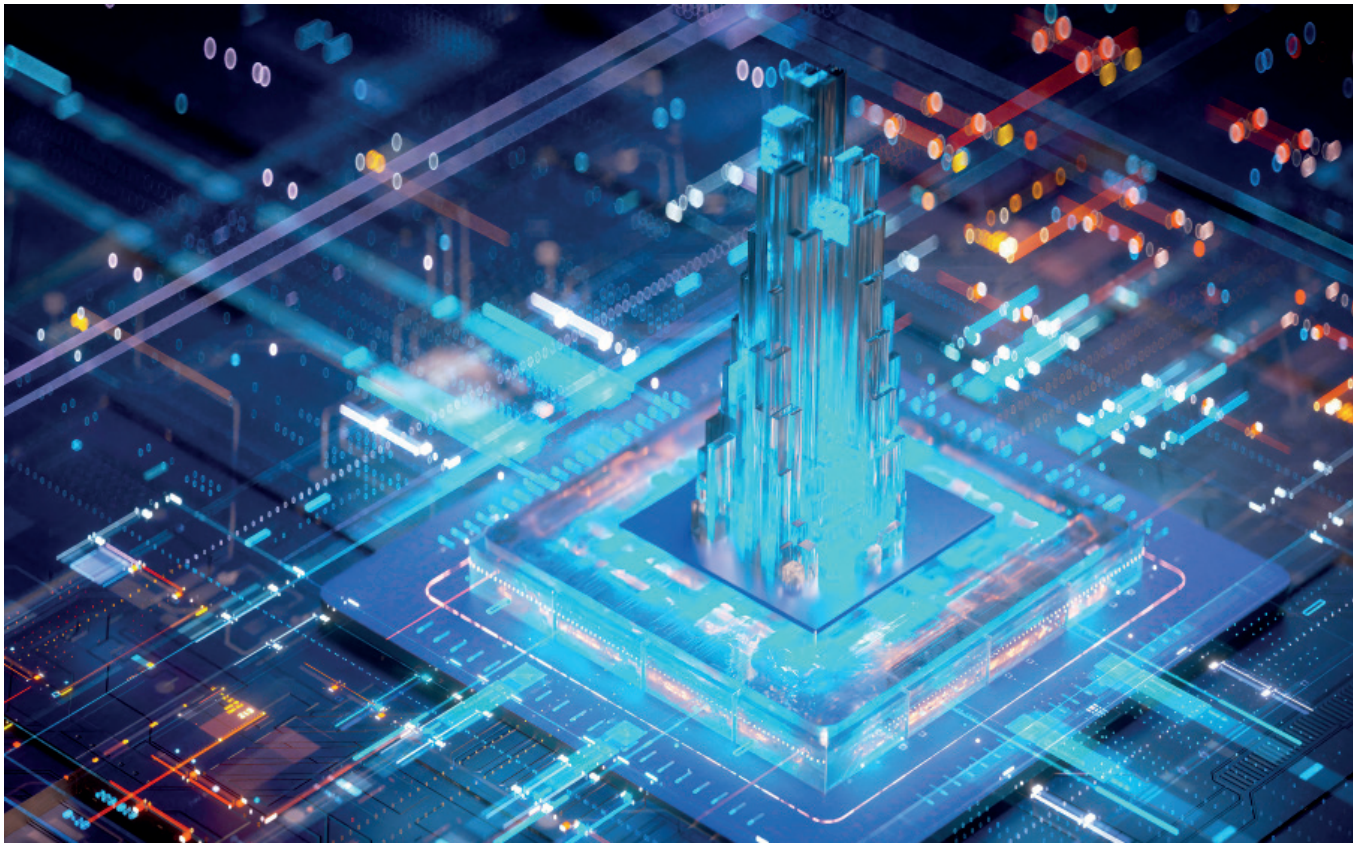
Support Team

Yasemin Akin
Assistenz Zürich

Monia Gieriet
Head of Administration and Event Management

Amina Kabashi
Assistenz Lausanne

Priska Weber
Assistenz Thun



2. Highlights

CYD Campus Konferenz über Künstliche Intelligenz

Am 26. Oktober 2023 hat der CYD Campus seine jährliche Konferenz im Kursaal in Bern veranstaltet. Das Thema der Konferenz lautete «Sicherheit im Zeitalter der Künstlichen Intelligenz». Mehr als 350 Personen nahmen am Anlass teil. Das Thema ist für den Cyber-Defence Campus sehr relevant, da Künstliche Intelligenz in der Cybersicherheit heute allgegenwärtig ist. Einerseits ist es möglich, Systeme durch die Verwendung von KI-Algorithmen sicherer zu machen. Beispiele hierfür sind die Erkennung von Malware oder Anomalien in Kommunikationsnetzen. Andererseits kann Künstliche Intelligenz auch ein Sicherheitsrisiko darstellen. Böswillige Akteurinnen und Akteure haben die Möglichkeit, das Verhalten von Algorithmen für KI auf verschiedene Weise zu beeinflussen, z.B. durch Data Poisoning. Um die Problematik besser zu verstehen, haben wir verschiedene Partnerinnen und Partner aus der akademischen Welt und der Industrie eingeladen, damit sie uns ihre Sicht auf das Thema näherbringen.

Die Konferenz begann mit einer Präsentation von Christophe Nicolas, CIO der Kudelski Gruppe. Als CIO eines der grössten Sicherheitsunternehmen der Schweiz und durch seine Erfahrung bot er spannende Einblicke in die Branche. Im Anschluss zeigte uns Juri Ranieri, auf welche Weise Google Sicherheit und KI in vielen seiner Produkte kombiniert, um diese sicherer zu machen. Carmela Troncoso von der EPFL gab uns einige Einblicke in den Datenschutz bei maschinellem Lernen (ML) – eine wichtige Herausforderung bei der Entwicklung von ML-Systemen mit personenbezogenen Daten. Darüber hinaus haben wir in diesem Jahr einigen unserer Studierenden die Möglichkeit geboten, ihre Arbeit in Form eines Elevator Pitch zu präsentieren. Wir hatten die Ehre, Korpskommandant Thomas Süssli, Chef der Armee, zu begrüssen, der uns seine Vision zu Sicherheit und KI in der Schweizer Armee darlegte. Das Thema Quantum ist heute mit vielen offenen Fragen verbunden. Christa Zoufal von IBM erklärte daher, wie die KI von den Fortschritten im Quantencomputing profitieren kann. Neben dem Datenschutz ist die Erklärbarkeit eine weitere zentrale Herausforderung, die gelöst werden muss, bevor KI auf breiter Basis eingesetzt werden kann. Philippe Cudré-Mauroux von der Universität Fribourg gab uns einige Anregungen, wie das Problem gelöst werden könnte. Anschliessend sprach Christine Choirat vom Bundesamt für Statistik als Vertreterin des Kompetenznetzwerks Künstliche Intelligenz der Schweizerischen Eidgenossenschaft von ihren Erfahrungen bei der Implementierung von KI in der Bundesverwaltung. Wie allseits bekannt, sind grosse Sprachmodelle (Large Language Models - LLMs) seit der Einführung von ChatGPT leicht zugänglich geworden. Um besser zu verstehen, was bei der Cyberverteidigung auf dem Spiel steht, haben bei einer Podiumsdiskussion drei Expertinnen und Experten auf diesem Gebiet die Chancen und Gefahren von LLMs erörtert.

Korpskommandant Thomas Süssli (Chef der Armee) referiert über die Herausforderungen der Armee im Bereich der Künstlichen Intelligenz an der CYD Campus Konferenz

Innovation bei der sicheren Smartphone-Kommunikation

Ein Hauptaugenmerk lag dieses Jahr auf der Sicherheit der Smartphone-Kommunikation, insbesondere bei sensiblen Informationen. Hervorzuheben sind drei Innovationsvorhaben: Das erste Projekt war die Sicherung von Smartphone-Kommunikation. Im Fokus des Projektes lag die Entwicklung und Nutzung einer Nachrichten-App für den Versand sensibler Daten. Der CYD Campus setzt in seiner Lösung auf die Nachrichten-App Threema und auf das SCION-Netzwerk, zwei Technologien mit Schweizer Hintergrund. In einem zweiten Projekt überzeugte das US-amerikanische Startup Ostorlab diesen Herbst die Jury der CYD Campus Startup Challenge und durfte auf der CYD Campus Konferenz am 26. Oktober 2023 seine innovativen Ansätze zur Sicherheitsanalyse mobiler Anwendungen präsentieren. Ostorlab hat einen Scanner für mobile Applikationen entwickelt, der es Organisationen ermöglicht, Sicherheitslücken in mobilen Anwendungen, sowohl bei Android- wie auch bei iOS-Anwendungen, effizient zu identifizieren. Beim dritten Vorhaben ging es um die Sicherheit der Smartphone Betriebssysteme. Die heute verbreiteten Smartphone-Ökosysteme Android und iOS bieten ein hohes Mass an Funktionalität und Flexibilität. Während Android und iOS für die Speicherung und Bearbeitung von nicht klassifizierten Daten breit eingesetzt werden, ist ein Einsatz im Bereich der klassifizierten Daten aktuell nicht oder nur sehr eingeschränkt möglich.

Cyber Training @ Cyber-Defence Campus

Das VBS beauftragte im Rahmen der Nationalen Cyberstrategie (NCS) den Cyber-Defence Campus mit dem Pilotprojekt «Cyber Training @ Cyber-Defence Campus»[1]. Das Projekt soll das Cyber-Ausbildungsangebot in der Schweiz stärken in dem es ein Konzept für die Koordination der Cyber Trainings in der Bundesverwaltung (ziviler und militärischer Stellen) erarbeitet. Zudem soll es die Möglichkeiten für die Integration ziviler Partnerinnen und Partner, z. B. kantonaler Behörden, Betreiberinnen sowie Betreiber kritischer Infrastrukturen in die Trainingslandschaft der Bundesverwaltung aufzeigen. Dabei stellt der CYD Campus ein fundiertes Trainingsangebot zur Verfügung. Cyber Training ist dabei nicht als individuelle Grundausbildung zu verstehen – vielmehr handelt es sich um spezifische Gruppenübungen mit Fokus auf wichtige Schnittstellen (z.B. zwischen Technik und Management). Um dieses Ziel zu erreichen, arbeitet der CYD Campus bei der Konzeption der technischen Übungen aber auch strategischen Simulationen eng mit dem Bundesamt für Cybersicherheit (BACS) zusammen und nutzt Synergien mit der Industrie wie auch der Cyber Training Range der Schweizer Armee.

Wie geht der CYD Campus dabei vor? Bis im Sommer 2024 werden verschiedene Analysen durchgeführt und unterschiedliche Schulungsformate getestet, um einerseits die Bedürfnisse der Zielgruppen zu validieren und andererseits ideale Rahmenbedingungen für Cyber Training in der Bundesverwaltung zu schaffen. Dabei konnte der CYD Campus im Herbst 2023 bereits zwei technische Trainings (zu Industrial Control Systems und Car Security) in Kombination mit einschlägigen Hackathons erfolgreich durchführen. Weiter ist für das Frühjahr 2024 noch eine Krisensimulation in Zusammenarbeit mit einer kantonalen Behörde vorgesehen. Die daraus gewonnen Erkenntnisse bilden die Grundlage für die weitere Entwicklung des Projekts «Cyber Training @ Cyber-Defence Campus».

1 https://www.cydcampus.admin.ch/de/cyber-training

Einblicke aus dem Cyber Training / Hackathon über die Sicherheit von E-Autos im Oktober in Thun

Aufbau des Technologie Monitoring-Teams

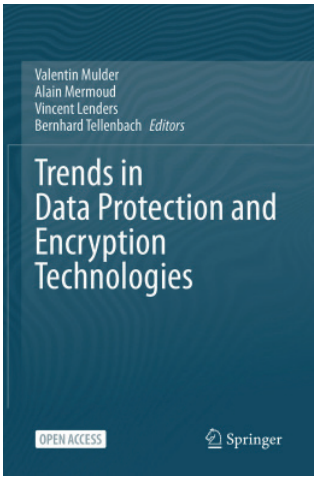
Dieses Jahr wurde beim Cyber-Defence Campus ein neues Team gebildet, welches von Dr. Alain Mermoud geleitet wird, und sich ausschliesslich mit der Analyse von Trends, Risiken und Abhängigkeiten von digitalen Technologien beschäftigt. In der heutigen digitalen Welt entwickeln sich Cyber-Bedrohungen, die sich die neuesten digitalen Technologien zunutze machen, schneller als je zuvor. Es ist eine Herausforderung, bei der Erkennung dieser Bedrohungen und der Bewertung ihrer möglichen Auswirkungen auf dem Laufenden zu bleiben. Valentin Mulder stiess Mitte 2023 nach einem zuvor beim CYD Campus abgeschlossenem Hochschulpraktikum als Vollzeitmitarbeiter zum Technologie Monitoring-Team (TM-Team). Im Oktober 2023 erhielt das Team mit Dr. Julian Jang-Jaccard, vormals Professorin und Leiterin des Cybersecurity Lab an der Massey University in Neuseeland weitere Verstärkung. Im Februar 2024 wird Perceval Faramaz, ebenfalls ein ehemaliger Hochschulpraktikant vom CYD Campus, die internationalen Entwicklungen verfolgen. Zudem wird das Team von zahlreichen Wissenschaftlerinnen und Wissenschaftlern, Hochschulpraktikantinnen und -praktikanten, Fellows und Studierenden von verschiedenen Hochschulen unterstützt.

In diesem Jahr hat das Team seinen Fokus auf drei wichtige Technologietrends gesetzt: Verschlüsselungstechnologien, generative Künstliche Intelligenz und Quantum Computing. Eine durch das TM-Team durchgeführte Studie liefert einen Überblick über die Entwicklungen, den gegenwärtigen Stand der Technik und die Cyber-Defence-Implikationen generativer Sprachmodelle, sogenannter Large Language Models (LLM).

Diese vor Kurzem veröffentlichte Studie[1] entstand in Zusammenarbeit mit Effixis SA, der EPFL, der HEC Lausanne sowie der HES-SO Valais-Wallis und liefert der Industrie, der öffentlichen Verwaltung und der Wissenschaft in der Schweiz einen detaillierten Einblick in die Entwicklung und die Risiken von LLM.

Ein Buch über Trends bei 38 Verschlüsselungstechnologien und Technologien zum Schutz von Daten ist in Zusammenarbeit mit über 50 Expertinnen und Experten aus Hochschulen und Industrie 2023 erschienen.

Das Monitoring über Quantum Technologien erfolgt laufend.



Das Buch „Trends in Data Protection and Encryption Technologies" ist in Open Acces unter folgender Adresse erhältlich https://link.springer.com/book/10.1007/978-3-031-33386-6

1 https://arxiv.org/abs/2303.12132

Quantifizierung der Cybersecurity-Forschungslandschaft in der Schweiz

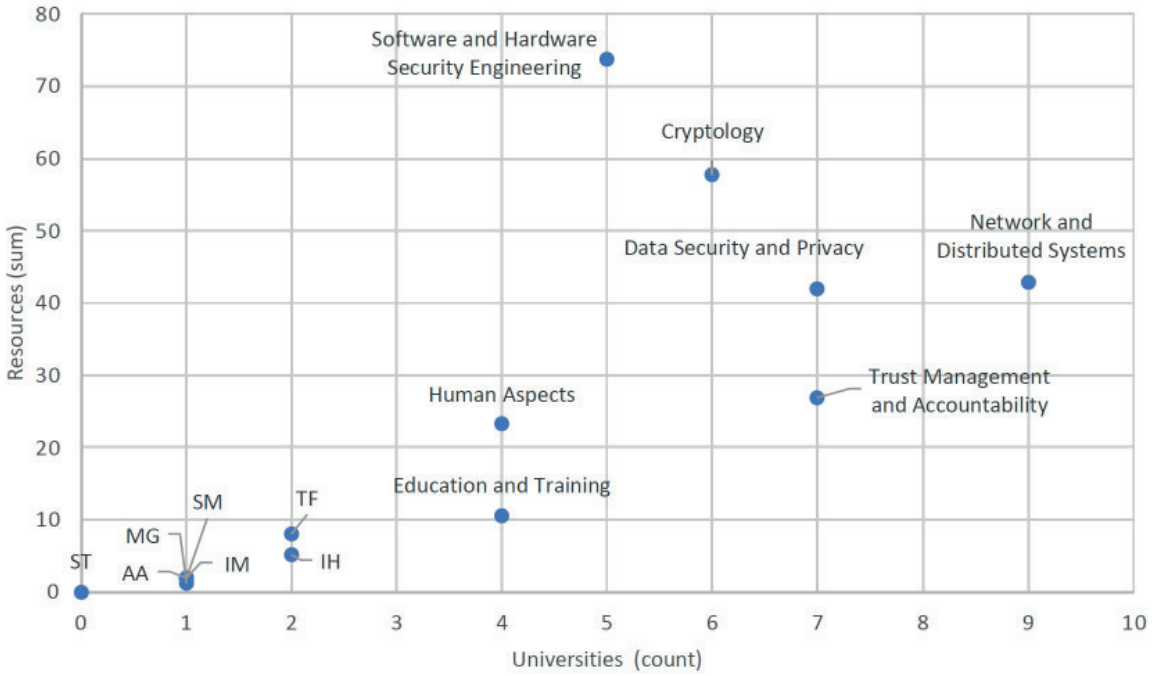
Die Nationale Cyberstrategie (NCS) der Schweiz unterstreicht die zentrale Rolle der Cybersicherheitsforschung für die Abwehr digitaler Bedrohungen, das Wirtschaftswachstum und die Innovationskraft der Schweiz. Doch wer investiert wie viel in welche Forschungsbereiche? Diese Fragen sind schwer zu beantworten, da die Schweizer Hochschulen eine weitgehende Autonomie bei der Festlegung ihrer Forschungsschwerpunkte geniessen.

Der CYD Campus ist federführend an verschiedenen NCS-Massnahmen beteiligt und war zunächst mit dem Problem der Datenerhebung konfrontiert. Er führte deshalb zusammen mit der Schweizerischen Akademie der Technischen Wissenschaften (SATW) eine umfangreiche quantitative Erhebung zur Cybersicherheitsforschung in der Schweiz durch.

In der Studie wurden 22 Schweizer Hochschulen befragt und deren Forschungsaktivitäten in 14 verschiedenen Bereichen der Cybersecurity untersucht. Die Ergebnisse zeigen, dass in der Schweiz insgesamt 297 Vollzeitäquivalente (VZÄ) in der akademischen Cybersicherheitsforschung beschäftigt sind.

Der Grossteil der Forschungsanstrengungen entfällt auf nur drei Bereiche: Software- und Hardware-Sicherheitstechnologie, Kryptologie sowie Netzwerk- und verteilte Systeme. Auf sie entfallen zusammen 174 VZÄ. Im Gegensatz dazu kommen die fünf am wenigsten erforschten Bereiche, wie Sicherheitsmanagement und Governance, zusammen auf nur 7.2 VZÄ. Gemessen an der Zahl der beteiligten Hochschulen ist der Forschungsbereich Netzwerke und verteilte Systeme am beliebtesten – nicht weniger als neun Hochschulen sind in diesem Bereich aktiv.

Die Studie liefert eine wichtige Datenbasis für politische Entscheidungsträgerinnen und Entscheidungsträger, Hochschulen und Interessengruppen aus Industrie und Förderinstituten. Nun können Ungleichgewichte diskutiert, strategische Bereiche gezielt gestärkt und mögliche blinde Flecken identifiziert werden, mit dem Ziel, die Schweiz als eines der führenden Länder in der globalen Cybersicherheitslandschaft zu positionieren.



Anzahl der Schweizer Universitäten und Gesamtressourcen in FTE, die für jeden Forschungsbereich bereitgestellt werden. (TF: Theoretische Grundlagen; IH: Incident Handling and Digital Forensics; AA: Assurance, Audit, and Certification; IM: Identity Management; SM: Security Measurements; MG: Security Management and Governance; ST: Steganography, Steganalysis and Watermarking)

3. Studierende & Fellows

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 an. Im Jahr 2023 konnten 39 Studierende ein Praktikum beim Cyber-Defence Campus absolvieren. Die Praktikantinnen und Praktikanten stammen aus verschiedenen Hochschulen.

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 an der EPFL, nahe der ETHZ sowie auf dem Campus in Thun durch. Im Jahr 2023 wurden Arbeiten von 28 Studierenden durch den CYD Campus begleitet.

CYD Fellows

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

Die neuen CYD Proof-of-Concept-Fellowship zielen insbesondere darauf ab, angewandte Forschung zu unterstützen, die zu einem innovativen Produkt oder einer Dienstleistung führt, mit der Absicht, einen echten Einfluss auf die Cyberverteidigung in der Schweiz zu nehmen und das Potenzial für die Kommerzialisierung solcher Produkte oder Dienstleistungen zu bewerten.

Im Jahr 2023 waren **zwölf Fellows** aktiv:

Dr. Ana-Maria Cretu
CYD Postdoctoral Fellow
November 2023 – Oktober 2025
Projekttitel: Methods for the evaluation of technologies that promise privacy

Edoardo Debenedetti
CYD Doctoral Fellow
Juni 2023 – Mai 2027
Projekttitel: Real-world Machine Learning Security and Privacy

Guillaume Dubuis
CYD Master Fellow
Februar 2023 – Juli 2023
Projekttitle: Topological Data Analysis for Attack Detection in Energy Systems

Dr. Francesca Falzon
CYD Postdoctoral Fellow
Juli 2023 – Juni 2025
Projekttitel: Towards More Practical Encrypted Databases with Expressive Queries

Dr. Lucianna Kiffer
CYD Postdoctoral Fellow
September 2022 – August 2024
Projekttitel: Security and Usability of Blockchain Networks

Dina Mahmoud
CYD Doctoral Fellow
September 2020 – August 2023
Projekttitel: Attacks and Defenses on FPGA-CPU Heterogeneous systems

Louis-Henri Merino
CYD Doctoral Fellow
Juni 2022 – Mai 2024
Projekttitel: Coercion-Resistant Remote E-Voting Systems with Everlasting Privacy

Basil Ottinger
CYD Master Fellow
November 2023 – April 2024
Projekttitel: Towards Comprehensive Measurement of Global DNS Amplification Threats

Simon Sommerhalder
CYD Master Fellow
November 2023 – April 2024
Projekttitel: Challenges in Robust Detection of Attack Traffic

Alessandro Stolfo
CYD Doctoral Fellow
Januar 2022 – Dezember 2025
Projekttitel: Privacy-Preserving Learning of Neural Language Models

Simran Tinani
CYD Doctoral Fellow
September 2021 – August 2023
Projekttitel:
Nonabelian Groups in Cryptography

Jodok Vieli
CYD Master Fellow
Oktober 2022 – März 2023
Projekttitel: Systematization of DNS DoS: Attack Characterization, Mitigation and Measurement

Hochschulpraktikanten/-innen

Sami Abuzakuk

Khalid Aleem

Camille Arruat

Thomas Berkane

Cristian-Alexandru Botocan

Daniel Celeny

Victor Carles

André Charneca

Lucas Crijns

Isis Daudé

César Descalzo

Max Duparc

Marc Egli

Perceval Faramaz

Nicholas Sperry Grandhomme

Francesco Intoci

Sarah Ismail

Inan Kadioglu

Simon Kindhauser

Maxime Laval

Louis Leclair

Erik Wadell Ledin

Michiel Lüchinger

Léo Meynent

Valentin Mulder

Iana Peix

Octave Plancherel

Bruno Ploumhans

Guillaume Régnier

Evgueni Rousselot

Etienne Salimbeni

Martin Sand

Simon Sommerhalder

Igor Szymanowski

Alessandro Tavazzi

Andrea Alexis Thäler

Maxime Würsch

Marc Xapelli

Naima Zingg

Studierende

Patrick Louis Aldover

Dominique Alguacil

Robin Bisping

Marc Bollhalder

Sebastian Brunner

Isis Daudé

Luc Desmeules

Daniel Dorigatti

Kaya Ercihan

Timothy Felix

Silvan Flum

Sébastien Gillard

Valentin Huber

Jan Kreischer

Tobias Lüscher

Fabia Müller

Silvan Niederer

Pascal Schärli

Franklyn Sciberras

Oliver Senn

Benjamin Simmonds

Mihhail Sokolov

Simon Sommerhalder

Stefan Weber

Adrian Zanga

Qianjun Zheng

Vladyslav Zubkov

Doktorierende

Despoina Giarimpampa

Eric Jedermann

Giacomo Longo

4. Talentförderung

Dr. Lucianna Kiffer - Postdoctoral Fellow am CYD Campus und an der ETH Zürich

Welche Trends siehst du im Cybersektor in den nächsten fünf bis zehn Jahren als relevant an?

In dem Bereich, in dem ich arbeite, sehe ich einen wachsenden Trend hin zu mehr verteilten Anwendungen. Dazu gehört, dass der traditionelle Finanzsektor stärker in den Blockchain-Bereich integriert wird und diese miteinander verbundenen Netzwerke sich auf eine Zukunft hinbewegen, in welcher globale Nutzerinnen und Nutzer die Möglichkeit haben, schneller und kostengünstiger zu interagieren. Ich sehe auch einen Trend weg von zentralisierten Dienstleistenden und hin zu mehr Kontrolle der Nutzerschaft über die eigenen Daten und deren Verwendung.

Was ist in deinen Augen der wichtigste Beitrag des CYD Campus zu Cyberfragen?

Einer der wichtigsten Beiträge ist, dass die Studierenden Zugang zu sehr aktuellen Forschungsproblemen und der Infrastruktur erhalten. Sie haben die Möglichkeit, in verschiedenen Bereichen mit der physischen Infrastruktur, die der CYD Campus hat, zu forschen und zu arbeiten. Ebenfalls wichtig, ist die grossartige Unterstützung durch die Fachleute beim CYD Campus.

Auf welche Bereiche hast du dich bei deiner Arbeit als Fellow konzentriert?

Durch die Zusammenarbeit mit der ETH und der Betreuung von Master- und Bachelorarbeiten beschäftige ich mich mit einer Vielzahl von Themen. Generell beschäftige ich mich aber mit der Benutzerfreundlichkeit von Kryptowährungs- und Blockchain-Systemen. Dies beinhaltet die Messung der Netzwerke, auf denen diese Systeme basieren, die Untersuchung von Details auf Protokollebene und auch die Messung, wie neue Protokolle veröffentlicht werden und wie diese Protokolle das gesamte System und seine Benutzerinnen und Benutzer beeinflussen. Aber im weiteren Sinne interessiere ich mich sehr für Peer-to-Peer und dezentrale Netzwerke im Allgemeinen, nicht nur in ihrer Anwendung auf Blockchain-Systeme.

Was waren die bisherigen Höhepunkte deines Fellowships?

Eines der Highlights war, dass ich vor etwa einem Jahr, ein paar Monate nach Beginn meines Fellowships, an einem Workshop zum Thema dezentralisierte Finanzen teilnehmen und dort einen Vortrag halten konnte. Dabei ging es darum, dass Forschende eine Woche lang an einem abgelegenen Ort zusammengekommen sind und gemeinsam an Problemen gearbeitet haben. Dadurch begann ich eine Zusammenarbeit mit Personen von verschiedenen Universitäten, die immer noch andauert. Das war wirklich grossartig. Der Zugang zu solchen Gelegenheiten ist eindeutig ein Highlight. Denn er bietet die Möglichkeit, sich mit verschiedenen Studierenden, Absolventinnen und Absolventen sowie Doktorierenden international zu vernetzten, die grossartige Arbeit leisten, und die Möglichkeit, ihre Arbeit mit ihnen zu erforschen.

Welche spannenden Forschungsthemen und Fragen siehst du für potenzielle neue Fellows?

Generell arbeite ich in einem Bereich, in dem es für Forschende immer wie mehr Fragen gibt, da sich die Dinge ständig ändern und immer mehr Protokolle und Messungen benötigt werden. Ein Thema, das ich als interessantes Forschungsgebiet für den CYD Campus sehen würde, ist die Tatsache, dass immer mehr Institutionen mit Kryptowährungen und Blockchain-Protokollen arbeiten und interagieren und ihre eigenen Versionen von genehmigten Systemen erstellen, um mit bestehenden Systemen zu interagieren.

Warum würdest du das Fellowship empfehlen?

Meine Erfahrung war, dass man unglaublich viel Forschungsfreiheit erhält, die man sonst vielleicht nicht hätte. Auch die Verbindungen zwischen den Forschungszentren und den Universitäten bieten viele Ressourcen und die Möglichkeit, sich mit verschiedenen Personen auszutauschen - das ist sehr wertvoll.

Simon Sommerhalder - CYD Master Fellow von der ETH Zürich

Wie hast du die Bewerbung für das CYD Fellowship empfunden?

Rückblickend betrachtet war es schon ein grosser Aufwand, aber es hat sich auf jeden Fall gelohnt. Mittlerweile ist es wahrscheinlich einfacher geworden, da die Registrierungsplattform vor einem Jahr noch in den Kinderschuhen steckte.

Über welches Thema schreibst du deine Arbeit?

Meine Arbeit beschäftigt sich mit der Frage, ob man mit Trojanern infizierte Geräte über ihren Netzwerkverkehr erkennen kann. Dies ist sehr herausfordernd, da praktisch alle Anwendungen, Viren und Trojaner inklusive, ihren Netzwerkverkehr verschlüsseln. Wir versuchen deshalb, mittels Künstlicher Intelligenz Verhaltensmuster festzustellen, die diese Trojaner gemeinsam haben und sie von anderen Programmen unterscheiden.

Was hat dich beim CYD Campus angesprochen, um deine Arbeit hier zu schreiben?

Bevor ich die konkrete Stelle hatte, wusste ich bereits, dass ich ein Projekt auf dem Gebiet «Network Intrusion Detection» machen wollte, da dieses Thema beinahe alle meine Interessen und Studiumsschwerpunkte abdeckt. Als ich auf der Suche nach einer Masterarbeit war, bin ich im Internet auf die CYD Campus Konferenz gestossen, habe aber leider kein Ticket mehr bekommen. Einen Tag danach habe ich dann Bernhard Tellenbach vom CYD Campus an einem Event der Cybergroup der ETH kennengelernt und so ist dann alles ins Rollen gekommen. Bernhard ist jetzt übrigens auch mein Betreuer.

Welche spannenden Einblicke hast du bisher erhalten?

Es ist mir vor allem bewusst geworden, wie vielseitig das Gebiet der Cybersicherheit ist. Durch die verschiedenen Events des CYD Campus durfte ich Einblicke in viele Forschungsarbeiten bekommen. Spannend fand ich dabei vor allem auch die Forschung, die der CYD Campus auf dem Gebiet von LLMs und deren Gefahrenpotential durchführt. Ein Highlight war zudem, dass ich an einem Hackathon teilnehmen durfte, an dem wir die Cybersicherheit von verschiedenen Automodellen überprüften.

Wie findest du den Austausch mit deinen Betreuern?

Ich finde den regelmässigen Austausch mit meinen Betreuern sehr wertvoll. Es ist zwar teilweise auch unangenehm, da man nicht immer gleicher Meinung ist, aber genau deshalb der ideale Ort, um persönlich weiterzukommen und mich auf die Arbeitswelt vorzubereiten. Ich bin sehr dankbar für die verschiedenen Personen, mit denen ich hier zusammenarbeiten darf.

In welche Richtung möchtest du dich in Zukunft entwickeln und wie hilft dir der CYD Campus dabei?

Ich weiss noch nicht, was ich nach der Masterarbeit machen werde. Bisher habe ich die Erfahrung gemacht, dass sich zur gegebenen Zeit die richtige Tür auftun wird. Dass der CYD Campus massgebend daran beteiligt sein wird, ist nicht auszuschliessen, da ich hier viele verschiedene Personen und Firmen kennenlernen durfte.

5. Cybersicherheit

Die Forschung am CYD Campus stellt eine Investition dar, um das erforderliche Fachwissen und die wissenschaftlich-technischen Fähigkeiten für die Aufgaben des Bundes im Cyber-Defence-Bereich nachhaltig zu sichern. Als wichtiger Bestandteil des Technologiemanagements dient sie der Erstellung detaillierter Pläne für zukünftige Technologien und Innovationsprojekte des VBS. Diese Forschung trägt zur Entwicklung notwendiger operationeller Fähigkeiten in der Cyber-Verteidigung bei und unterstützt wissenschaftlich-technische Planungen und Anschaffungen im VBS. Die Forschungsprojekte werden in Kooperation mit Universitäten sowie Industriepartnerinnen und Industriepartnern realisiert.

Quantensichere Kryptographie

Die fortschreitende Forschung im Bereich Quantencomputer birgt kryptologische Risiken. Bisherige digitale Signaturverfahren (Digital Signature Schemes) und asymmetrische Kryptosysteme (Public Key Encryption), die gegenüber klassischen Computern sicher sind, können durch Quantencomputer gebrochen werden.

Aus diesem Grund hat das National Institute of Standards and Technology (NIST) in den letzten Jahren die Erforschung und Standardisierung von kryptographischen Verfahren vorangetrieben, von denen angenommen wird, dass sie gegen solche Angriffe sicher sind. Im August 2023 hat das NIST nun für drei der vorgeschlagenen Verfahren, die es für ausreichend ausgereift für eine Standardisierung hält, entsprechende Entwürfe zur Veröffentlichung als Federal Information Processing Standards (FIPS 203 auf der Basis von CRYSTAL-KYBER, FIPS 204 auf der Basis von CRYSTAL-Dillithium und FIPS 205 auf der Basis von SPHINCS*) veröffentlicht. Andere Verfahren benötigen laut NIST mehr Zeit für die Evaluierung, insbesondere die rund 40 neuen Signaturverfahren, die im Rahmen eines Aufrufs zur Einreichung weiterer Verfahren im September 2022 bis Juni 2023 eingereicht wurden. Ziel des Projekts ist es, die Sicherheit der vorgeschlagenen Verfahren zu untersuchen und Methoden zur Kombination von klassischen und quantensicheren Verfahren zu erforschen.

In diesem Jahr lag der Schwerpunkt auf der vertieften Untersuchung der Sicherheit von codebasierten Verfahren (z.B. Finalist «Classic McEliece» und «BIKE») und von Verfahren, die auf multivariaten Polynomen basieren. Hinsichtlich der Kombinationsverfahren wurden der aktuelle Stand der Forschung sowie aktuelle und geplante Standards für Multi-Key Encryption und Multi-Key Signature Schemes untersucht.

Sichere und souveräne Smartphone Plattformen

Ein Smartphone besteht aus Modulen und Produkten einer Vielzahl von Software- und Hardwareanbietenden. Soll ein Smartphone für die Speicherung und Verarbeitung von sensiblen Daten, z.B. für klassifizierte Daten, genutzt werden, erfordert dies ein hohes Mass an Vertrauen in viele oder bestenfalls alle dieser Anbietende. Moderne Smartphone-Plattformen bieten heute jedoch zunehmend Möglichkeiten, dieses Vertrauen im Idealfall auf einzelne Anbieterinnen und Anbieter zu reduzieren, z.B. auf Hardwareherstellende zur Realisierung sogenannter «Trusted Execution Environments» (TEE). Ziel des Projektes ist es, die Möglichkeiten und Grenzen aktueller TEE-Technologien zu untersuchen und eine Lösung für die nahtlose Integration bestehender Smartphone-Ökosysteme („unsichere Welt") und hochsensibler Anwendungen („sichere Welt") vorzuschlagen. In diesem Jahr wurde ein erster Prototyp auf einem aktuellen Smartphone implementiert. Während die vorgeschlagene Lösung prinzipiell funktioniert, müssen im nächsten Jahr noch einige Herausforderungen in den Bereichen Performance und Zugriff auf Peripheriegeräte (z.B. Bildschirm und Netzwerk) gelöst werden, die von der sicheren und der unsicheren Welt gemeinsam geteilt werden müssen.

Sichere mobile Betriebssysteme

Die heute verbreiteten Smartphone-Ökosysteme Android und iOS bieten ein hohes Mass an Funktionalität und Flexibilität. Während Android und iOS für die Speicherung und Bearbeitung von nicht klassifizierten Daten breit eingesetzt werden, ist ein Einsatz im Bereich der klassifizierten Daten aktuell nicht oder nur sehr eingeschränkt möglich. Da jedoch ein Bedarf in der Schweiz besteht, wurde ein Projekt mit dem Ziel gestartet, mögliche Lösungen zur Deckung des Bedarfs zu identifizieren und zu untersuchen. 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 Komponenten. 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 der Herstellerin oder dem Hersteller zu trennen, um die Souveränität über die Anwendung zu gewährleisten und die Sicherheit zu erhöhen.

Sicherheitsanalyse von Firmware von mobilen Geräten

Software-Sicherheit ist ein wichtiger Baustein, um einen hohen Cyber Eigenschutz zu erreichen. Die Identifikation von Software-Schwachstellen, seien sie absichtlich (z.B. durch Kompromittierung der Supply Chain) oder unabsichtlich eingebracht, leistet hierzu einen wichtigen Beitrag. Während für die (automatisierte) statische oder dynamische Analyse von Applikationen bereits verschiedene Ansätze und Werkzeuge existieren, ist dies für andere Bereiche, wie z.B. die Firmware von mobilen Endgeräten und die darauf vorinstallierten (System-)Applikationen, nicht oder nur teilweise der Fall. In diesem Projekt werden daher neuartige Ansätze zur automatisierten Analyse von Firmware mobiler Geräte mit Fokus auf die dynamische Analyse untersucht, um das Risiko von Schwachstellen in Firmware zu minimieren. In diesem Jahr wurde eine systematische Literaturanalyse zum Stand der Forschung durchgeführt und ein Prototyp zum dynamischen Testen von vorinstallierten Android-Apps entwickelt. Der Prototyp umfasst einen Dienst, der vorinstallierte Apps aus einer Android-Firmware extrahiert und die extrahierten Apps in eine benutzerdefinierte Firmware einspielt.

Cybersicherheit in der Domotik und Gebäudetechnik

Die immer stärkere Vernetzung und Digitalisierung der Gebäudetechnik macht diese zunehmend zu einem interessanten Angriffsziel. Um die Chancen und Risiken aktueller und zukünftiger Technologien in diesem auch als Domotik bezeichneten Bereich besser zu verstehen und ihnen proaktiv begegnen zu können, müssen diese untersucht und erprobt werden können. Ziel dieses Projektes ist es, die Voraussetzungen dafür zu schaffen. Dazu wurde in diesem Jahr mit der Planung, dem Design und der Implementierung einer Testbench für Gebäudeautomation begonnen. Die Testbench soll die in der Bundesverwaltung eingesetzten Building Automation and Control Systems (BACS) möglichst genau abbilden. Das im Projekt entwickelte Konzept umfasst verschiedene „Koffer", die einzelne Gebäudeautomationssysteme repräsentieren: Anlagenautomation, Raumautomation, Zählersysteme, Brandmeldesysteme, IoT, etc.. Jeder Koffer ist mit einem Backbone verbunden, der das technische Netzwerk darstellt. Im kommenden Jahr soll die Testbench implementiert und im Rahmen eines Hackathons einem ersten Härtetest unterzogen werden.

Cyber-Forensik in industriellen Kontrollsystemen

Während für klassische Windows- und Linux-basierte IT-Systeme eine Vielzahl von Werkzeugen und Anleitungen für die forensische Analyse von Cyber-Vorfällen zur Verfügung stehen, gibt es für das Umfeld industrieller Steuerungssysteme eher wenige Tools. Ziel des Projektes war es, effektive forensische Techniken und Werkzeuge für Operational Technology (OT)- und Umspannwerksautomatisierungssysteme zu identifizieren. Darüber hinaus wurde ein Schulungsmodul entwickelt und erfolgreich getestet, das Teilnehmenden mit unterschiedlichen Vorkenntnissen in die forensische Analyse im Kontext von OT-Umgebungen einführt. Es wurden Werkzeuge zur Durchführung von drei forensischen Aufgaben entwickelt und verfeinert: Artefaktsammlung und Festplattenanalyse, Analyse von IEC61850 Datenpaketen und Speicheranalyse.

Sicherheit von Wide-Area (grossräumigen) Netzwerken

Viele öffentliche und private Organisationen verwenden geografisch verteilte Netzwerke (Wide Area Networks, WANs), um ihre Standorte miteinander zu verbinden. Da diese WANs für den Betrieb der Organisation oft kritisch sind, ist ihre Sicherheit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit von entscheidender Bedeutung.

Um ein gutes Sicherheitsniveau zu erreichen, werden solche Netze häufig mit einer dedizierten Netzinfrastruktur aufgebaut. Dieser Ansatz ist jedoch sehr kostenintensiv. In den letzten Jahren neu entwickelte Technologien versprechen kostengünstigere und flexiblere Lösungen bei vergleichbarer Sicherheit. In diesem Projekt untersucht der CYD Campus, wie neue Technologien (z.B. SCION aus der ETH Forschung) und programmierbare Netzwerkarchitekturen (SDN / P4) für sichere WANs eingesetzt werden können.

Nachdem der CYD Campus im Jahr 2022 ein eigenes Testnetz mit SCION zwischen seinen drei Standorten aufgebaut hat, lag der Fokus in diesem Jahr auf der Weiterentwicklung von SCION in Zusammenarbeit mit der ETH Zürich und in der Kombination von SCION mit anderen Technologien (z.B. zur Verschleierung von Metadaten). Unter anderem wurde eine Erweiterung für SCION entwickelt, die es erlaubt, Netzwerkverkehr nur über Geräte mit bestimmten Eigenschaften zu senden. Dies ermöglicht es beispielsweise einer Organisation, den Verkehr zwischen ihren Standorten nur über Geräte zu senden, die mit der neusten Software ausgestattet sind und somit keine bekannten Sicherheitslücken aufweisen.

Automatisierung von Cyber-Defence Teams

Cyber-Angriffe werden immer zahlreicher, raffinierter und schwieriger zu erkennen. Dies macht es für die Verteidigenden schwierig, Schritt zu halten. Sie sind gezwungen, ihre Verteidigungsfähigkeiten so weit wie möglich zu automatisieren, um ihre Reaktionsfähigkeit und Effizienz zu verbessern.

In diesem Projekt untersuchen wir verschiedene Möglichkeiten, wie die Verteidigung von Cyber-Infrastrukturen automatisiert werden kann. Da die Entwicklung und Erprobung neuer Methoden direkt an realen Cyber-Angriffen schwierig und riskant ist, nutzen wir stattdessen eine jährlich stattfindende Cyber-Defence-Übung als Testumgebung. Bei dieser Übung mit dem Namen «Locked Shields» verteidigen etwa 25 Verteidigungsteams ihre Infrastruktur gegen zahlreiche Angriffe eines Angriffsteams. Normalerweise bestehen die Blue Teams (die Verteidiger) aus Fachleuten mit viel Erfahrung im Bereich Cyber-Defence. Gemeinsam mit Forschenden der niederländischen Militärakademie und des NATO CCDCOE untersucht der CYD Campus nun das Potenzial eines vollständig automatisierten Teams, das ohne menschliche Beteiligung an Locked Shields teilnehmen kann.

Während des diesjährigen Locked Shields wurden die Grundlagen für die Weiterentwicklung des «virtuellen» Blue Teams gelegt. So wurde das Grundgerüst des Teams implementiert und die Forschenden haben wichtige Daten für die Weiterentwicklung gesammelt. Ziel ist es nun, dass das virtuelle Blue Team im nächsten Jahr an Locked Shields teilnehmen kann. Es wird aber wohl noch einige Jahre dauern, bis es den Expertinnen und Experten der «traditionellen» Blue Teams ernsthaft Konkurrenz machen kann.

Automatisierung von Security Operation Centers (SOC)

Die rasante Entwicklung der Cybersecurity-Bedrohungen und die zunehmende Komplexität der Angriffe zwingen die Security Operation Centres (SOCs) dazu, innovative Ansätze zu erforschen, um ihre Erkennungs- und Reaktionsfähigkeiten zu verbessern. Das Security Operation Centre (SOC) ist nach wie vor die erste Verteidigungslinie gegen diese dynamischen und ausgefeilten Bedrohungen, was eine kontinuierliche Innovation und Anpassung erfordert. In diesem Zusammenhang hat die Integration von Künstlicher Intelligenz (KI) in SOC-Praktiken grosse Aufmerksamkeit erregt und verspricht, die Effektivität und Effizienz von Cybersicherheitsoperationen im Vergleich zur Anwendung regelbasierter Tools zu revolutionieren.

Angesichts der steigenden Nachfrage nach KI-gesteuerten Lösungen im Bereich SOC untersuchen wir, wo und wie KI zur Automatisierung und Vereinfachung der Prozesse dienen kann. Die diesjährige Übersichtsarbeit untersucht verschiedene Forschungsfragen und versucht, die vorherrschenden Trends und Anwendungsmuster zu identifizieren, indem sie den aktuellen Stand der Technik bei der Anwendung von KI in SOCs in einer Umfrage untersucht. Zudem werden Modelle auf der Basis von neuronalen Netzen und LLM experimentell anhand von historischen Daten untersucht.

Hacking Micro Drones

Unbemannte Luftfahrzeuge (Unmanned Aerial Vehicles - UAVs), auch Drohnen genannt, stellen eine Revolution im Sicherheits- und Militärbereich dar. Aufgrund der jüngsten Fortschritte bei der Miniaturisierung und der sinkenden Kosten sind Mini-UAVs auch im zivilen Bereich sehr populär geworden. Diese Drohnen können sogar mit tödlichen Waffen bestückt werden, wie man es im Krieg in der Ukraine beobachten kann. Zudem stellen sie für das Militär und die Sicherheitsbehörden eine Bedrohung dar, da sie mit leistungsfähigen Sensoren ausgestattet sind und zur Infiltration oder Datenerfassung über Sperrgebieten eingesetzt werden können. Militär und 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-UAVs zu erforschen, um die von ihnen ausgehende Bedrohung zu neutralisieren. Insbesondere wird untersucht, ob es möglich ist, die Kontroll- und Navigationskanäle durch fortgeschrittene Signalstörungs-, Signalspoofing- und Signalmanipulationsangriffe zu diesem Zweck zu nutzen. In diesem Jahr lag der Schwerpunkt auf komplexem Multi-Drohnen-GPS-Spoofing, das im Labor erfolgreich demonstriert wurde.

Automatische Exploit Generierung für den 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, mobilen- oder elektronischen Kleingeräten, etc.) verwendet werden. Durch diese weite Verbreitung ist der Linux Kernel ein interessantes Ziel für Angreiferinnen und Angreifer, die ein System kompromittieren wollen.

Im Rahmen eines gemeinsamen Forschungsprojektes mit IBM Research Zürich, wird an der Methodik geforscht, um zu beurteilen ob ein mögliches Fehlverhalten (engl. Bug) im Linux Kernel sicherheitsrelevant ist, d.h. effektiv ausgenutzt werden kann oder nicht. Die Beantwortung dieser Fragestellung ist unter anderem deshalb wichtig, da eine Vielzahl von offenen Bugs für den aktuellsten Kernel öffentlich zugänglich ist, und zur priorisierten Behebung von ausnutzbaren Bugs verwendet werden könnte.

Als Resultat der diesjährigen Forschungstätigkeiten wurde einerseits ein Forschungspaper erstellt, welches das bisher gewonnene Fachwissen im Bereich der Automatischen Exploit Generierung (AEG) in Bezug auf den Linux Kernel zusammenfasst. Anderseits wurde an einem Proof-of-Concept Tool weitergearbeitet, dessen Anwendbarkeit mittels ersten Kernel Bugs verifiziert werden konnte, für welche entsprechend Exploits generiert wurden. Eine Ausweitung der Anwendbarkeit auf weitere Bugs und Schwachstellenklassen ist für das kommende Jahr vorgesehen.

Ebenfalls wurde im Rahmen des Forschungsprojektes diesjährig ein neues Unterprojekt gestartet, welches automatisiert nach sogenannten Data-Only Angriffsvektoren suchen soll. Angriffe mittels Data-Only Techniken sind jüngst populärer gewordenen, da damit moderne Sicherheitsmechanismen des Linux Kernels (wie z.B. Control Flow Integrity - CFI) umgangen werden können. Die Funktionsfähigkeit des implementierten Ansatzes konnte bereits mit ersten Resultaten belegt werden, d.h. es wurden erste bisher unbekannte Kernel Objekte gefunden, deren Manipulation die Kapazitäten einer Angreiferin oder eines Angreifers erweitern können.

Schutz von unsicheren Avionik-Systemen

Dieses Forschungsprojekt befasst sich mit der Analyse von Schwachstellen in der Avionik-Hardware und den damit verbundenen Protokollen. In den vergangenen Jahren haben CYD Campus Forschende mit Hilfe des Avionik-Labors in Thun Angriffe auf die Technologien ADS-B (Automatic Dependent Surveillance–Broadcast), CPDLC (Controller-Pilot Data Link Communications) und FLARM sowohl theoretisch als auch in der Praxis analysiert. FLARM ist ein Kollisionswarngerät für Leichtflugzeuge und Drohnen, das in der Schweiz entwickelt wurde und weltweite Beachtung und Verbreitung gefunden hat. Im Jahr 2023 widmeten sich die Forschenden der praktischen Analyse des Kollisionswarnsystems TCAS (Traffic Collision Avoidance System), das in grösseren Flugzeugen eingesetzt wird. Es gelang ihnen, den ersten realistischen Angriff ausserhalb von theoretischen Betrachtungen und Simulationen zu zeigen. Ähnliches gelang in Zusammenarbeit mit Skyguide und Eurocontrol beim Thema CPDLC. Darüber hinaus wurden die Auswirkungen von Hochfrequenzstörungen des Global Positioning System (GPS) in Verkehrsflugzeugen, insbesondere nach dem Ausbruch des Ukraine-Krieges, untersucht.

Cyber in der Luft- und Raumfahrt

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

Im Bereich der Satelliten war der CYD Campus 2023 in verschiedenen Segmenten sehr aktiv. So wurde erstmals ein Angriff auf LEO-Systeme (Low Earth Orbit) gezeigt, der auch passive Nutzerinnen und Nutzer lokalisieren kann. Lokalisierung war auch ein Thema, um GPS-Interferenzen mittels Drohnen und Richtantennen aufzuspüren. Schliesslich wurden neue praktische Angriffe auf Bodenstationen entwickelt, die über die drahtlose Schnittstelle ausgeführt werden können, und die Hintergründe der stark zunehmenden Sicherheitsprobleme im Satellitenbereich wurden eingehend analysiert.

Der Faktor Mensch bei Sicherheit und Safety

Phishing-Angriffe werden immer raffinierter und zielen darauf ab, Menschen gezielt anzugreifen und kognitive Verzerrungen auszunutzen, beispielsweise durch die Vermittlung des Eindrucks von Autorität oder Dringlichkeit. Frühere Ansätze zur Benutzerschulung konzentrierten sich auf URL-Warnungen, textbasiertes- oder klickbasiertes Training und führten zu gemischten Ergebnissen. Für ein interaktiveres Training, das nicht an die Bildschirme der Benutzerinnen und Benutzer gebunden ist, untersuchen wir das Potenzial von Augmented Reality (AR)-Technologien zur Verbesserung der Phishing-Erkennung. Durch visuelle Darstellungen der Verzerrungen, die Angreifende typischerweise ausnutzen, und die haptische Interaktion der Benutzerinnen und Benutzer damit, soll das Training die Nutzerschaft in die Lage versetzen, kognitive Verzerrungen durch erhöhte Aufmerksamkeit und Misstrauen zu bekämpfen. In einer Laborstudie mit 100 Benutzerinnen und Benutzern haben wir die Phishing-Erkennungsraten, die Benutzerinteraktion und die Bewertung des AR-basierten Trainings im Vergleich zu einer klickbasierten Variante und einer Kontrollbedingung evaluiert. Unsere Ergebnisse zeigen, dass ein interaktives Phishing-Training, das kognitive Verzerrungen berücksichtigt, die Erkennungsraten um 33% erhöhen kann und dass interaktive Elemente gut wahrgenommen werden. Auch AR-Technologien verbessern das Training, jedoch sind weitere Forschungen notwendig, um dies zu bestätigen.

Sicherheit von elektrischen Fahrzeugen und Ladeinfrastrukturen

Im Zuge der Umstellung auf Elektrofahrzeuge im VBS muss auch die Sicherheit der bestehenden Ladeinfrastruktur überprüft werden. Vorarbeiten haben bereits gezeigt, dass bei gewissen Systemen mit Power Line Communication (PLC) der Datenfluss drahtlos aus der Ferne abgehört werden kann. Dies kann verschiedene Auswirkungen auf die Sicherheit und den Datenschutz von Fahrzeugen und Infrastruktur haben. Während des CYD Campus Car Hackathon in Thun im Oktober 2021 wurde ein aktiver Angriff auf ein Ladesystem entwickelt, bei dem ein sogenannter Denial-of-Service (DoS)-Angriff mit geringem Aufwand den Ladevorgang drahtlos unterbricht und beendet. Der Angriff mit dem Namen Brokenwire wurde dem National Cyber Security Centre (NCSC) gemeldet, und die beteiligten Forschenden stehen in Kontakt mit Fahrzeug- und Ladegeräteherstellern, um den Angriff zu entschärfen. Die Analyse solcher Angriffe und möglicher Gegenmassnahmen wurde im Laufe des Jahres 2022 durchgeführt.

Im Jahr 2023 wurden die Sicherheitsanalysen ausgeweitet. So untersuchten die Forschenden des CYD Campus mit ihren Partnerinnen und Partnern die Auswirkungen von drahtlosen Angriffen auf Batteriemanagementsysteme und eine Forschungsarbeit befasste sich mit der Sicherheit von Bluetooth-Systemen in zivilen Fahrzeugen. Auch ein Car Hackathon wurde wieder durchgeführt, bei dem gemeinsam die Firmware von Autos und Ladestationen mit modernen Fuzzing-Methoden untersucht wurde.

Self-Sovereign Identity (SSI) als Basis für nationale digitale Identität

Nach der Ablehnung des damaligen E-ID-Konzepts durch das Volk im Jahr 2021 hat der Bund eine öffentliche Vernehmlassung zum Zielbild E-ID durchgeführt. Eine Mehrheit der 60 teilnehmenden Kantone, Parteien, Hochschulen, Organisationen und Unternehmen hat sich für SSI als technologische Basis der neuen E-ID ausgesprochen. Der Bundesrat hat daraufhin einen Richtungsentscheid zugunsten von SSI gefällt und diesen Ansatz im neuen E-ID-Gesetz verankert. Auch die EU verfolgt im Rahmen von EIDAS 2.0 den Weg in Richtung SSI.

SSI ist ein neues Paradigma, das die Souveränität der Nutzerinnen und der Nutzer über ihre Identität und ihren digitalen Nachweis in den Mittelpunkt stellt. Zentrale Infrastrukturelemente, die die Handlungen einzelner Individuen kontrollieren, korrelieren und überwachen können, werden weitestgehend vermieden. SSI kombiniert viele Basistechnologien wie Blockchain-basierte Distributed Ledger (DLT), kryptographische Beweise über Identitätsattribute (Zero-Knowledge Proofs), PKI mit verteilter Schlüsselverwaltung sowie verschiedene Softwarekomponenten wie mobile Wallets und Agentinnen und Agenten, die in einem P2P-Netzwerk verbunden sind. Dementsprechend ist der Technologie-Stack von SSI sehr komplex und es gibt viele mögliche Ausprägungen.

SSI ist eine junge Technologie und die internationale Standardisierung ist noch im Gange. Damit SSI eine sichere technologische Basis für kritische Infrastrukturen wie den nationalen elektronischen Personalausweis werden kann, müssen verschiedene Aspekte erforscht werden. Dazu gehören die Sicherheit der Protokolle und der implementierten Systeme, die Skalierbarkeit für Millionen von Nutzerinnen und Nutzern, der Schutz der Privatsphäre und auch die Benutzerfreundlichkeit. Der CYD Campus hat sich dieses Jahr mit dem E-ID Team und der SSI Community der Schweiz vernetzt. Als Mitglied des Technical Advisory Circle analysiert er Technologien und berät FEDPOL und BIT bei technologischen Entscheidungen.

Offene Forschungsfragen werden im Rahmen eines PhD Fellowship und diverser Masterarbeiten in Zusammenarbeit mit Schweizer Hochschulen untersucht.

Sicherheit in 5G

Mit dem neusten Update für 5G-Netzwerke wird eine neue Sicherheitsfunktion namens Authentication and Key Management for Applications (AKMA) eingeführt. Diese Funktion zielt darauf ab, sichere Verbindungen zwischen Telefonen oder anderen Geräten und bestimmten Anwendungen herzustellen, indem die anfängliche Sicherheitsüberprüfung genutzt wird, wenn sich das Gerät mit dem Netzwerk verbindet.

Unsere Untersuchungen zeigen jedoch, dass AKMA in seiner derzeitigen Form einige schwerwiegende Schwachstellen aufweist, die von Angreifenden ausgenutzt werden könnten. Diese Schwachstellen könnten es jemandem ermöglichen, Kommunikationen mitzuhören und mitzuverfolgen, Daten abzufangen oder sogar herauszufinden, welches Gerät versucht, eine Verbindung zu einer Anwendung herzustellen. Wir haben diese Probleme identifiziert und Vorschläge gemacht, wie sie behoben werden können, um AKMA sicherer zu machen und diese Arten von Angriffen zu verhindern.

Ein Hauptproblem, das wir festgestellt haben, ist, dass die Kompromittierung einer Anwendungsfunktion in einem 5G-Netzwerk die Sicherheit aller Verbindungen zwischen Anwendungen und Geräten beeinträchtigen kann. Das bedeutet, dass Angreifende, die sich Zugang zu einem Teil des Netzes verschaffen, potenziell auf viele sensible Informationen zugreifen oder die Kommunikation abhören könnten. Es ist wichtig, dass diese Schwachstellen vor einer breiten Einführung behoben werden, um die Nutzerinnen und Nutzer und ihre Daten zu schützen.

Datenschutz bei Lawful Interception

Wenn Strafverfolgungsbehörden zur Unterstützung von Ermittlungen auf Informationen von Telefongesellschaften zugreifen müssen, nennt man das Lawful Interception (LI). In den neuesten 5G-Mobilfunknetzen gibt es neue Datenschutzfunktionen, die es den Strafverfolgungsbehörden erschweren, diese Informationen zu erhalten, ohne zu riskieren, dass sie in die falschen Hände geraten. Diese Studie stellt einen neuen Weg vor, wie Strafverfolgungsbehörden Informationen von Telefongesellschaften anfordern können, ohne die Privatsphäre zu gefährden. Sie verwendet eine spezielle Methode, die ein Gleichgewicht zwischen dem Erhalt der benötigten Informationen und der Wahrung der Privatsphäre im 5G-Netzwerksystem herstellt.

Lawful Interception ist eine gesetzliche Vorschrift für Kommunikationsdienstleistende (CSPs), die Strafverfolgungsbehörden (LEAs) beim Zugriff auf Netzwerkdaten für strafrechtliche Ermittlungen unterstützen. In den Mobilfunknetzen der 5. Generation (5G) stellt die Verbesserung des Datenschutzes bei den Netzwerkerkennungen eine Herausforderung für die LEAs dar, da sensible Informationen möglicherweise an nicht vertrauenswürdige CSPs weitergegeben werden. In dieser Studie wird ein System vorgestellt, das es LEAs ermöglicht, die Auflösung von Netzwerkkennungen von CSPs privat anzufordern. Das System verwendet ein neuartiges Protokoll, das die Abfrage von Informationen und die Berücksichtigung von Datenschutzaspekten ausgleicht und so die Leistung verbessert, während die Vertraulichkeit innerhalb der 5G LI-Infrastruktur gewahrt bleibt.

Diese Forschung bietet eine Lösung für Strafverfolgungsbehörden, um Lawful Interception im 5G-Kernnetz durchzuführen und gleichzeitig ihre Operationen vor nicht vertrauenswürdigen Kommunikationsdienstleistenden zu schützen. Durch ein neuartiges Verfahren zur Informationsbeschaffung optimiert das System das Gleichgewicht zwischen Datenschutz und Leistung. Experimente zeigen eine verbesserte Leistung bei der Auflösung von Identitäten bei gleichzeitigem Schutz sensibler Informationen, der Gewährleistung der Anpassungsfähigkeit an verschiedene Betriebsszenarien und der Verwaltung grosser Datensätze. Insgesamt geht diese Lösung auf die Datenschutzbedenken im Zusammenhang mit der Ermöglichung von LI innerhalb des 5G-Kernnetzes ein.

Die Forschung des CYD Campus befasst sich mit der Cybersicherheit von Flugzeugen

6. Data Science

Maschinelles Lernen und Künstliche Intelligenz haben einen festen Platz in unserer Gesellschaft eingenommen. Zahlreiche Algorithmen oder Tools sind inzwischen für die Allgemeinheit verfügbar. Ein Beispiel hierfür ist ChatGPT, das von vielen Menschen genutzt wird, um Texte zu erstellen oder Fragen zu beantworten. Der Bereich der Large Language Models (LLMs) hat sich in den letzten zwölf Monaten besonders entwickelt. Diese Modelle können in verschiedenen Situationen zur Unterstützung von Anwenderinnen und Anwendern eingesetzt werden. Wir dürfen deren Fähigkeiten jedoch nicht überschätzen oder blind den von ihnen generierten Antworten und Texten vertrauen. Die KI ist ein weiterer Bereich, der sich rapide entwickelt. Es stehen verschiedene Modelle zur Verfügung, um künstliche Bilder aus Texten zu erstellen. Beispiele hierfür sind Dall-E oder Midjourney.

In unserem Forschungsprogramm Data Science versuchen wir, Trends zu erkennen und deren Zukunftspotenzial in verschiedenen Anwendungsbereichen der Datenanalyse zu bewerten. Das Forschungsprogramm soll uns die notwendigen Fähigkeiten geben, unsere Partnerinnen und Partner aus dem VBS oder dem Rest der Bundesverwaltung beraten zu können, wie sie durch Datenanalyse Informationen gewinnen können, die ihnen einen Mehrwert für ihre Tätigkeit bieten. Je nach Art der Daten und der zu lösenden Aufgabe setzen wir verschiedene Methoden ein. Einige Fragen lassen sich mit statistischen Ansätzen beantworten, wohingegen andere Probleme fortschrittlichere Methoden wie Deep Learning erfordern. Zunächst gilt es, ein tieferes Verständnis in die Daten zu erhalten, da diese je nach ihrer Art, Strukturierung und Verteilung die zu wählende Vorgehensweise erheblich beeinflussen. Um unsere Fähigkeiten weiterzuentwickeln, arbeiten wir eng mit akademischen Partnerinnen und Partnern zusammen und nehmen viele Studierende (Master, PhD und Postdoc) auf. In diesem Kapitel greifen wir die wichtigsten Themen aus dem Bereich Data Science auf, die uns im Jahr 2023 beschäftigten.

Robustheit und vertrauenswürdige KI

Auswirkungen der Daten auf die Robustheit

In diesem Projekt geht es darum, neuronale Netze gegen feindliche Angriffe zu verteidigen. Wir erforschen die Auswirkungen struktureller Veränderungen. Dabei fokussieren wir uns darauf, welche Daten für das Training robuster Modelle verwendet werden sollten. Unsere Arbeit basierte auf folgenden **vier Ansätzen**:

Threshold Network: Aktivierungsfunktionen werden während der Testdauer modifiziert, um ein lokal lineares Verhalten zu erzeugen, das sich an biologischen Neuronen anlehnt. Ziel ist es, die Robustheit zu erhöhen, indem kleine Werte unterdrückt werden und somit deren Ausnutzung durch Angreifende verhindert wird. Dieser Ansatz ist zwar anfällig für die sehr kostenintensiven EOT (Expectation over Transformation-)Angriffe, aber es gibt einen Schwellenwert, ab dem sich die Robustheit des Modells gegen typische und weniger kostenintensive Angriffe (z.B. PGD, AutoAttack...) ohne zusätzliche Kosten und bei vergleichbarer Genauigkeit deutlich verbessert werden kann.

Feedback-Netz: Da die Label-Destillation die Robustheit eines Modells verbessert, wollen wir ähnliche Ergebnisse erzielen, indem wir die Bilder vorverarbeiten, um ihre Qualität zu verbessern. Eine separate Akteurin oder ein separater Akteur bewertet, welche Massnahmen zur Verbesserung der Bildqualität umgesetzt werden sollen, wobei die Verlustverbesserung als auch die Vorhersagekorrektur berücksichtigt werden. Unsere Experimente zeigen, dass Daten nicht bereinigt werden sollten, um sie dem Label besser anzugleichen, obgleich das Gegenteil hilfreich wäre.

Datengenerierung mit Diffusionsmodellen: Bei diesem Ansatz modifizieren wir Diffusionsmodelle, um mehr Robustheit durch anspruchsvollere Trainingsdaten zu erzielen. Bei diesem Ansatz werden während des Diffusionsprozesses Störungen durch Angreifende eingebracht. Es gelingt uns, neue Bilder zu erzeugen, die das Modell täuschen und sich deutlich von den Bildern unterscheiden, die ohne unseren Ansatz erzeugt wurden. Der einzige beobachtete Nachteil ist ein Anstieg von Out-of-Distribution (OOD-)Mustern, die nicht systematisch angegangen werden können.

Sampling im Einbettungsraum: Um die Generierung von OOD-Mustern zu vermeiden, arbeiten wir bei diesem Ansatz im Einbettungsraum und verwenden CRATE, ein linear trennbares Einbettungsmodell. Wir stellen fest, dass Samples, die sich in der Nähe der Grenze befinden, häufiger ein falsches Label tragen. Hinzu kommt, dass das Random Uniform Sampling im Einbettungsraum zu einer geringeren Bildvielfalt führt. Schliesslich zeigen wir, dass – anders als in der Literatur behauptet – die Robustheit nicht einfach durch Entfernen oder Hinzufügen anspruchsvoller Samples verbessert wird.

Gegnerisches verteiltes föderales Lernen

Föderales Lernen (FL) ist ein verteiltes Paradigma im Bereich des maschinellen Lernens (ML), das die Entwicklung von Modellen ermöglicht, indem es Daten von mehreren Entitäten nutzt und dabei deren Dateneigentümerschaft beibehält. Bei FL gibt es einen designierten Federator Node, welcher im Voraus bestimmt wird. Bei Distributed Federated Learning wird dieser Federator dynamisch bestimmt und kann über die Zeit ändern.

FL ist jedoch wegen seiner Verteilung, insbesondere bei dezentralem FL (DFL), anfällig für Angriffe von aussen. Daher konzentrieren wir uns auf neuartige Angriffe und Schutzmechanismen für DFL, die sowohl aus offensiver als auch aus defensiver Sicht notwendig sind. Unsere diesjährigen Aktivitäten waren in **vier Bereiche** unterteilt:

Die Entwicklung und Implementierung eines Moduls zur Robustheitsanalyse für eine DFL-Plattform (Fedstellar): Das Robustheitsmodul besteht aus i) der Komponente für bösartige Angriffe und ii) der Komponente für die Robustheitsaggregation. Es wurden mehrere bösartige Angriffe in die entsprechende Komponente integriert, darunter gezielte/ungezielte Label-Flipping-Angriffe, gezielte/ungezielte Sample-Poisoning-Angriffe, Backdoor-Angriffe und Model-Poisoning-Angriffe. Darüber hinaus wurden einige Protokolle zur Robustheitsaggregation, wie beispielsweise Krum, Median, Trimmed-Mean, FLTrust, Sentinel, SentinelGlobal in die Komponente für Robustheitsaggregations integriert, um die DFL-Plattform vor Poisoning-Angriffen zu schützen.

Die Entwicklung und Implementierung eines auf Moving Target Defense (MTD) basierenden Ansatzes zur Eindämmung von Poisoning-Angriffen auf DFL (Voyager): Voyager besteht aus drei Hauptkomponenten: einem Anomalie-Detektor, einem Netztopologie-Explorer und einem Verbindungs-Bereitsteller. Wird ein anormales Modell im Netz entdeckt, dann reagiert der Topologie-Explorer strategisch, indem er Verbindungen mit vertrauenswürdigeren Teilnehmenden herstellt, um das Modell zu schützen.

Die Entwicklung und Implementierung eines Protokolls zur Robustheitsaggregation für die Verteidigung von DFL gegen Poisoning-Angriffe (Sentinel): Sentinel nutzt die Zugriffsmöglichkeit auf lokale Daten und definiert ein dreistufiges Aggregationsprotokoll, bestehend aus Ähnlichkeitsfilterung, Bootstrap-Validierung und Normalisierung, um das Modell vor bösartigen Aktualisierungen zu schützen. Sentinel wurde mit verschiedenen Datensätzen sowie mit unterschiedlichen Arten von Poisoning-Angriffen und Bedrohungsstufen evaluiert und konnte dabei seine Abwehrfähigkeit gegen ungezielte und gezielte Poisoning-Angriffe gegenüber dem bisherigen Stand der Technik verbessern.

Die Bewertung der Robustheit gegenüber Poisoning-Angriffen für ein Federated Reinforcement Learning (FRL) Framework (Framework für föderales bestärkendes Lernen): Im Zuge dieser Arbeit wurde ein FRL-basierter Ansatz zur Eindämmung von Malware-Angriffen auf ressourcenbeschränkte Geräte entwickelt und prototypisch angewendet. Hierbei wurde FRL gründlich auf seine Robustheit analysiert.

Entwicklung einer vertrauenswürdigeren KI

Vertrauenswürdige KI ist ein aufkommendes Konzept, das mehrere bereits bestehende Grundsätze in sich vereint, wie zum Beispiel:

i) menschliches Handeln und Aufsicht
ii) technische Robustheit und Sicherheit
iii) Datenschutz und Datenverwaltung
iv) Transparenz
v) Vielfalt, Nichtdiskriminierung und Fairness
vi) gesellschaftliches und ökologisches Wohlergehen
vii) Verantwortlichkeit

Hierbei konzentrierten wir uns auf die Entwicklung neuartiger Lösungen zur Bewertung der Vertrauenswürdigkeit herkömmlicher Modelle für KI und föderales Lernen (Federated Learning - FL). Unser Fokus lag auf den folgenden **drei Hauptzielen**:

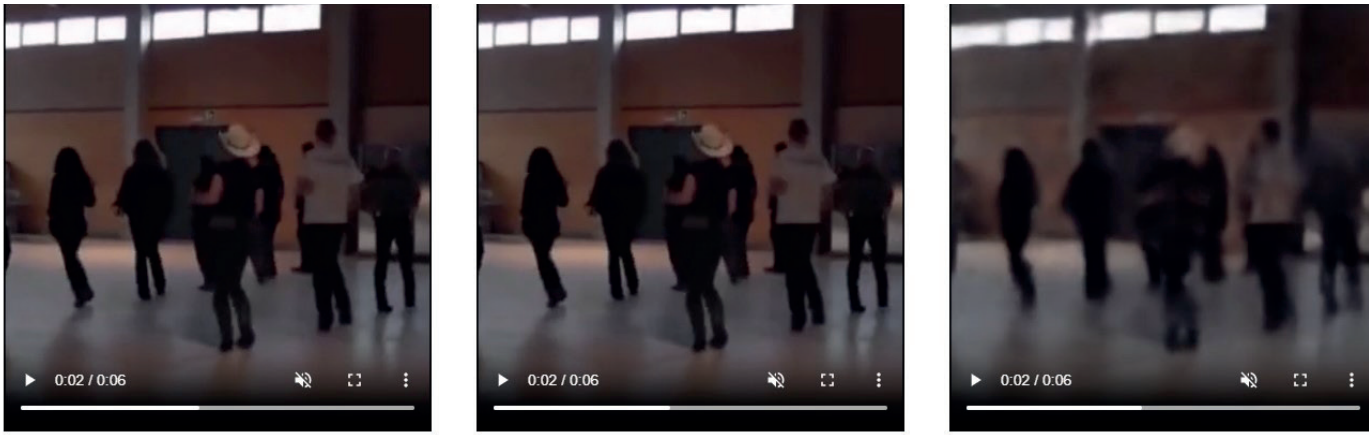
Vertrauenswürdigkeit des föderalen Lernens: Dazu wurde eine umfassende Taxonomie eingeführt, die aus sechs Säulen (Datenschutz, Robustheit, Fairness, Erklärbarkeit, Rechenschaftspflicht und Föderation) und über 30 Metriken zur Berechnung der Vertrauenswürdigkeit von FL-Modellen besteht. Danach wird ein Algorithmus namens FederatedTrust entwickelt, welcher auf den in der Taxonomie benannten Säulen und Metriken basiert. Ein Prototyp von FederatedTrust wurde implementiert und in den Lernprozess eines bewährten FL-Frameworks integriert. Abschliessend wurden fünf Experimente mit verschiedenen Konfigurationen von FederatedScope (mit unterschiedlichen Teilnehmern, Auswahlraten, Trainingsrunden und differentiellem Datenschutz) durchgeführt, um den Nutzen von FederatedTrust nachzuweisen.

Nachhaltiges und vertrauenswürdiges föderales Lernen: Hierbei wird die Säule der Nachhaltigkeit in die bisherige Taxonomie für vertrauenswürdiges FL eingeführt. Somit ist diese Arbeit die erste, bei der sämtliche Anforderungen erfüllt werden, die von einer Gruppe von KI-Fachleuten der Europäischen Kommission aufgestellt wurden. Die Säule der Nachhaltigkeit bewertet die Umweltauswirkungen des FL-Systems unter Einbeziehung von Begriffen und Metriken für Hardware-Effizienz, Komplexität der Föderation und Kohlenstoffintensität des Energienetzes. Im Anschluss wurde ein Algorithmus zur Bewertung der Vertrauenswürdigkeit von FL-Modellen entwickelt und implementiert, welcher die Nachhaltigkeit einbezieht. Umfangreiche Evaluierungen mit dem FederatedScope-Framework und verschiedenen Szenarien mit unterschiedlichen Föderationsteilnehmenden, Komplexitäten, Hardware und Energienetzen beweisen den Nutzen der vorgeschlagenen Lösung.

Bewertung von vertrauenswürdiger KI mit fehlendem Datensatz: In dieser Arbeit wurde ein Generator für synthetische Datensätze entwickelt, der den Vertrauenswert von Modellen mit fehlenden Daten berechnen soll. Die erarbeitete Lösung bietet zwei Möglichkeiten zur Generierung eines synthetischen Datensatzes (MUST und MAY), die sich in der Anzahl der statistischen Eigenschaften des Originaldatensatzes unterscheiden, welcher als Input dient, um den Kompromiss zwischen Datenschutz und Genauigkeit zu erreichen. Die Generierung des Datensatzes und die Bewertung der Vertrauenswürdigkeit wurden in zwei Szenarien getestet und bewertet. Die Ergebnisse von vier verschiedenen Vertrauensbewertungen (True Score, Limited Score, Advanced Score MUST und Advanced Score MAY) werden für jedes Bewertungsszenario verglichen, analysiert und erörtert.

Effizienz und Robustheit von Deep Learning-Algorithmen für Steganographie in Videodaten

Steganographie, d.h. das Verstecken von kryptographischen Signaturen in Medieninhalten (z.B. einem Video), kann heute mittels moderner Deep Learning-Algorithmen umgesetzt werden. Gerade im Bereich der Videodaten zeigen diese Algorithmen noch starke Limitierungen in Bezug auf deren Laufzeit (Effizienz) und Robustheit gegenüber verschiedensten Transformationen von Videos (z.B. Kompression bei Hochladen auf eine Social Media-Plattform). Im Fokus dieses Projekts standen Methoden, die genutzt werden können, um eine digitale Signatur in Videos zu verstecken. Durch eine solche Signatur ist es möglich, die Authentizität der Videodaten (d.h. deren Ursprung und Integrität des Inhalts) zu überprüfen. Mit dem Aufkommen immer leistungsfähigerer generativer KI zur Erzeugung synthetischer Videodaten und deren Einsatz im Kontext von Beeinflussungsoperationen nimmt die Bedeutung solch digitaler Signaturen zu. Offiziell produzierte Videoinhalte könnten so beispielsweise mit einer digitalen Signatur versehen werden, welche wiederum durch die Empfängerin oder den Empfänger elektronisch verifiziert werden kann.



Beispielanwendung eines effizienzgesteigerten Deep Learning-Algorithmus zur digitalen Signatur von Videodaten. Von links nach rechts: Originalvideo (cover video), Video mit versteckter digitaler Signatur (container video), Rekonstruktion von Videoinhalt aus versteckter Signatur. Letzteres kann genutzt werden, um allfällige Manipulationen des Inhalts zu detektieren.

In diesem Projekt wurde eine etablierte Methode zur Erzeugung von Videosignaturen erweitert, so dass die Signaturen auch nach Kompression durch gängige Algorithmen (z.B. H264-Kompression) erhalten bleiben. Zudem wurde ein Algorithmus entwickelt, der es erlaubt die Signatur für hochaufgelöste Videodaten zu generieren, wie sie für professionell produzierte Inhalte typisch sind. Damit konnte gezeigt werden, dass in Zukunft digitale Signaturen für Videodaten, die mittels Deep Learning erzeugt wurden, in Zeiten von Social Media ein potenzielles Werkzeug zur Wahrung derer Authentizität ist.

Generative KI

Erforschung von Deep Content Generation

In den letzten Jahren wurden immer leistungsfähigere Methoden zur Generierung von synthetischem Bild- und Videomaterial publiziert. Insbesondere sogenannte Diffusionsmodelle (z.B. DALL-E oder Stable Diffusion) sind mittlerweile in der Lage täuschend echte Bilder zu generieren und offerieren diverse Mechanismen zur Gestaltung des Resultats (z.B. über Eingabetext oder -bild). Vermehrt werden diese Methoden nun von Bedrohungsakteurinnen und Bedrohungsakteuren im Rahmen von Beeinflussungsoperationen eingesetzt. Bild- und Videomaterial wird erzeugt, um falsche Behauptungen glaubwürdiger zu machen und damit den Informationsraum nachhaltig zu beeinflussen.

In diesem Projekt wurde eine Bestandsaufnahme der momentan verfügbaren Methoden gemacht und aus der Sicht einer Bedrohungsakteurin oder eines Bedrohungsakteurs eine Reihe von Einsatzszenarien definiert. Dieser Katalog an Szenarien war die Grundlage zur Ableitung des Bedrohungspotenziales und Charakterisierung der Limitierungen der verfügbaren Algorithmen. Die Resultate dieses Projekts bieten die Grundlage für weiterführende Massnahmen zur Abwehr von Beeinflussungsoperationen mit synthetischen Bildinhalten (z.B. für Tabletop-Übungen, Entwicklung von Detektionsalgorithmen, etc.). Erkenntnisse aus diesem Projekt wurden zudem diversen bundesinternen Arbeitsgruppen zur Verfügung gestellt.

Chancen & Risiken von Generativer KI

Generative Künstliche Intelligenz (KI) umfasst Methoden, die i) in der Lage sind aus grossen Datenmengen Wahrscheinlichkeitsverteilungen zu schätzen und ii) darauf aufbauend neue synthetische Datenbeispiele generieren können. Diese Methoden bieten für die Cyberverteidigung der Schweiz sowohl Chancen als auch Risiken.

In der Regel sind moderne generative Modelle auf Datenquellen unterschiedlicher Modalitäten trainiert (z.B. Bild- und Textdaten). Damit können diese Modelle zunehmend flexibel auf verschiedenste Anwendungsszenarien massgeschneidert werden. Hervorzuheben ist hierbei die Auswertungsunterstützung von unterschiedlichen Datenquellen für die Beantwortung militärischer und nachrichtendienstlicher Fragestellungen. So können beispielsweise Satellitenbilder oder Audiodateien durch generative KI automatisch mit Tags versehen werden, welche den Inhalt der Daten charakterisiert, filtrierbar und durchsuchbar machen. Des Weiteren können generative Modelle auch genutzt werden, um versteckte digitale Signaturen in Dateien zu hinterlegen, die für Authentifizierungszwecke im Dienste der Informationssicherheit eingesetzt werden können.

Nebst diesen Chancen bringen diese Methoden aber auch neue Herausforderungen und Risiken für die Cyberverteidigung mit sich. Insbesondere Methoden zur synthetischen Generierung von Bild- und Videomaterial können von Bedrohungsakteurinnen und Bedrohungsakteuren für diverse Zwecke im Rahmen einer hybriden Kriegsführung eingesetzt werden. Eine Zunahme an KI-erzeugten Medieninhalten wird es für Bürgerinnen und Bürger zunehmend erschweren wahre von falschen/fiktiven Inhalten zu unterscheiden. Analystinnen und Analysten in militärischen und nachrichtendienstlichen Einheiten werden ebenfalls gefordert sein. Synthetisches Bild- und Videomaterial könnte in Zukunft von Bedrohungsakteurinnen und Bedrohungsakteuren zu Zwecken der militärischen Täuschung eingesetzt werden. Propagandamaterial kann zunehmend automatisiert, in grossem Stil produziert und über Kanäle in den sozialen Medien verteilt werden. Social Engineering kann durch den Einsatz von synthetischen Medieninhalten zusätzlich an Glaubwürdigkeit gewinnen und bringt den Faktor Mensch bei Cyberattacken weiter unter Druck. Erste Studien zeigen zudem subtile Beeinflussungsvektoren z.B. durch den Gebrauch von Textbausteinen, die mit Large Language Models erzeugt wurden, auf. Zusammenfassend lässt sich sagen, dass der Informationsraum in Zukunft vermehrt mit synthetischen Inhalten durchsetzt sein wird. Dabei wird die Unsicherheit darüber zunehmen, welche Quelle und Information als glaubwürdig angesehen werden kann.

Synthetische Bilderzeugung mit Stable Diffusion am Beispiel eines HIMARS Lenkwaffenwerfers. Von links nach rechts: Originalbild, Kantenbild (Canny-Edge Map), fünf verschiedene synthetische Beispiele. Das Kantenbild dient als Input für Stable Diffusion und garantiert, dass die Geometrie des Fahrzeugs möglichst erhalten bleibt. Stable Diffusion kann nun das Originalbild so verändern, dass das Fahrzeug in einer anderen Umgebung erscheint als auf dem Originalbild. Bedrohungsakteure könnten in Zukunft einen solchen Ansatz in Kombination mit einer gezielten Verbreitung über die sozialen Medien zur militärischen Täuschung einsetzen.

Verteiltes Lernen

Verteiltes föderales Lernen

Im Gegensatz zum konventionellen Ansatz des föderalen Lernens (FL), der auf einem zentralisierten Modell beruht, bei welchem eine einzige Entität Daten aus verschiedenen Quellen aggregiert, führt DFL die Aggregation über mehrere Knotenpunkte hinweg auf Peer-to-Peer-Basis durch. So werden die mit der zentralen Datenverarbeitung einhergehenden Risiken, wie z.B. einzelne Fehlerpunkte und Engpässe, verringert und damit der Datenschutz verbessert und die Systemrobustheit erhöht.

In diesem Framework haben wir eine neuartige Plattform namens Fedstellar entwickelt, die Wissenschaftlerinnen und Wissenschaftlern ein Tool zum Experimentieren mit DFL an die Hand gibt. Dank dieser innovativen Open-Source-Plattform können realistische DFL-Szenarien in virtuellen und physischen Geräten leichter erstellt werden, wobei ein Cluster von Raspberry Pis als zugrunde liegende Infrastruktur verwendet wird, um die Zusammenarbeit beim Modelltraining zu verbessern und gleichzeitig den Datenschutz zu gewährleisten. Die Tatsache, dass Fedstellar von mehr als 20 Forschenden in verschiedenen Einrichtungen genutzt wird, zeugt von seiner Effizienz und Benutzerfreundlichkeit. Ausgehend von dieser Plattform können wir nicht genug betonen, wie wichtig es ist, robuste Sicherheitsmassnahmen in das DFL-Framework zu integrieren und die kritischen Herausforderungen anzunehmen, welche das Internet der Dinge hinsichtlich des Datenschutzes und der Datensicherheit an uns stellt.

Darüber hinaus stellen wir ein innovatives, nahtlos in Fedstellar integriertes Sicherheitsmodul vor, in dem modernste Verschlüsselungs- und Moving Target Defense-Techniken kombiniert sind. Dieses Modul verbessert die Sicherheit von DFL-Netzwerken erheblich und belegt die Anpassungsfähigkeit und Widerstandsfähigkeit der Plattform gegenüber komplexen Cyberbedrohungen. Ein sehr wichtiger Beitrag, den wir mit Fedstellar leisten, besteht darin, Anwenderinnen und Anwendern die Erstellung massgeschneiderter Topologien zu ermöglichen, mit denen sie die dezentralisierte Aggregation von Modellparametern steuern und so die Effizienz und den Datenschutz von föderalen Lernprozessen verbessern können. Zukünftige Arbeiten werden sich mit der Untersuchung von Mobilität und adaptiven dynamischen Topologien auf der Grundlage von Reputationsbedingungen oder Modellähnlichkeit, der Erstellung von leichtgewichtigen Modellen und benutzerdefinierten Aggregationen sowie anderen Techniken zur Optimierung der Föderation befassen.

Schutz von IoT-Geräten

In der dynamischen und kontinuierlich wachsenden Welt des Internets der Dinge (IoT) stechen zwei unterschiedliche, sich jedoch ergänzende Forschungslinien im Bereich des individuellen IoT-Fingerprintings hervor: Identifizierung und Authentifizierung. Beide Forschungslinien verfolgen das gemeinsame Ziel, zusätzliche Sicherheit für Netze zu schaffen, indem innovative Identifizierungs- und Authentifizierungsmethoden herangezogen werden, die auf maschinellen und Deep-Learning-Techniken (ML/DL) basieren. Diese Forschungslinien gehen in zwei Richtungen. (1) Zunächst befassen wir uns mit dem komplexen Thema der Geräteidentifizierung in IoT-Netzwerken. Hierbei kommt eine LSTM-CNN-Architektur zum Einsatz, die das Leistungsverhalten der Hardware von IoT-Geräten anhand eines Zeitreihenansatzes analysieren und daraus lernen soll. Der Durchbruch dieser Forschungsarbeit liegt in der Erreichung einer herausragenden Identifizierungsgenauigkeit, was auf eine robuste Fähigkeit zur korrekten Identifizierung legitimer Geräte bei gleichzeitiger Minimierung falscher Identifizierungen hindeutet. Zudem wird in dieser Forschung die Resilienz der Architektur gegenüber Angriffen untersucht. Angesichts der immer ausgefeilteren Cyberbedrohungen ist dies ein wichtiger Aspekt. Das System zeichnete sich zwar durch seine Widerstandsfähigkeit gegen kontextbezogene Angriffe aus, wie z.B. solche, die auf Temperaturschwankungen beruhen, erwies sich jedoch als anfälliger für erweiterte ML/DL-Umgehungstechniken, wie MIM, BIM oder JSMA. Es wurden Gegenmassnahmen eingeführt, wie gegnerisches Training und Modelldestillation, um die Systemabwehr zu verbessern. Diese Massnahmen haben die Erfolgsquote der effektivsten Angriffe nachweislich drastisch gesenkt und somit die Sicherheit von IoT-Geräten gegen Umgehungsversuche erhöht, ohne die Leistung wesentlich zu beeinträchtigen. (2) Anschliessend konzentrieren wir uns auf die Authentifizierung einzelner IoT-Geräte. Der neue Denkansatz dieser Forschungsarbeit besteht im Einsatz von Transformer-Autoencodern, um für jedes Gerät eindeutige Fingerprints des Hardware-Verhaltens zu erstellen. Die innovative Verwendung von Transformer-Modellen, die sich besonders gut für die Verarbeitung von Zeitreihendaten eignen, ermöglicht es, die spezifischen Störungen und Schwankungen der Hardwareleistung zu erfassen und als zuverlässiges Mittel zur Authentifizierung zu nutzen. Eine hohe True-Positive-Rate (TPR) in Verbindung mit einer niedrigen False-Positive-Rate (FPR) belegt eindeutig, wie effektiv Transformer-Autoencoder zwischen authentischen und nicht authentischen Geräten unterscheiden können. Sie unterstreicht auch das Potenzial dieses Ansatzes, die Sicherheit und damit die Vertrauenswürdigkeit von Anwendungen innerhalb des IoT-Ökosystems erheblich zu verbessern.

Verarbeitung und Verstehen natürlicher Sprache

Chancen und Gefahren von grossen Sprachmodellen (Large Language Models - LLMs)

Die Sprachmodellierung, d.h. die Zuweisung von Wahrscheinlichkeiten zu den Token der natürlichen Sprache, ist schon seit geraumer Zeit eine Teilaufgabe zahlreicher Pipelines der Verarbeitung natürlicher Sprache (Natural Language Processing - NLP), beispielsweise in der maschinellen Übersetzung oder bei der Beantwortung von Fragen. Mit dem Aufkommen von Konversationsagenten wie ChatGPT (Ende 2022) ist sie jedoch ins Rampenlicht gerückt. Das Transformer-Modell mit seiner Encoder-Decoder-Architektur und Selbstaufmerksamkeit hat die Sprachmodellierung revolutioniert, wobei die Ära der grossen Sprachmodelle bereits 2018 mit dem ELMo-Modell begonnen hat. Wenngleich der Transformer ursprünglich für die neuronale maschinelle Übersetzung verwendet wurde, können Modelle, die nicht notwendigerweise eine solche Sequenz-zu-Sequenz-Transformation vornehmen, entweder nur den Decoder-Teil verwenden, wenn das Ziel das Verstehen der Textstruktur ist, oder den Encoder-Teil, wenn es um die Texterzeugung geht. Damit können diese Modelle für eine Vielzahl von NLP-Aufgaben eingesetzt werden, vorausgesetzt, dass die Pipeline gut definiert ist.

Die Textgenerierung, insbesondere in Konversationsumgebungen, scheint jedoch der interessanteste Anwendungsfall zu sein. Auch wenn LLMs eine bemerkenswerte Fähigkeit zur Generierung qualitativ hochwertiger Texte zeigen, so bleiben sie doch nur sehr clevere Rate-Algorithmen, die an einem immensen Umfang geschriebenen Textes trainiert wurden. Werden sie jedoch intelligent eingesetzt und mit Retrieval in Form von Retrieval Augmented Generation oder nicht mit Text, sondern mit anderen Datenmodalitäten gekoppelt, erschliesst sich ein enormes Potenzial. Bei den Modellen selbst handelt es sich jedoch nicht um Suchmaschinen oder Tools zur Überprüfung von Fakten, Wissensspeicher etc.. Sie generieren Ergebnisse aus den von den Daten gewonnenen Mustern, ohne deren Bedeutung zu verstehen. Das bedeutet, dass sie auch die in den Trainingsdaten enthaltenen Verzerrungen beibehalten oder die Informationen aus den Inputs speichern, was sie anfällig für die Preisgabe vertraulicher Daten, die Erzeugung unangemessener Inhalte oder Halluzinationen macht.

Erkennung von künstlich generiertem und irreführendem Text in sozialen Medien

Jüngste Fortschritte bei grossen Sprachmodellen wie ChatGPT – dem am schnellsten expandierenden Verbraucherprodukt aller Zeiten, haben gezeigt, dass von LLMs generierter Text auf den ersten Blick nicht von Text unterschieden werden kann, der von Menschen verfasst wurde. Die Tatsache, dass es nicht möglich ist, zwischen generiertem und von Menschen geschriebenem Text zu unterscheiden, birgt zahlreiche Gefahren in verschiedenen Bereichen. Eine dieser Gefahren ist beispielsweise die Fähigkeit automatisierter Bots, sich als Menschen auszugeben und die öffentliche Meinung durch schnell erstellte, irreführende Beiträge zu manipulieren, oder die Erstellung akademischer Texte, die von betrügerischen Autorinnen und Autoren als echt deklariert werden. Dieses Problem wird durch halluzinierende LLMs verstärkt, die falsche, aber kaum nachprüfbare Tatsachenbehauptungen aufstellen. Das Hauptziel des vorgeschlagenen Projekts besteht in der Entwicklung von Techniken zur Erkennung von Text mit Fehlinformationen, der von grossen Sprachmodellen generiert wird, sowie in der Untersuchung von persuasiven Beiträgen in sozialen Medien. Untersuchungen haben ergeben, dass die Mehrheit der Erwachsenen nicht unterscheiden kann, ob ein Text von Menschen geschrieben oder von einem LLM generiert wurde. Dies stellt uns vor zahlreiche Herausforderungen, angefangen von der Möglichkeit der betrügerischen Autorenschaft, bis hin zur automatischen Verbreitung gezielter Fehlinformationen. Die Effizienz und Eignung aktueller Detektoren zur Erkennung von LLM-generiertem Text ist nach wie vor ein aktiver Forschungsbereich. Für die effektive Bewertung solcher Erkennungssysteme ist ein anpassungsfähiger Benchmarking-Datensatz, der den Zustrom von LLMs bewältigen kann und verschiedene potenzielle Aufgaben abdeckt, unumgänglich. Ein Beitrag dieses Projekts ist nicht zuletzt die Einführung eines umfassenden Datensatzes, der für das Benchmarking von Detektoren für «Instruction-tuned»-LLMs zugeschnitten ist.

Effiziente Sprach- und Dialektidentifizierung für Sprachen, die in weniger verbreiteten Schriftsystemen geschrieben sind

In diesem Projekt konzentrieren wir uns auf die Erforschung von Lösungen zur Dialektklassifizierung in nicht-lateinischen Sprachen, mit besonderem Augenmerk auf die arabische Sprache. Ziel ist die Untersuchung der Möglichkeiten aktueller mehrsprachiger Modelle in nicht-lateinischen Sprachen. Die bisherigen vortrainierten Spracherkennungsmodelle konzentrieren sich hauptsächlich auf Englisch und lateinische Sprachen (alphabetische Schriften sind die häufigste Schriftart und werden in mindestens 85% der Sprachen verwendet). Weniger verbreitete Schriftarten können die Leistung mehrsprachiger Modelle erfahrungsgemäss beeinträchtigen, weshalb hier noch ein breites Forschungsfeld vor uns liegt. In einigen Fällen wird das Problem durch den Mangel an Ressourcen in den Zielsprachen (oder Dialekten) noch verschärft. Dies gilt insbesondere für Sprachen, die nicht das uns bekannte lateinische Alphabet verwenden. Arabisch, das eine Konsonantenschrift, auch Abdschad genannt, verwendet, wird von einer grossen Gemeinschaft von etwa 400 Millionen Menschen gesprochen, die über verschiedene Länder verteilt und in ihren regionalen Sprachvarietäten ausserordentlich vielfältig ist. Arabisch ist in 22 Ländern Amtssprache, deren Dialekte jedoch gegenseitig unverständlich sind. Gemeinsam werden sie auch als umgangssprachliches oder gesprochenes Arabisch bezeichnet, da sie nur in Gesprächen und mündlich verwendet werden. Die Hauptziele dieses Projekt bestehen in der Analyse der mehrsprachigen Modelle für nicht-lateinische Sprachen (in diesem Projekt Arabisch), der Untersuchung der aktuellen Lösungen für die Klassifizierung arabischer Dialekte sowie der Identifizierung und Entwicklung von Ansätzen zur Verbesserung ihrer Leistungen.

Bewertung der Robustheit eines Large Language Model gegenüber seinem Missbrauch in der Schweizer Cyberverteidigungslandschaft

Mit diesem Projekt sollen die ersten Grundlagen geschaffen werden, damit sich das Schweizer Cyberverteidigungssystem auf den gross angelegten Einsatz von LLMs und die mit einem solchen Einsatz verbundenen neuen Angriffspunkte vorbereiten kann. Hierdurch wird auch ein Beitrag zu den Aufgaben des CYD Campus geleistet, Mittel zur Abwehr neuartiger Cyberbedrohungen zu entwickeln. Um dieses Ziel zu erreichen, werden in diesem Projekt manuelles und automatisiertes LLM-Red-Teaming, das Screening von domänenspezifischem Wissen, die Bewertung von Verzerrungen bei der Generierung und selbstzensierte Generierung eingesetzt, um die Robustheit der aktuellen Generation von LLMs gegenüber Missbrauch bei offensiven Cyberoperationen zu bewerten.

Das Fine-Tuning der Konversationsagenten von LLMs verspricht die Lösung eines bei allen Benutzeroberflächen seit Langem bestehenden Problems: die Fähigkeit zu einer vollständig natürlichsprachlichen Konversation. Die Vorteile der Nutzung solcher Anwendungen sind zwar verlockend, sie bergen jedoch auch eine Reihe von Schwachstellen. LLMs sind dafür bekannt, dass sie anfällig für die Umgehung von Beschränkungen sind – sogenannte «Jailbreaks». Eine weitere LLM-Anwendung, die für viel Aufmerksamkeit und umfangreiche Präsentationen gesorgt hat, wurde durch ihre Text-to-Code-

Fähigkeiten ermöglicht. Sie wurde durch das Fine-Tuning der Konversationsagenten zugänglicher und durch weiteres grundlegendes LLM-Pretraining auf Code-Dokumentation–Code-Paaren – leistungsfähiger gemacht. Auch wenn alles darauf hinzudeuten scheint, dass einige State-of-the-Art (SotA)-LLMs ausreichend funktionale Codes generieren können, um in funktionsfähige Produkte aufgenommen zu werden, so wurde die allgemeine Robustheit dieser Codes gegenüber Cyberangriffen bisher nicht systematisch untersucht. Die Schaffung der Grundlagen für eine solche systematische Bewertung stellt ein weiteres Ziel dieses Projekts dar. Nicht zuletzt müssen Informationsoperationen, um in der Schweiz erfolgreich zu sein, eine wichtige Sprachbarriere überwinden. Ob dies durch den Einsatz von LLMs möglich ist, ist eine Frage, die dieses Projekt ebenfalls beantworten soll.

MAXIM: Verbesserung und Erklärung von NMT-Systemen

Dieses Projekt hat sich zum Ziel gesetzt, die Beschreibung der Anfälligkeit neuronaler maschineller Übersetzungssysteme (NMT-Systeme) zu erleichtern. Dabei soll verdeutlicht werden, wie wichtig es ist, starke Abwehrmechanismen und robustere NMT-Systeme für Anwendungen im echten Leben zu entwickeln.

In diesem Projekt stellen wir verschiedene Methoden vor, um Angriffe auf NMT-Systeme zu generieren. NMT-Modelle sind anfällig für sorgfältig geplante Störungen ihrer Inputs, sogenannte gegnerische Angriffe. Selbst dann, wenn das gegnerische Beispiel dem Originalsatz semantisch ähnlich ist, kann sich die Qualität der Übersetzung im Falle eines ungezielten Angriffs drastisch verschlechtern oder im Falle eines gezielten Angriffs zur Verwendung bestimmter Begriffe führen. Ungezielte gegnerische Störungen werden in diesem Projekt so angelegt, dass die gegnerischen Beispiele in der Ausgangssprache bedeutungserhaltend und in der Zielsprache bedeutungszerstörend sind.

Das Projekt sieht zwei Arten von gegnerischen Angriffen vor. Auf der einen Seite gibt es die optimierungsbasierte Methode zur Generierung von Störungen und auf der anderen Seite den an der Klassifizierung geleiteten Ansatz für Angriffe auf neuronale maschinelle Übersetzungen. Beide Methoden zeigen eine beeindruckende Erfolgsquote bei Angriffen sowohl in Black-Box- als auch in White-Box-Szenarien. Die so erzeugte Störung kann im Anschluss verwendet werden, um die zugrunde liegenden Modelle in Zukunft robuster zu machen.

Fit on Duty

Vorhersage von Zusammenbrüchen

Militärpersonal kann körperlich anstrengenden Situationen ausgesetzt sein, die sich aus einer Kombination von Faktoren wie Schlafmangel, anhaltender körperlicher Aktivität, psychischem und physischem Stress etc. ergeben. Um das Risiko von Unfällen und Verletzungen zu verringern, wäre es von Vorteil, über ein Warnsystem zu verfügen. Das sollte erkennen können, wann sich eine Person in einer solchen Situation befindet. Auf der Grundlage einer Bewertung des aktuellen Gesundheitszustands sollte es feststellen können, ob die Aktivität unterbrochen werden sollte und sich die Person erholen muss. Das Projekt «Fit on Duty» setzt sich zum Ziel, ein solches Warnsystem mit Hilfe von tragbaren Sensoren und maschinellem Lernen (ML) zu entwickeln. Die Sensoren erfassen die biomedizinischen Daten der Trägerin oder des Trägers (Herzfrequenz, Temperatur, Beschleunigung etc.), auf deren Grundlage ein ML-Algorithmus zur individuellen Bewertung des aktuellen Gesundheitszustands trainiert wird. Die diesjährige Erststudie ermöglichte es, praktische Erfahrungen mit der Erfassung biomedizinischer Daten von Militärpersonal zu sammeln und ein grundlegendes Verständnis für deren Qualität und die darin enthaltenen Informationen zu entwickeln. Die Studie brachte einige der logistischen und technischen Herausforderungen im Hinblick auf eine breit angelegte Anwendung eines solchen Warnsystems zu Tage und lieferte wichtige Erkenntnisse über die Anforderungen, die ein solches Warnsystem erfüllen muss.

Biomedizinische Edge-KI

In dieser Zusammenarbeit mit einer Schweizer Hochschule entwickeln wir als Machbarkeitsstudie ein tragbares Gerät, das in der Lage ist, den Gesundheitszustand seiner Trägerin oder seines Trägers zu beurteilen und in kritischen Situationen Warnungen auszusenden, um so im Idealfall Unfälle und Verletzungen zu vermeiden. Dieses Gerät kann, dank seiner Fähigkeit, mehrere Tage lang autonom zu funktionieren und die aktuell gesammelten Sensordaten zu analysieren, zu lernen und zu klassifizieren, in Echtzeit Aufschluss über den Gesundheitszustand seiner Trägerin oder seines Trägers geben. Zusätzlich kann es als Datensammler sowie als Rechenressource in einem verteilten Framework fungieren und ermöglicht bei Bedarf das Training komplexerer Modelle für maschinelles Lernen. Durch den Einsatz von Technologien wie IoT und eingebetteten Systemen sowie die Verwendung von Frameworks wie Edge-Computing und verteiltem ML zeigt diese Studie in einer Anwendung, wie durch die moderne Technologie das Risiko von Unfällen und Verletzungen verringert werden kann.

Deep Learning für Sicherheit

Bei der sich rasch entwickelnden Künstlichen Intelligenz sind grosse Sprachmodelle (Large Language Models, LLMs) zu Schlüsselelementen moderner computergestützter Linguistik und KI-Anwendungen geworden. Ihre beispiellosen Erfolge bei der Verarbeitung natürlicher Sprache haben nicht nur die Leistungsstandards durchbrochen, sondern auch ihre Integration in verschiedene Softwarelösungen vorangetrieben. Während die Industrie LLMs nutzt, um Benutzerinteraktionen zu verwalten und Entscheidungsprozesse zu automatisieren, bringt diese Integration neue Sicherheitsrisiken mit sich. Eine herausragende Bedrohung ist „Prompt Injection“, die von Sicherheitszentren weltweit intensiv untersucht wird. Im Gegensatz zu herkömmlichen Angriffen auf maschinelles Lernen kann dieser Angriff weitreichende Folgen haben, vom unberechtigten Zugriff auf private Informationen bis hin zur Ausführung von eingeschleustem Code. Bei einem Prompt-Injection-Angriff lenkt eine Angreiferin oder ein Angreifer das LLM von seiner beabsichtigten Aufgabe ab, indem ein speziell entworfener String eingeschleust wird, der stattdessen eine eingeschleuste Nutzlast ausführt.

Wir zeigen, dass motivierte Angreifende die Effektivität solcher Angriffe erheblich steigern können, indem mit Hilfe neuronaler Netze Trigger erzeugt werden, die auch in komplexen Prompts zuverlässig Nutzlasten aktivieren. Darüber hinaus laufen Forschungsprojekte, um die Robustheit und Sicherheit von LLMs gegen solche Angriffe zu untersuchen und möglicherweise zu erhöhen.

Dr. Gérôme Bovet begrüsst die Teilnehmer der CYD Campus Konferenz über KI in Bern

7. Technologie Monitoring

In der heutigen digitalen Welt entwickeln sich Cyber-Bedrohungen, die neueste digitale Technologien nutzen, schneller als je zuvor. Es ist eine Herausforderung, hinsichtlich der Aufklärung dieser Bedrohungen und der Bewertung ihrer potenziellen Auswirkungen auf dem neuesten Stand zu bleiben.

Missionsbeschreibung des Technologie Monitorings beim Cyber-Defence Campus:

Mission	Unsere Mission ist es, Trends im Bereich Cyber Technologien zu erkennen, zu überwachen, zu analysieren und vorherzusagen.
Vision	Unsere Vision ist es, ein in der Schweiz und im Ausland anerkanntes Technologieobservatorium zu werden.
Ziel	Unser Ziel ist es, Community-getriebene und in Massnahmen umsetzbare technologische Frühaufklärung für die nationale Sicherheit, die Sicherheitspolitik, die Marktforschung und das strategische Management zur Verfügung zu stellen.
Werte	Die Arbeit orientiert sich an unseren Werten und ist: wissenschaftlich, quantitativ, exklusiv, offen (Zugang, Quellen, Daten) und kollaborativ: Zusammenarbeit mit der akademischen Welt, der Industrie und der Verwaltung.

Unsere Missionsbeschreibung ist auf den im Jahre 2023 ausgelegten strategischen Zielen der Nationalen Cyberstrategie (NCS) ausgelegt, in deren Mittelpunkt die Analyse von Trends, Risiken und Abhängigkeiten steht.[1]

1 https://www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html

Die vorhergehende NCS für die Jahre 2018 bis 2022 unterstrich in Massnahme 1 die Bedeutung von «Früherkennung von Trends und Technologien und Wissensaufbau». Um dem zu entsprechen, richtet das Technologie Monitoring-Team (TM-Team) seine Anstrengungen auch an der Strategie Cyber VBS[1] aus und geht speziell auf die wichtige Aufgabe «Trendmonitoring und Unterstützung» ein. Dies beinhaltet die Durchführung gründlicher Technologie- und Marktbeobachtung, internationales Scouting von Startup-Unternehmen und die Pflege eines Kollaborations-Netzwerks mithilfe der folgenden Ansätze:

Ein wissenschaftlicher und quantitativer Ansatz

Traditionelles Technologie Monitoring stützt sich sehr stark auf manuelle und qualitative Methoden. Abweichend hiervon nutzen wir die neusten Fortschritte bei Big Data und Künstlicher Intelligenz, um nicht nur einen quantitativeren Ansatz zu ermöglichen, sondern auch prädiktive Verfahren zu integrieren und unser Technologie Monitoring damit zu verbessern. Unser Ansatz basiert im Wesentlichen auf Open Data und wissenschaftlichen Methoden.

Unser Technologie Monitoring liefert den folgenden Entscheidungsinstanzen in der Schweiz in Massnahmen umsetzbare technologische Frühaufklärung:

- Schweizer Armee (z. B. Chef der Armee, Armeestab, Kommando Cyber)
- Nationales Zentrum für Cybersicherheit (NCSC), neu Bundesamt für Cybersicherheit
- Bundesamt für Rüstung armasuisse

Darüber hinaus tragen die Aktivitäten des Technologie Monitoring Portfolios zu Cyber-Strategien auf verschiedenen Ebenen bei:

1. Nationale Cyberstrategie (NCS)
2. Strategie Cyber VBS
3. Gesamtkonzeption Cyber der Schweizer Armee
4. Business Architektur des CYD Campus

Ein Ansatz für eine exklusive Technologie- und Marktbeobachtungsplattform

Unser Ansatz basiert ausserdem auf unserer hauseigenen Plattform für die Technologie- und Marktbeobachtung (Technology and Market Monitoring, TMM), die wir in Zusammenarbeit mit der Industrie und Partnerinnen und Partnern aus der akademischen Welt entwickeln und pflegen. Unsere TMM-Plattform sammelt wertvolle Einblicke, die unsere Technologie-Analystinnen und -Analysten mit ihren eigenen Erkenntnissen und ihrer Scouting-Expertise zu umfassenden Analysen verknüpfen.

Large Language Models (LLM) im Bereich Cybersicherheit: Bedrohung, Exposition und Eindämmung

Eine durchgeführte Studie liefert einen Überblick über die Entwicklungen, den gegenwärtigen Stand der Technik und die Cyber-Defence-Implikationen generativer Sprachmodelle, sogenannter Large Language Models (LLM).

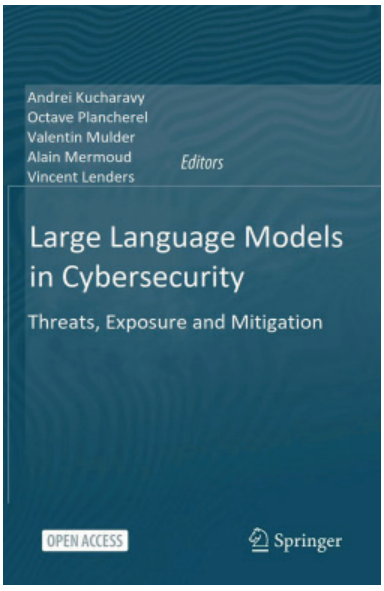
Diese öffentlich veröffentlichte Studie liefert der Industrie, der öffentlichen Verwaltung und der Wissenschaft in der Schweiz einen detaillierten Einblick in die Entwicklung und in die Risiken von LLM.

Die Studie fokussiert sich auf die Auswirkungen auf die Schweiz und auf die Entwicklung und den derzeitigen Stand der betreffenden KI-Modelle. Sie liefert Einblicke in deren Fähigkeiten und zukünftige Bedrohungen. Hier einige der Einblicke in die Studie:

• LLMs können aufgrund unausgewogener Daten beim Trainieren Fehlinformationen erzeugen. Andererseits kann diese Technologie auch für aktive Desinformationskampagnen missbraucht werden. Die Veröffentlichung privater Informationen stellt eine potenzielle Bedrohung dar. LLMs werden nämlich nicht nur mit öffentlich in Internet zugänglichen Daten trainiert, sondern auch indirekt mit Eingaben der Benutzerin oder des Benutzers ins System. Daher sollten keinerlei private Daten in LLMs eingegeben werden.

• Suchmaschinen mit LLM-Erweiterung können das Internet effizienter und tiefer durchsuchen. Dadurch können auch «versteckte» Informationen wie Datenbanken und Programmcodes im Deep Web – dem nicht gut indexierten und daher mit normalen Suchmaschinen nicht erkennbaren Teil des Internets – ans Licht gebracht werden.

• Viele der bekannten Bedrohungen im Cyberspace wurden mithilfe von LLMs einfacher zugänglich und skalierbarer. Um die Technologie vor Missbrauch zu schützen, muss die Verwendung von LLMs kontinuierlich überwacht werden. Die Menschen müssen über ihre Risiken aufgeklärt werden und es dürfen keine privaten Informationen eingegeben werden. Die vollständige Studie enthält eine detaillierte Analyse der LLM-Landschaft, der Grenzen von LLM sowie die Risiken dieser Technologie für die Cyber-Abwehr der Schweiz.



Vorschau des neuen Buches zu LLMs im Bereich Cybersicherheit, welches im Jahre 2023 im Rahmen des Technologie Monitorings erarbeitet wurde

1 https://www.vbs.admin.ch/de/sicherheit/cybersicherheit.html#dokumente

Erweiterung des TM-Teams

Die Technologie Monitoring Aktivitäten werden seit der Gründung des CYD Campus im Jahr 2019 kontinuierlich umfangreicher. Geführt wird das Team unter der Leitung von Dr. Alain Mermoud (vorne rechts im Bild). Valentin Mulder (vorne links im Bild) stiess Mitte 2023 nach einem erfolgreichen Praktikum aus dem CYD Talentprogramm im Vorjahr als Vollzeitmitarbeiter zum TM-Team. Im Oktober 2023 erhielt das Team mit Dr. Julian Jang-Jaccard (vorne in der Mitte im Bild), vormals Professorin in Neuseeland, weitere Verstärkung von wissenschaftlicher Seite.

Hochschulpraktikantinnen und Hochschulpraktikanten leisten einen zentralen Beitrag für das TM-Team und wirken an vielfältigen Projekten mit. Ein kurzer Überblick zu unseren Praktikanten und zu ihren Projekten (obere Reihe von links nach rechts):

Evgueni Rousselot
Quantum computer insights exploration

Daniel Celeny
Measurement of cyber risks and their costs for the equity markets

Maxime Würsch
Benchmark for technology mining using data extraction

Octave Plancherel
«Large Language Models in Cybersecurity» Buch

Martin Sand
«Trends in Quantum Technologies» Buch

Thomas Berkane
Emergence of cybersecurity technology from an evolutionary perspective

Die folgenden kurzen Interviews mit den beiden neuen Mitgliedern des TM-Teams vermitteln Einblicke in ihren jeweiligen Hintergrund und in ihre Beiträge.

Interview mit Valentin Mulder

An welchen Themen hast du während deines Praktikums gearbeitet?

Während meines Praktikums konnte ich an den verschiedensten Projekten arbeiten. Erwähnenswert sind drei besonders spannende Projekte. Zunächst war das Herausgeben und Koordinieren des Buchs «Trends in Data Protection and Encryption Technologies» eine gute Möglichkeit, um zu verstehen, wie der Cyber-Defence Campus mit Industrie, Universitäten und dem öffentlichen Sektor zusammenarbeitet. Das zweite dieser Projekte war die Startup Challenge, bei der ich gelernt habe, wie sich der Technologietransfer von innovativen Startup-Unternehmen in den Verteidigungssektor bewerkstelligen lässt. Und schliesslich habe ich die Scouting-Tätigkeit unterstützt und mir dabei ein Netzwerk aufgebaut.

Welchen allgemeinen Ratschlag würdest du künftigen Praktikantinnen und Praktikanten für ihre Zeit am Cyber-Defence Campus geben?

Sie sollen flexibel und offen sein, denn nur so können sie das Praktikum geniessen und ihr volles Potenzial erschliessen. Tatsächlich können Projekte, die zu Beginn nicht sehr interessant zu sein scheinen, oft auch spannende Herausforderungen bereithalten. Es ist auch ein grosser Vorteil, dass wir Büros in verschiedenen Städten haben. Das ist ein grosser Vorteil, der grossartige Chancen für den Aufbau eines Netzwerks bieten kann.

Aus welcher Motivation heraus hast du ein Praktikum am Cyber-Defence Campus angenommen?

Ich wollte im Bereich der Cyber-Abwehr arbeiten. Für mich sind Überlegungen, wie ein Staat seine Bürgerinnen und Bürger und seine kritischen Infrastrukturen in einem sich stetig verändernden technologischen Umfeld schützen sollte, ein ebenso komplexes wie spannendes Problem.

Wie hat dich dein Praktikum auf deine Vollzeitstelle am Cyber-Defence Campus vorbereitet?

Das Praktikum war die ideale Vorbereitung auf meine Arbeit. Ich hatte das Glück, eng mit meinem jetzigen Vorgesetzten zusammen zu arbeiten und habe viel von ihm gelernt. Ausserdem waren die Projekte, an denen ich gearbeitet habe, ein grossartiger Test. Diese beiden Faktoren haben mir einen guten Start bei meiner Arbeit für das TM-Team verschafft.

Welche Position belegst du derzeit, was gefällt dir daran am besten und inwieweit wurden deine Erwartungen an die Vollzeitstelle erfüllt?

Ich möchte drei verschiedene Aspekte herausgreifen. Zunächst einmal die Vielseitigkeit der Arbeit, die nie langweilig wird. Zum Zweiten können wir unsere Projekte gemäss den vorgegebenen Zielen selbständig durchführen. Wir sind dadurch sehr flexibel. Und schliesslich die schnelle Entwicklung des Cyber-Defence-Sektors. Es ist ausgesprochen spannend, mitten im Zentrum dieser Veränderungen zu sein.

Wo siehst du dich selbst in zehn Jahren?

Ich möchte weiter die Schnittstellen zwischen Cyber-Abwehr, technischem Fortschritt und deren strategischen Implikationen erkunden.

Interview mit Dr. Julian Jang-Jaccard

Erzähle uns etwas über deinen Hintergrund und deine bisherige berufliche Erfahrung.

Vor meiner Zeit am CYD Campus war ich Professorin und Leiterin des Cybersecurity Lab an der Massey University in Neuseeland. Zuvor war ich leitende Forscherin an der Commonwealth Scientific and Industrial Research Organization (CSIRO) in Australien. Zwischen meinem Abschluss in Computerwissenschaften und meiner Promotion arbeitete ich mehrere Jahre lang als professionelle Software-Entwicklerin.

Von welchen Kulturschocks, Erfahrungen oder Unterschieden zwischen deiner bisherigen Arbeit in Neuseeland und dem CYD Campus kannst du berichten?

Die Arbeit am CYD Campus ist wesentlich strukturierter und kundenorientierter als bei meinen bisherigen Stellen. Ein wichtiger Teil des Arbeitslebens am CYD Campus (oder ganz allgemein in der Schweiz) scheint die Pflege von Netzwerken zu sein, wozu auch viele Anlässe gehören. Ausserdem ist dies meine erste Erfahrung mit einer offenen Büroumgebung im Gegensatz zu Einzelbüros. Meiner Ansicht nach hat das sowohl Vor- als auch Nachteile.

Aus welcher Motivation heraus wolltest du am Cyber-Defence Campus arbeiten?

Ich habe mich beworben, weil ich hier meine Forschungen im Bereich Cybersicherheit, die ich schon seit 25 Jahren betreibe, fortsetzen kann. Der CYD Campus sagt mir als Arbeitgeber zu, weil er zur Bundesverwaltung gehört und ich der Ansicht bin, dass meine Arbeit somit auf nationaler Ebene höheres Gewicht erhält.

Welche Position besetzt du derzeit, was gefällt dir daran am besten und inwieweit wurden deine Erwartungen an die Vollzeitstelle erfüllt?

Ich bin wissenschaftliche Projektleiterin im Technologie Monitoring-Team (TM-Team). Am meisten freue ich mich über die Möglichkeit, im Rahmen neuer und disruptiver Technologien zu arbeiten und Zugang zu den besten Fachleuten der Schweiz und darüber hinaus zu haben.

Wo siehst du dich selbst in zehn Jahren?

In zehn Jahren möchte ich immer noch das tun, was mir am besten gefällt. Ich möchte im Bereich Cybersicherheit Forschungs- und Entwicklungsarbeit leisten, mit der nächsten Generation Cybersecurity-Expertinnen und -Experten interagieren und mit den Besten dieses Fachgebiets zusammenarbeiten.

Forschungsprojekte

Das TM-Team forscht aktiv mit verschiedenen Organisationen zusammen. Dazu gehören sowohl inländische als auch internationale Partnerinnen und Partner.

Benchmark für das Technologie-Mining mittels Datenextraktion

Durch die schnelle Entwicklung des Cybersecurity-Umfelds entstehen neue Bedrohungen für Organisationen, die sichere und zuverlässige Systeme betreiben müssen. Trends müssen daher in Echtzeit oder so zeitnah wie möglich nachverfolgt werden. Zu diesem Zweck werden verschiedene Methoden des Technologie Monitoring eingesetzt, insbesondere bibliometrische Trendanalysen. Am Anfang stand der Versuch, die Entwicklung der Technologien hinter LLMs mit bestehenden Methoden mittels Google Trends und OpenAlex zu beobachten. Die Ergebnisse zeigten jedoch, dass Standardmethoden nicht ausreichten. Daher wurde die Anwendung von Entitätsextraktoren auf spezifische Texte untersucht. Zunächst wurden bestehende Entitätsextraktoren mit Vorabdrucken in der Kategorie Computerwissenschaften (cs) auf arXiv untersucht, einschliesslich LLM-basierte. Die Ergebnisse legten nahe, dass die Entitätsextraktoren aufgrund der nicht-wissenschaftlichen Datensätzen, mit denen sie trainiert wurden, keine qualitativen Ausdrücke liefern, mit denen sich wissenschaftliche Artikel gruppieren lassen. Daher wurde eine Methode für die Extraktion relevanter zusammengesetzter Substantive implementiert, die sich auf die Struktur der Sätze und statistische Analysen stützt. Mit dieser Methode liessen sich die für Cybersicherheit relevanten arXiv-Listings präziser erkennen. Aus dem Ergebnis lässt sich schliessen, dass die Methode wichtige Erkenntnisse in einem sich schnell entwickelnden Bereich wie der Cybersicherheit liefert. Wir können somit annehmen, dass es möglich ist, Wissensgraphen zu entwickeln, mit denen sich die indirekten Auswirkungen von Technologien messen lassen.

Entstehung von Cybersicherheit-Technologien aus evolutionärer Perspektive

In der dynamischen Welt der Cybersicherheit laufen die Entstehung und Entwicklung von Technologien sehr schnell ab, sodass das gesamte Szenario kontinuierlichen Fluktuationen unterworfen ist. Traditionelle Methoden für das Monitoring neu entstehender Technologien und die Vorhersage künftiger Trends waren für den Umgang mit diesen schnellen Veränderungen nicht ausreichend ausgestattet. Um dem gerecht zu werden, zielte das Projekt auf die Entwicklung eines innovativen Ansatzes für die Beobachtung der Entwicklung von Cybersecurity-Technologien ab. Die Methode war durch die Evolutionstheorie inspiriert und beinhaltet Konzepte wie genetische Codierung, Mutationen und Anpassung. Um die Methode zu testen, wurde eine Untersuchung mit Code-Repositorien mit Bezug auf Cybersicherheit durchgeführt, wie den Plattformen, auf denen die sich in der Entwicklung befindenden Quellcodes gehostet werden. Durch die Analyse der Entwicklung dieser Repositorien aus dem Blickwinkel der neuen Methode konnten wichtige Mutationen erkannt werden, die die Entwicklung vorantreiben. Die gewonnenen Einblicke bieten die Gelegenheit, neu entstehende Repositorien vorherzusagen und solche zu erkennen, die künftig mit hoher Wahrscheinlichkeit an Bedeutung gewinnen werden.

Messung von Cyber-Risiken und deren Kosten für die Aktienmärkte

Angesichts der immer häufigeren und kostspieligeren Cyber-Angriffe werden Cyber-Versicherungen wichtig. Allerdings setzen die betreffenden Verträge ein eingehendes Verständnis der systemischen Cyber-Risiken in der Wirtschaft sowie der Cyber-Risiken auf Unternehmensebene voraus. Es gibt keinen leicht verfügbaren Score für Cyber-Risiken und nur wenige oder keine standardisierte Berichtspflichten für Cyber-Risiken, die sich zudem sehr schnell entwickeln. Daher liessen sich die Cyber-Risiken von Unternehmen bislang mithilfe traditioneller Methoden auf Grundlage historischer Daten und der Einschätzung von Fachleuten nur schwierig abschätzen. Um diese Situation zu verbessern, wurde ein maschinelles Lernmodell so trainiert, dass es die Cyber-Risiken börsennotierter Aktiengesellschaften anhand der Offenlegungen dieser Unternehmen quantifizieren kann. Durch Verknüpfung dieser Risikomessgrösse mit den Schwankungen der Aktienkurse ist es möglich, die Kosten der eingegangenen Cyber-Risiken für spezifische Unternehmen und die Gesamtwirtschaft zu bestimmen. Dieser Ansatz kann Cyber-Versicherinnern und -Versicherern, Regulatorinnen und Regulatoren sowie politischen Entscheidungsträgerinnen und Entscheidungsträgern helfen, Cyber-Risiken und deren Kosten besser einzuschätzen.

Wissenschaftliche und technische Beobachtung mit Flowatcher und die entsprechende Verfolgung der LLM-Entwicklung

Ziel der Studie war es, einflussreiche Veröffentlichungen zu erkennen, die die Analyse signifikanter Fortschritte in grossen generativen Sprachmodellen ermöglichen. Die durchgeführte Untersuchung sollte zu einem besseren Verständnis der potenziellen Auswirkungen der betreffenden Entwicklungen auf die neusten Technologien und demzufolge auch auf die Cyber-Abwehr in den kommenden Jahren führen. Traditionell werden für derartige Forschungen wichtige Plattformen wie ScienceDirect, Springer Link, die ACM Digital Library und die bibliographische Sammlung von DBLP durchsucht. Dieser Prozess arbeitet oftmals mit strukturierten Abfragen der betreffenden Datenbanken, um relevante Veröffentlichungen zu finden. Im Rahmen der vorliegenden Studie haben wir die Nützlichkeit von Flowatcher als unterstützendes Tool für den effizienten Ablauf dieser Aufgaben untersucht. Bei Flowatcher handelt es sich um eine Monitoring-Plattform, die es ermöglicht, Monitoring-Ergebnisse zu sammeln, zu verarbeiten und zu verbreiten. Flowatcher bietet verschiedene Arten von Monitoring-Tools, wie zum Beispiel Alarme, RSS-Feeds, Metasuchmaschinen oder das Hinzufügen von Feldbeobachtungen.

Supercomputer und Quantencomputing im Hinblick auf die Cybersicherheit unter Verwendung der Datenbank von Web of Science

Ziel der Studie war die umfassende Untersuchung der Entwicklungstrends bei Quantencomputing, Supercomputern und Cybersicherheit mittels einer integrativen bibliometrischen und szientometrischen Analyse. Im Rahmen der Untersuchung werden soziale Netzwerke analysiert und Keyword- und Cluster-Analysen durchgeführt, um komplexe Verknüpfungen innerhalb des wissenschaftlichen Fachbereichs zu erkennen. Mithilfe der Ergebnisse können zentrale Forschende erkannt werden, die an der Schnittstelle von Quantencomputing und Cyber-Sicherheit arbeiten. Sie liefern Einblicke in die Arbeiten der wichtigsten Akteurinnen und Akteure auf diesem Fachgebiet. Darüber hinaus lässt die Studie die weltweit wichtigsten Investorinnen und Investoren in die betreffenden Bereiche erkennen und leistet somit einen wichtigen Beitrag zum Verständnis der Forschungslandschaft.

Swiss Technology Observatory und Zusammenarbeit mit Swissintell

Das am Cyber-Defence Campus entstandene Swiss Technology Observatory[1] versammelt eine interdisziplinäre und internationale Forschergemeinde. Heute wird die Website des Swiss Technology Observatory gemeinsam mit Swissintell, der Swiss Association for Market Research, Competitive Intelligence and Strategic Planning (SMCS) gepflegt. Diese Zusammenarbeit führt insbesondere auf dem Gebiet des Technologie Monitoring zu zahlreichen Synergien.

Einblick in die Technologie Monitoring Konferenz

1 https://technology-observatory.ch/

CYD Campus Teammitglieder an der EPFL

Der Stand des CYD Campus an CONNECTED im August 2023, der grössten Armeeausstellung zum Thema Digitalisierung und Cyber in der Schweizer Armee

8. Innovation

Resultate der Innovationsprojekte

Sichere Smartphone Kommunikation über 5G/SCION/Threema

Unsere Innovationsvorhaben drehten sich um zwei Szenarien mit Schweizer Sicherheitslösungen: Ermöglichung der sicheren Kommunikation zwischen privaten Smartphones und einer internen Threema-Einrichtung über das SCION-Netzwerk und 5G.

Um diese Szenarien zu testen, wurde ein Threema-Server in den Räumlichkeiten vom Cyber-Defence Campus installiert, der nur über das SCION-Netz zugänglich ist. SCION (Scalability, Control, and Isolation On Next-Generation Networks) ist eine innovative Netzarchitektur, die mehrere Probleme der derzeitigen Internet-Architektur lösen soll. Es wird hauptsächlich von Forschenden der ETH Zürich mit dem Ziel entwickelt, ein sichereres, skalierbareres und zuverlässigeres Internet zu schaffen. Unsere Zusammenarbeit mit den Mobilfunkbetreibenden Swisscom und Sunrise ermöglichte es, unser Setup mit den Mobilfunkbetreibenden zu verbinden und eine nahtlose Benutzererfahrung zu bieten. Die kontrollierte Testumgebung ist eine wichtige Komponente bei der Bewertung der Sicherheit dieses Ansatzes.

Im Rahmen dieses Projekts haben wir auch eine Evaluierung durchgeführt, um die robusteste Architektur für ein sicheres Smartphone zu ermitteln. Dabei wurde die Praktikabilität der Verwendung eines Hypervisors zur gleichzeitigen Ausführung mehrerer Instanzen von Android auf modernen Smartphones demonstriert. Unsere Zusammenarbeit mit Partnerinnen und Partnern aus der Industrie und Studierenden der EPFL in den letzten zwei Jahren hat zu diesem Ansatz geführt, der die Risiken wirksam trennt.

Die Verfügbarkeit von sicheren Smartphones mit diesen Funktionen ist nun Realität geworden und stellt einen wichtigen Meilenstein in unseren Bemühungen dar.

Cyber Toolkit

Die Übung Locked Shields bietet eine perfekte Gelegenheit, neue Softwares und Konfigurationen zu testen, da die zu verteidigende Infrastruktur (die von den Organisatorinnen und Organisatoren zur Verfügung gestellt wird) repräsentativ ist und die durchgeführten Angriffe ebenfalls dem neuesten Stand der Technik entsprechen. In diesem Zusammenhang führten wir Proof-of-Concepts durch, bei denen wir verschiedene Softwares (sowohl COTS als auch massgeschneiderte) dem Blue Team der Schweizer Armee für Locked Shields zur Verfügung stellten, um sie während der Übung zu testen. Die verschiedenen Softwarekomponenten bieten eine Orchestrierung und harmonisierte Konfiguration von Cyber-Defence-Werkzeugen. Daraus folgt ein Cyber-Defence-System mit erweiterten proaktiven Anti-Virus-Malware-Funktionalitäten und Netzwerkaufklärung. Zu den wichtigen Funktionalitäten gehören beispielsweise automatisierte dynamische Malware Analysen, Antizipation durch vorgängige Analyse von C2-Kanälen, oder die Aufklärung und Überwachung von OT-Netzwerken und Web Application Firewall um Perimeter zu schützen. Die automatisierte defensive Endpunktverteidigung basiert auf KI.

Blue Team Automation

Das Projekt Blue Team Automation zielt darauf ab, Cybersicherheitsaufgaben zu automatisieren und ein autonomes System für Cyberverteidigungsübungen zu schaffen. Durch die Analyse von Locked Shields-Daten aus dem Jahre 2022 bewertet die Plattform die Sichtbarkeit und Erkennung von Red Team-Angriffen und entwickelt neue Cybersicherheitsmethoden. Ausserdem wird eine modulare Abwehrlösung entwickelt, die Warnungen, IT-Details und Massnahmen für eine schnelle Reaktion auf Bedrohungen integriert.

Durch den Zugriff auf Locked Shields-Daten und deren Konsolidierung konnten entscheidende Erkenntnisse über die Herausforderungen von Blue Teams gewonnen werden. Die automatisierte Plattform identifizierte Red Team-Aktivitäten, die zu umsetzbaren Warnungen für automatisierte Cybersicherheitsreaktionen führten. Diese umfangreiche Studie bietet umfassende Sicherheitseinblicke und stellt normalisierte Daten für eine breitere Forschungsnutzung und eine verbesserte Projekttransparenz bereit. Sie unterstreicht die Notwendigkeit von Ereignissen auf tieferer Ebene für die Verknüpfung von Warnungen und führt rationalisierte Methoden für Warnungen ein. Diese Errungenschaften ebnen den Weg für autonome Cybersicherheitssysteme, die die Angriffserkennung und -reaktion verbessern und die Modularität im Umgang mit Bedrohungen betonen.

Perimeter Überwachung mit automatischer Objekterkennung

Das Innovationsprojekt konzentrierte sich auf die Anwendung moderner Technologien des maschinellen Lernens zur zuverlässigen Objekterkennung in Überwachungsbildern. Ziel war es, ein funktionierendes Proof-of-Concept zu erarbeiten und Expertise im Bereich Machine Learning Operations aufzubauen. Die Initiative entstand aus der Notwendigkeit, militärische Flugplätze oder Waffenplätze auf potenziell störende Objekte wie Tiere oder Menschen zu überwachen. In kurzer Zeit wurde ein Minimal Viable Product (MVP) entwickelt und im Feld qualitativ getestet. Der Ansatz ermöglichte eine Echtzeit-Überwachung mit bestehenden Überwachungskameras und KI-Technologie, um drohende Gefahren auf einer 2D-Karte darzustellen. Das System wurde erfolgreich auf dem Militärflugplatz Dübendorf getestet und funktionierte unter verschiedenen Bedingungen zuverlässig. Das Projekt verbessert zudem das Wissen über KI in verschiedenen Bereichen der Armee. Es wird angestrebt, das System auf die automatisierte Kameraüberwachung auszuweiten und in Zukunft auch Wärmebild- und Infrarotkameras zu integrieren, um die Funktionalität weiter zu verbessern.

Cyber Startup Challenges

Smartphone Sicherheit

Die Cyber Startup Challenge fand dieses Jahr zum vierten Mal statt. Im Juni 2023 startete der CYD Campus seinen Aufruf zum Thema innovative Lösungen im Bereich «Sicherheit von Smartphone-Anwendungen und deren potenziellen Bedrohungen». Zehn Startups folgten dem Aufruf und präsentierten ihre Lösungen der Jury, welche aus Cyberfachleuten des VBS besteht.

Das US-amerikanische Startup Ostorlab überzeugte die Jury und durfte auf der CYD Campus Konferenz am 26. Oktober 2023 seine innovativen Ansätze zur Sicherheitsanalyse mobiler Anwendungen präsentieren. Ostorlab hat einen mobilen Applikationen Scanner entwickelt, der es Organisationen ermöglicht, Sicherheitslücken bei mobilen Anwendungen, sowohl bei Android- wie auch bei iOS-Anwendungen, effizient zu identifizieren.

Ostorlab setzt statische und dynamische Analysemethoden ein, um Schwachstellen zu identifizieren, die erhebliche Sicherheits- und Reputationsschäden für Unternehmen verursachen können. Diese reichen von Sicherheitsverletzungen, über Datenlecks bis hin zu kompromittierter Kommunikation. Weitere mögliche Schwachstellen sind unberechtigte Zugriffe, veraltete Softwarekomponenten, freiliegende sensible Informationen, schlechte Verschlüsselungspraktiken und unsichere Datenübertragungen.

Der Applikations-Scanner von Ostorlab Mobile unterstützt auch Software Bill of Materials (SBOM)-Dateien zur Erkennung veralteter und anfälliger Abhängigkeiten. Zudem verfügt der Scanner über automatisierte App-Interaktionen für umfassende Sicherheitstests und hat eine starke Erfolgsbilanz bei der Erkennung und Meldung kritischer Schwachstellen, was seine Effektivität unterstreicht.

Firmware Sicherheitsanalyse

Die Sicherheit vernetzter Geräte wie Gebäudesteuerungen, Zugangskontrollsysteme und Überwachungskameras stellt eine grosse Herausforderung dar, da diese Geräte oft nicht nahtlos in Überwachungsprozesse integriert werden können. Dies führt zu potenziellen Risiken durch unklare Sicherheitsstandards in lokalen Netzwerken.

Eine Lösung bietet die Firmware-Analyseplattform von ONEKEY, die Schwachstellen in Geräten aufspürt, ohne mit den sensiblen Netzwerken verbunden zu sein.

Während eines zehnmonatigen Proof-of-Concept im Rahmen der Cyber Startup Challenge 2022 hat der CYD Campus die Wirksamkeit der ONEKEY-Plattform auf die Probe gestellt. Es wurde ein Bewertungsschema entwickelt, mit dem vernetzte Geräte einfach klassifiziert und die Einhaltung von Mindestsicherheitsanforderungen dargestellt werden können. Während des PoCs wurden die Firmware-Images von mehr als 60 IoT-Geräten auf Schwachstellen und Compliance-Verletzungen analysiert. Dabei wurden zahlreiche Schwachstellen identifiziert und ihnen Common Vulnerabilities and Exposures Numbers (CVE-Nummern) vergeben.

Abschliessend wurden Prozesse rund um Patch Management, Vulnerability Management und Asset Management entworfen, um zu zeigen, wie eine solche Plattform auch automatisiert integriert werden kann.

Privacy-preserving Cyber Threat Intelligence Sharing

Die Arbeit mit dem Schweizer Jungunternehmen Decentriq, dem Gewinner der Cyber Startup Challenge 2021, wurde fortgesetzt. Der Fokus der Challenge lag auf dem Thema «Boost your Information Sharing and Analysis Center (ISAC)». Decentriq bietet eine Software-as-a-Service (SaaS) Plattform an, die eine sichere und private Datenzusammenarbeit ermöglicht. Decentriq bietet «Data Clean Rooms», die es ermöglichen, Ereignisdaten auszutauschen und anonyme Erkenntnisse zu gewinnen, ohne den Datenschutz zu gefährden. Decentriq verwendet eine «Confidential Computing» Technologie, um zu gewährleisten, dass niemand, einschliesslich der Plattformbetreibenden, direkten Zugriff auf die Daten hat. Die Plattform bietet somit eine Lösung für den Zielkonflikt zwischen der gemeinsamen Nutzung sensibler Daten und deren Schutz. Wir haben eine erfolgreiche Zusammenarbeit mit wichtigen Akteurinnen und Akteuren des Schweizer Finanzsektors abgeschlossen: Der Zürcher Kantonalbank, der Schweizerischen Nationalbank und SIX. Unser gemeinsamer Fokus lag auf sensiblen Cyberangriffsdaten, mit dem Ziel, die Sicherheit der kritischen Infrastrukturen unseres Landes zu stärken und gleichzeitig die Privatsphäre ihrer Daten zu schützen. Aufbauend auf diesem Erfolg bauen wir unsere Partnerschaft mit Decentriq weiter aus und streben die Umsetzung dieser Initiative im gesamten Finanzsektor an.

Dr. Colin Barschel (rechts im Bild) bei der Verkündung des Gewinners der Startup Challenge 2023

Gruppenbild des Ostorlab Teams, Gewinner der Cyber Startup Challenge 2023

9. Internationales Scouting und Kooperationen

Scouting

Im Jahr 2023 konzentrierte sich das CYD Campus Startup-Scouting auf die Schweiz, die USA, Israel, das Vereinigte Königreich und Frankreich, mit einigen Unternehmen in anderen Ländern. Das Scouting konzentrierte sich auf neue Technologien in den Bereichen Cybersicherheit und KI, um die wichtigsten Trends und Akteurinnen und Akteure in einem frühen Stadium zu identifizieren. Es wurden Interviews mit rund 100 Startups und Unternehmen geführt. Die Ergebnisse dieser Interviews wurden strukturiert an potenzielle Interessentinnen und Interessenten innerhalb der öffentlichen Verwaltung weitergeleitet.

Um Zugang zu den interessantesten Startups zu erhalten und Unternehmen in der Frühphase zu identifizieren, stützt sich der CYD Campus auf ein breites Netzwerk, das von Risikokapitalgebenden bis zu Acceleratorinnen und Acceleratoren und von Botschafterinnen und Botschaftern bis zu Wirtschaftsförderungsorganisationen reicht. Zu den wichtigsten Partnerinnen und Partnern gehören die Swisscom Aussenstelle im Silicon Valley und das Swissnex Netzwerk. Ein weiteres wichtiges Scoutinginstrument ist die Teilnahme an weltweit führenden Konferenzen wie der RSA Conference in San Francisco, Black Hat, Defcon, USENIX Security, Cybertech und Cyberweek in Tel Aviv sowie der European Cyber Week in Rennes. Diese Veranstaltungen bieten die Möglichkeit, in kurzer Zeit eine grosse Anzahl von Unternehmen sowie Partnerinnen und Partnern zu treffen.

Die im Rahmen der Scouting-Aktivitäten identifizierten Startups führten zu mehreren Proof-of-Concepts. Darüber hinaus wurden die gewonnenen Informationen zur Unterstützung des Beschaffungsprozesses und zum besseren Verständnis des Cyber-Marktes genutzt.

Internationale Zusammenarbeit

Die Zusammenarbeit mit internationalen Partnerinnen und Partnern ist im Cyberspace unerlässlich. Da sich Bedrohungen und böswillige Akteurinnen und Akteure nicht an Landesgrenzen halten, ist die Schweiz auf eine enge Zusammenarbeit angewiesen. Die internationale Zusammenarbeit ist auch einer der drei strategischen Pfeiler der neu lancierten Schweizer Armeestrategie 2030.

Forschungspartnerschaften

Der CYD Campus führt Forschungsprojekte mit Wissenschaftlerinnen und Wissenschaftlern von weltweit führenden Universitäten wie der University of Oxford, der University of Southern California und der Ruhr-Universität Bochum durch.

Multinationale Zusammenarbeit

Der CYD Campus arbeitet auch mit internationalen Organisationen zusammen. So vertritt der CYD Campus die Schweiz bei den CapTechs Cyber and Information der Europäischen Verteidigungsagentur. Je nach Bedarf werden die Diskussionen zu konkreten Projekten intensiviert und CYD Campus-Forschende prüfen, ob ein Beitrag der Schweiz sinnvoll ist. Diese Gremien dienen auch als Plattform für den informellen Austausch zwischen Fachleuten. So ist der CYD Campus federführend bei den Schweizer Bemühungen um eine mögliche Beteiligung an einem zukünftigen PESCO-Projekt im Bereich der Cyber-Ranges Federation (CRF). Ziel der CRF ist es, die Leistungsfähigkeit der europäischen Cyber Ranges (CR) zu verbessern, indem bestehende nationale Cyber Ranges zu einem grösseren Cluster zusammengeschlossen werden. Auch die NATO ist eine wichtige Kooperationspartnerin. Der CYD Campus leistet einen wichtigen Beitrag zu den Aktivitäten des CCDCOE in Tallinn, sowohl durch die Präsenz unseres Forschers William Blonay vor Ort, als auch durch Forschungsbeiträge ihres Arbeitsprogramms. Im Jahr 2023 wurde William Blonay zum „Green Team Leader" für die Cyberübungen des Zentrums befördert. Darüber hinaus beteiligt sich der CYD Campus punktuell an interessanten STO-Arbeitsgruppen der NATO. Diese Projekte werden von der armasuisse-Geschäftsstelle in Brüssel unterstützt.

Bilaterale Austausche

Von grosser Bedeutung ist auch der bilaterale Austausch mit Partnerorganisationen des VBS in ausgewählten Ländern in Europa, Amerika und Asien. Der CYD Campus arbeitet sowohl mit grösseren Ländern zusammen, denen er sein hoch spezialisiertes Know-how zur Verfügung stellt, als auch mit kleineren, agilen Partnerinnen und Partnern, die vor ähnlichen Herausforderungen stehen. Je nach Partnerland geht es darum, Forschende mit ähnlichen Interessen zu finden, um Fachwissen, Methoden und Daten auszutauschen oder, in bestimmten Fällen, gemeinsame Forschungsprojekte durchzuführen. Diese Arbeit erstreckt sich auf alle Bereiche und Domänen des CYD Campus, von Technologie- und Marktüberwachung bis hin zu Cybersicherheit, Datenwissenschaft und Anwendungen des maschinellen Lernens. Der CYD Campus arbeitet eng mit dem armasuisse-Büro in Washington, den Schweizer Botschaften und den Verteidigungsattachés in aller Welt zusammen, um die Projekte zu koordinieren und zu verwalten.

Der Cyber-Defence Campus als Vorzeigebeispiel

Schliesslich ist der CYD Campus ein weltweit führendes Beispiel für die erfolgreiche Zusammenarbeit zwischen der Regierung, Hochschulen und Industrie. Jedes Jahr besuchen Delegationen aus verschiedenen Ländern den CYD Campus, um sich über dessen bewährte Verfahren zu informieren. In dem Bestreben, die globale Cyber Resilienz zu stärken, ist der CYD Campus bestrebt, sein Wissen mit Gleichgesinnten sowie Partnerinnen und Partnern zu teilen.

Advanced Course in Engineering (ACE)

Der Advanced Course in Engineering (ACE) ist ein Sommerpraktikumsprogramm mit Schwerpunkt auf Cyberverteidigung und -führung, das vom United States Air Force Research Lab organisiert wird. Das Programm kombiniert die Ausbildung in den Grundlagen der Cybersicherheit mit praktischen Anwendungen in simulierten Cyberwar-Szenarien. Die Trainees nehmen an Vorlesungen, Forschungsprojekten, Einsätzen in einem simulierten Cyber-Kriegsgebiet und Führungsseminaren teil, die in einer abschliessenden Übung gipfeln. Der Schwerpunkt des Programms liegt auf der Entwicklung von technischen, Führungs- und Problemlösungsfähigkeiten in einem umkämpften Cyber-Umfeld. Simon Kindhauser, Praktikant am Cyber-Defence Campus, leitete die Schweizer Delegation am Advanced Course in Engineering im Sommer 2023 und leistete einen wertvollen Beitrag zum Programm.

10. Kunden- & Portfoliauswertung

Das Cyber Dispositiv des Bundes ist gemäss der Cyber Strategie in drei Bereiche eingeteilt:

- Cybersicherheit (EFD)
- Cyberverteidigung (VBS)
- Cyberstrafverfolgung (EJPD)

Der CYD Campus als Teil der Cyberverteidigung erbringt seine primäre Leistung zugunsten seiner direkten Organisationen der armasuisse, der militärischen Organisationen der Verteidigung sowie dem Nachrichtendienst des Bundes. Ein wesentliches Kernmerkmal bei den Kundenaufträgen besteht darin, dass generiertes Wissen aus der CYD Campus Forschung und Innovation genutzt wird, um mit dessen Hilfe Beiträge für Grundlagenstudien, Anforderungen im Bereich der Beschaffung, Technologie-Transfer Konzepte sowie Arbeiten im Bereich der Cybersicherheit, des Data Science und dem Technologie Monitoring zu erbringen.

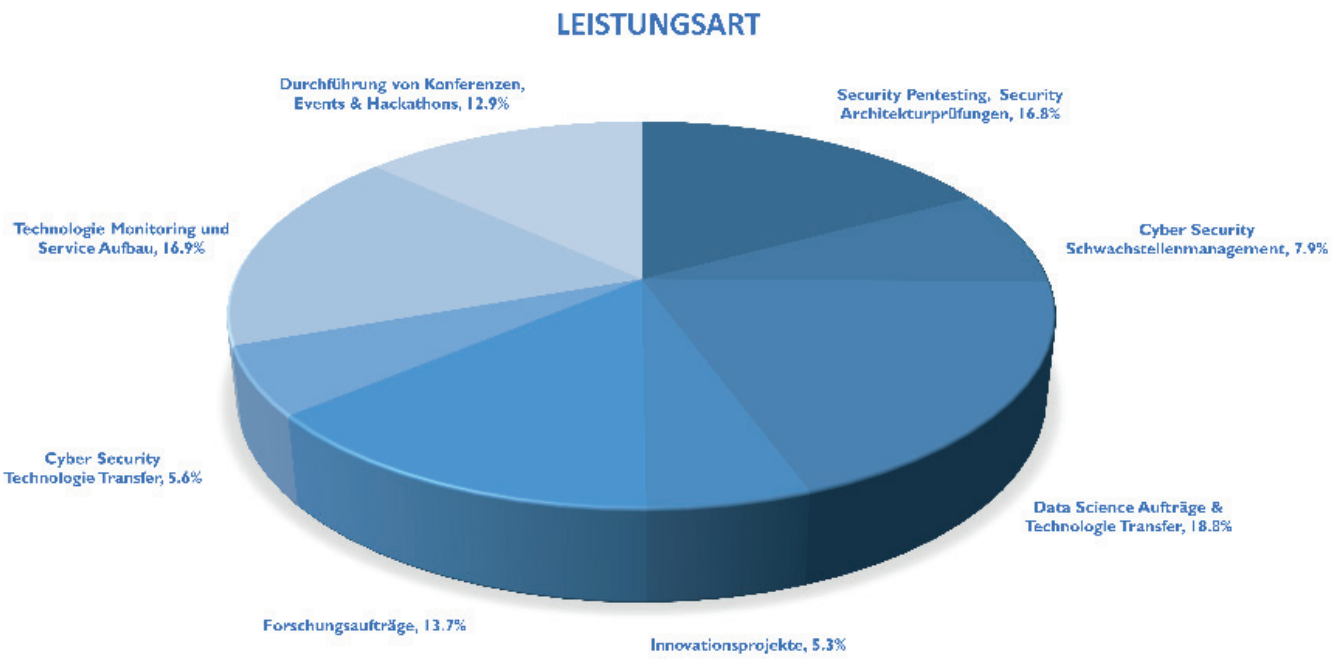
Die Gruppe Cybersicherheit erbrachte ihre Leistungen im Jahr 2023 - für die verschiedenen Kundengruppen - in den Schwerpunktsthemen der Security Prüfung in Anwendungen und leistete damit einen wesentlichen Beitrag zur Sicherheit in den geprüften Systemen.

Die Gruppe Data Science unterstützte mit ihren Arbeiten den Technologie-Transfer zum Aufbau von neuen Fähigkeiten der Verteidigung sowie von Studien für den Einsatz von neuen KI-Technologien für die Bild-, Sprach-, Signal- und Datenauswertung.

Das Technologie Monitoring – als neue Gruppe des Cyber-Defence Campus – wurde vermehrt von verschiedenen Organisationen der Verteidigung genutzt und erbrachte ihren Beitrag in der frühen Phase der Beschaffung zur Abklärung der Nutzbarkeit von neuen Cyber Technologien und für übergreifende Studien zum Ausweis des Technologie-Reifegrades in ausgewiesenen Bereichen der Cyber-Defence.

Im Jahr 2023 durfte der CYD Campus für nachfolgende Organisationen Arbeiten durchführen:

- Bundesamt für Rüstung armasuisse
- Gruppe Verteidigung
  - Armeestab
  - Projekt Kommando Cyber
  - Kommando Operationen
  - Kommando Ausbildung
- Nachrichtendienst des Bundes
- Generalsekretariat VBS
- Eidgenössisches Finanz-Departement
- Nationales Zentrum für Cybersicherheit NCSC
- Bundesamt für Polizei FEDPOL
- Bundeskanzlei



Detaildarstellung der direkten Auftragsleistungen und Dienste über alle Portfoliogruppen

11. Security Services

Im Jahr 2023 untersuchten Mitarbeitende des CYD Campus die Sicherheit von militärischen Systemen, die im Rahmen von Rüstungs- und IKT-Beschaffungen im VBS bearbeitet werden. Die Prüfungen erfolgten als Sicherheitsanalysen, Penetration Testing oder Sicherheitsberatungen. Auftraggebende waren in den meisten Fällen die Beschaffungsstellen von armasuisse.

Im Jahr 2023 waren das mehr als 30 Untersuchungen, insbesondere von folgenden Objekten:

- Web Anwendungen
- Fachanwendungen
- Middlewares
- Computernetzwerke
- Verschiedene Endgeräte und Serversysteme
- Kommunikationslösungen
- Sicherheitslösungen und -architekturen
- Führungsinformationssysteme
- Fahrzeuge
- Aviatik und Satellitenkommunikationssysteme

Leider dürfen die untersuchten Objekte sowie die Resultate der Prüfungen aus Klassifikationsgründen weder namentlich aufgeführt noch deren Schwachstelle ausgewiesen werden. Ausnahmen bilden Commercial-of-the-Shelf (COTS) Produkte, bei welchen die entdeckten Schwachstellen via CVE Nummer und Advisory gemeldet und dem CYD Campus als Entdecker zugerechnet werden.

Um trotzdem einen Einblick in die Highlights der Arbeiten zu erhalten, werden zwei Beispiele anonymisiert vorgestellt und die Liste der veröffentlichten Schwachstellen aufgeführt:

Pentesting einer Fachanwendung

Ziel des Auftrages war die Durchführung eines Pentesting auf eine neu entwickelte webbasierte Anwendung, die Prüfung der zugehörigen Web Application Firewall und deren Authentisierungslösung. Die Prüfung erfolgte dabei nach einem Whitebox-Ansatz.

Die Schwachstelle mit der höchsten Kritikalität nutzte dabei den Schlüssel eines hartkodierten RSA Keys, welcher in einem Code Repositories zugänglich war, und mithilfe dessen sich Angreifende von selbsterstellten Benutzerinnen und Benutzern die Rechte existierender Anwenderinnen und Anwendern aneignen konnten. Da die zugrunde liegende Identity and Access Management Lösung für weitere Anwendungen genutzt wurde, war die ausgewiesene Schwachstelle übergreifend und musste als Notmassnahme sofort behoben werden.

Sicherheitsuntersuchung Secure Boot

In der Sicherheitsprüfung Secure Boot wurde ein Kundenendgerät auf die Tauglichkeit der Hardware-basierten Sicherheitsmassnahmen im Boot Prozess untersucht. Es sollte dabei verifiziert werden, inwiefern die Massnahmen einen Betrieb eines sicheren Betriebssystems erlauben.

In der Untersuchung der Sicherheitslösung wurden acht mittlere und zwei kritische Schwachstellen identifiziert, wobei die kritischen Schwachstellen es Angreifenden erlauben, den Boot Prozess zu manipulieren und die Sicherheitslösung zu degradieren. Mit der degradierten Sicherheitslösung wird ein kompromittierter Boot Prozess möglich und dem sicheren Betriebssystem die Grundlage für den operativen Betrieb entzogen.

Beide Beispiele verdeutlichen den Mehrwert der Sicherheitsprüfungen und die Unerlässlichkeit, Systeme, Produkte und Softwarekomponenten von sicherheitskritischen Anlagen zu prüfen und den Nachweis für eine sichere operative Nutzung zu erbringen.

Die nachfolgende Tabelle listet die im Jahr 2023 veröffentlichten Schwachstellen auf. Die mit * markierten Schwachstellen wurden von mehreren Entitäten gefunden und der Herstellerin oder dem Hersteller vor deren Bekanntwerden gemeldet. Die CVE Nummer wird in solchen Fällen typischerweise der Entität zugerechnet, welche die Schwachstelle als erstes gemeldet hat.

Hardware / Software	CVE & Reports	Datum	CVSS
Fortiguard	CVE-2022-40682	März 23	7.1
Fortiguard	CVE-2022-40682	April 23	7.8
Sharekey (19 Schwachstellen)	Report	April 23	10
OPSWAT MetaDefender Kiosk	CVE-2023-36657	September 23	5.9
OPSWAT MetaDefender Kiosk	CVE-2023-36659	September 23	6.2
FortiClient (Windows)*	CVE-2022-40681	Oktober 23	7.1
Bleachbit	CVE-2023-47113	Oktober 23	7.8
FortiClient (Windows)*	CVE-2023-41840	November 23	7.4

Liste der im Jahre 2023 veröffentlichten und rapportierten Schwachstellen untersuchter Hard- und Software Komponenten

12. Labore

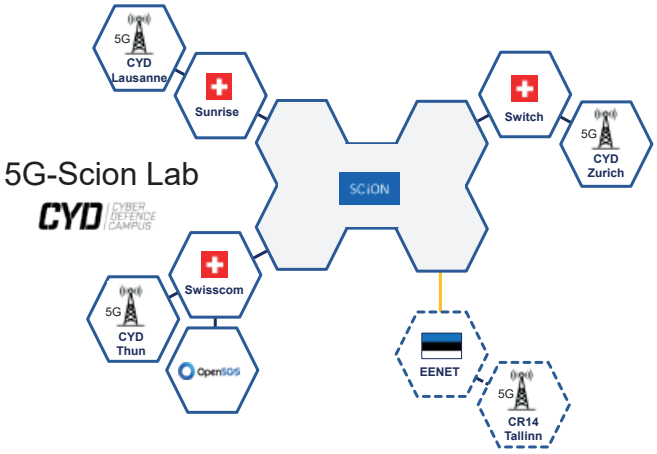
Der Cyber-Defence Campus betreibt an seinen drei Standorten eine Vielzahl von Laborinfrastrukturen und permanente Testinfrastrukturen, welche für Forschungsprojekte, Tests und Demonstrationen zur Verfügung stehen:

- WAN SCION Testbed (Thun, Lausanne und Zürich)
- 5G Lab (Thun)
- Cyber Avionics Labor (Thun)
- SATCOM Labor (Thun, Lausanne und Zürich)
- Hardware Security Lab (Thun)
- Data Science Labor (Thun)
- Security Lab (Thun)
- Hardware Security Lab (Thun)
- ICS Labor (Thun)
- IoT Labor (Thun)

Dieses Jahr wurden in einigen Bereichen Erweiterungen dieser Labore getätigt.

WAN SCION Testbed

Um internationale Use Cases über SCION zu demonstrieren wurde eine Erweiterung des SCION WAN Testbeds durchgeführt mit einem neuen SCION-Netzwerkknoten in Tallinn, Estland. Der Netzwerknoten in Tallinn verbindet die estnische Cyber Range von Cybexer mit dem CYD Campus an seinen drei Standorten über ein natives SCION Netzwerk. Die internationale SCION-Anbindung nach Tallinn erfolgt über Switch und Géant und demonstriert die Fähigkeit zur Bereitstellung eines sicheren SCION-basierten WANs über mehrere Länder und Internet Anbietende.

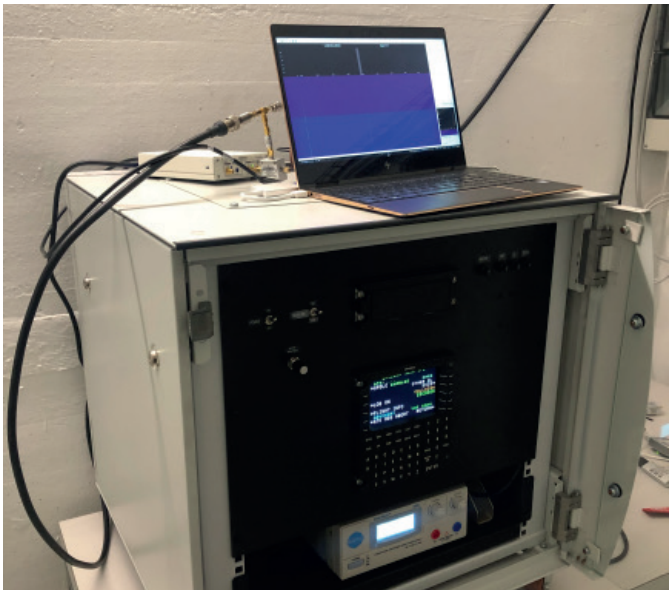


5G Lab

Im Jahr 2023 wurde das 5G-Labor um ein 5G-Standalone-Kernnetz (5G SA) mit der Open-Source-Software Open5GS und zwei Funkzugangspunkten mit mehreren mobilen Geräten erweitert. Die Funkzugangspunkte befinden sich in Thun und Zürich und sind über SCION mit dem 5G-Kern verbunden. So können wir diese wichtige neue Technologie testen, erforschen und für Trainingszwecke nutzen. Der Kern ist virtualisiert und läuft in unserem Rechenzentrum. Dies ermöglicht End-to-End-Tests der Sicherheit dieses neuen Protokolls. Ein Teil der Arbeiten wird in Zusammenarbeit mit dem NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) und der deutschen Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) durchgeführt.

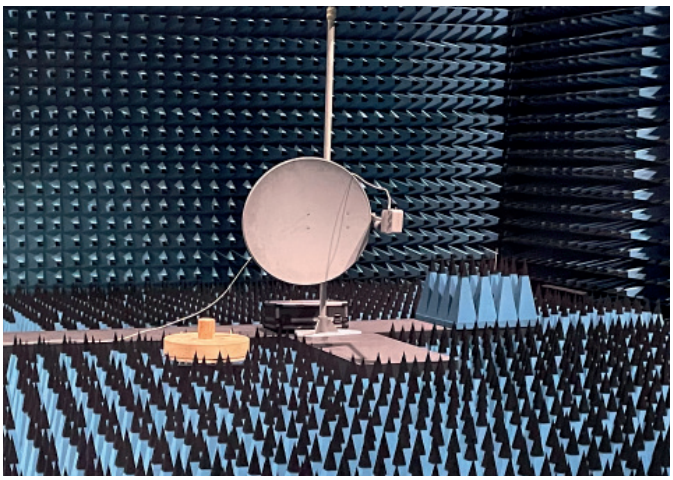
Cyber Avionics Lab

Das Cyber Avionics Lab wurde mit zwei kommerziellen Multilaterationssystemen (MLAT) im Kanton Zürich erweitert. Die MLAT-Systeme wurden in der Praxis auf ihre Resilienz gegen Spoofing getestet. Cyberangriffe gegen das Kollisionsvermeidungssystem TCAS wurden erstmalig im Cyber Avionics Lab in Thun erfolgreich getestet. Die Untersuchung von Gegenmassnahmen ist im Gange. Der Datenlink CPDLC wurde im Lab in Zusammenarbeit mit Skyguide und Eurocontrol auf seine praktische Sicherheit untersucht. Für den Datenbus ARINC 429 des Labors wurden Hard- und Software-Tools entwickelt, welche die volle Kontrolle über den Bus erlauben. Dies hilft bei der Analyse von Attacken und Gegenmassnahmen.



SATCOM Lab

Das SATCOM Lab wurde um eine Installation einer stationären 2.4m Antenne auf dem Dach unserer Büros in Thun erweitert. Diese erlaubt einen breiten Empfang und Analyse verschiedener Satellitensysteme. Mobile Erweiterungen sind für 2024 geplant. Desweiteren wurden verschiedene Kooperationen mit kommerziellen Betreibenden von Bodenstationen begonnen. Eine Sicherheitsanalyse des Aviatik-Datenlinks ADS-C wurde vorgenommen. Es wurde aufgezeigt wie ungeschützte Satellitenverbindungen genutzt werden, um Satellitenmodems aus der Distanz zu übernehmen.



Hardware Security Lab

In unserem neuen Hardware Security Lab können nun Analysen und Tests durchgeführt werden, um die Sicherheit von eingebetteten Systemen und IoT-Geräten zu prüfen. Dabei geht es um die Identifizierung von Schwachstellen in Hardware- und Softwarekomponenten, die Untersuchung potenzieller physischer Angriffe und damit einhergehender möglicher Extraktion von Daten und Informationen. Das Labor wird einen Beitrag dazu leisten, sichere und geschützte Hardwarekomponenten zuhanden der Beschaffung und Schwachstellenforschung zu prüfen, um den hohen Anforderungen an die Informationssicherheit gerecht zu werden.

Data Science Lab

Der Cyber-Defence Campus betreibt ein Data Science Lab (DSL). Im DSL wurden im Rahmen von LifeCycle Aktivitäten verschiedene Komponenten erneuert. Um dem stetig steigenden Speicherplatzbedarf gerecht zu werden wird der Speicherplatz neu per Storage Area Network (SAN) bereitgestellt und die Datensicherung erfolgt über eine Hardware Plattform, welche auf geringstem Platz bis zu einem Petabyte Disk Speicher bereitstellt. Diese Infrastruktur ermöglicht die lokale Durchführung von Big Data und KI Projekten im Lab.

13. Aktivitäten

Besuche

- 25.01.23: Besuch Stv. Rüstungschef beim CYD Campus, Lausanne
- 13.02.23: Besuch Cyber Lehrgang, Thun
- 09.03.23: Besuch GCSP Military Attaché Training Course, Thun
- 22.03.23: Cyber Hub Bundeswehr, Thun
- 05.04.23: NTC besucht den CYD Campus, Zürich
- 12.04.23: Rüstungschef Finnland, Thun
- 26.04.23: Swisscom Ventures besucht den CYD Campus, Zürich
- 26.04.23: KAPO ZH besucht den CYD Campus, Zürich
- 05.05.23: Besuch Offiziersgesellschaft Cyber beim CYD Campus, Zürich
- 12.05.23: Besuch Chef Swisscom Ventures beim CYD Campus, Lausanne
- 13.06.23: Besuch Bundesamt für Zivildienst, Thun
- 13.06.23: Besuch SiPol GS VBS, Thun
- 28.06.23: Besuch Accenture, Zürich
- 06.09.23: Besuch Hochschule Luzern und FUB, Zürich
- 11.09.23: Data Science: Daten als Einsatzmittel, Besuch Kader Fl Br 31, Thun
- 17.10.23: Besuch TLG Cyber, Thun
- 13.11.23: Besuch GS-VBS & Teilnehmende ada Fellowship VBS, Thun
- 15.11.23: Besuch Chef Kdo Cy Estland, Thun
- 14.12.23: Besuch A Plan, Thun

Events

- 02.05.23: Forschungsrapport Data Science & Cybersicherheit
- 19. – 23.06.23: Cyber-Alp Retreat, Sachseln
- 27.06.23: Workshop über Deep Content Generation and Cyber Influence Operations, Zürich
- 16. – 20.08.23: Connected 2023, Kloten
- 11. – 15.09.23: ICS Trainings und Hackathon, Thun
- 20. – 22.09.23: Swarm Intelligence Workshop, Zürich
- 08. – 14.10.23: Data Science Hackathon
- 16. – 20.10.23: Car Security Training und Hackathon, Thun
- 26.10.23: CYD Campus Konferenz, Bern
- 16.11.23: Technologie Monitoring Seminar, Lausanne
- 23.11.23: Jahresendanlass, Bern

Besuche im Ausland

- 25.01 – 02.02.2023: Technologie Monitoring und Cybertech, Israel
- 27.02 – 04.03.2023: SpaceSec Workshop und NDSS, USA
- 04.2023: Teilnahme an Locked Shields, Estland
- 23.03 – 24.03.2023: NATO STO SET-322, Paris, Frankreich
- 22.03 – 24.03.2023: University of Oxford, England
- 17.04 – 28.04.2023: RSA Conference und Scouting, USA
- 26.04 – 27.04.2023: CySat, Paris
- 16.05 – 18.05.2023: ICMCIS & NATO IST panel, Skopje, Mazedonien
- 30.05 - 02.06.2023: CyCon, Estland
- 01.06. – 18.08.2023: Air Force Research Labs, USA
- 15.06.2023: PESCO Federated Cyber Ranges, Estland
- 29.06 – 30.06.2023: EDA CapTech Cyber, Luxembourg
- 19.07 – 27.07.2023: Army Research OfficeL & ICML, USA
- 06.08 – 14.08.2023: Usenix Security, Defcon, Blackhat, Swisscom Outpost, USA
- 02. - 05.10.2023: DASC Konferenz, Barcelona, Spanien
- 04.10. – 10.10.2023: Scouting UK, London, England
- 05. - 14.10.2023: Data Science Hackathon, Spanien
- 27.10 – 06.11.2023: Army Research Labs & MILCOM, USA
- 30. - 31.10.2023: OpenSky Symposium, Toulouse, Frankreich
- 06. - 09.11.2023: Konferenz VMWare Explore, Barcelona
- 20. - 23.11.2023: European Cyber Week Rennes, Frankreich
- 26.11 - 01.12.2023: ACM CCS, Kopenhagen
- 04.12. – 08.12.2023: GLOBECOM, Malaysia

Teilnehmende am ICS Hackathon 2023 in Thun

14. Präsentationen

- 28.02.23: Cyber Intelligence Europe conference & exhibition, Bern
- 03.03.23: Scion National Testbed for Cyber Defence, Anapaya, Zürich
- 08.03.23: Can legislation and standardisation support aviation becoming more cyber resilient?, Airspace World, Genf
- 16.03.23: Encryption 2025, ICT Warrior Tech Talk, Bern
- 21.03.23: Cyber impacts auf Lfz und Air Ops, LW Stab, Aarau
- 29.03.23: ISSS Israelische und Schweizerische Innovation in Cyber Security, Rotkreuz
- 26.04.23: Swiss Night @RSA, San Francisco
- 09.05.23: Daten schützen im digitalen Zeitalter, Digital Day 2023
- 14.06.23: Workshop «ADINT», Emmenbrücke
- 27.06.23: Workshop «Deep Content Generation and Cyber Influence Operations», Zürich
- 12.08.23: Elon, Twitter and the PIA: How not to achieve Privacy in Aviation, DEFCON, USA
- 12.08.23: Labs and Trust: How to build a successful aviation cybersecurity research programme, DEFCON, USA
- 13.08.23: The Looming Perils for End Users in SATCOM, DEFCON, USA
- 30.08.23: Daten schützen im digitalen Zeitalter, NDB, Bern
- 01.09.23: Securing Critical Network Infrastructures, Uni Luxembourg
- 14.09.23: SBFI Workshop Cyber Forschungskooperation, Bern
- 19.09.23: ERFA 2023, ar Immo, Airolo/Olivone
- 18.10.23: Scion @ CYD Campus, Scion Day, Zurich
- 23.10.23: Cyber Training @ CYD Campus, Bern
- 22.11.23: Security Academy 2023 «IT-Dienstleistungen der Zukunft im VBS», Bern
- 06./07.12.23: Drone Remote ID spoofer and low cost receiver application, Black Hat Europe, London

Christa Zoufal von IBM Research präsentiert über Quantum Machine Learning an der CYD Campus Konferenz 2023

Dr. Martin Burkhart präsentiert Chancen und Herausforderungen von Self-Sovereign Identities (SSI)

15. Wissenschaftliche Publikationen

Dezember

Behavioral fingerprinting to detect ransomware in resource-constrained devices
Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Jan von der Assen, Dennis Shushack, Ángel Luis Perales Gómez, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, Computers & Security 2023;135:103510

LLMs perform poorly at concept extraction in cyber-security research literature
Maxime Würsch, Andrei Kucharavy, Dimitri Percia David & Alain Mermoud, arXiv

November

Efficient collective action for tackling time-critical cybersecurity threats
Sébastien Gillard, Dimitri Percia David, Alain Mermoud & Thomas Maillart, Journal of Cybersecurity 2023;9(1)

Watch This Space: Securing Satellite Communication through Resilient Transmitter Fingerprinting
Joshua Smailes, Sebastian Köhler, Simon Birnbach, Martin Strohmeier & Ivan Martinovic, CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, Kopenhagen, Dänemark.

Oktober

A first look at exploiting the Automatic Dependent Surveillance-Contract Protocol for open aviation research
Marc Xapelli, Tobias Lüscher, Giorgio Tresoldi, Vincent Lenders & Martin Strohmeier, Opensky Symposium, Toulouse, Frankreich

Assessing the sustainability and trustworthiness of federated learning models
Alberto Huertas Celdran, Chao Feng, Pedro Miguel Sanchez Sanchez, Lynn Zumtaugwald, Gérôme Bovet & Burkhard Stiller, arXiv

Lessons learned in transcribing 5000 h of air traffic control communications for robust automatic speech Understanding
Juan Zuluaga-Gomez, Iuliia Nigmatulina, Amrutha Prasad, Petr Motlicek, Driss Khalil, Srikanth Madikeri, Allan Tart, Igor Szoke, Vincent Lenders, Mickael Rigault & Khalid Choukri, Aerospace 2023;10(10):898

MTD-Based Aggregation Protocol for Mitigating Poisoning Attacks on DFL
Chao Feng, Alberto Huertas Celdran, Michael Vuong, Gérôme Bovet & Burkhard Stiller, arXiv

OpenSky Report 2023: Low Altitude Traffic Awareness for Light Aircraft with FLARM
Xavier Olive, Martin Strohmeier, Junzi Sun & Giorgio Tresoldi, DASC 2023, Digital Avionics Systems Conference, Barcelona, Spanien

P3LI5: Practical and confidEntial Lawful Interception on the 5G core
Francesco Intoci, Julian Sturm, Daniel Fraunholz, Apostolos Pyrgelis & Colin Barschel, 2023 IEEE Conference on Communications and Network Security (CNS), Orlando, USA

Scaling the Timing-Based detection of anomalies in Real-World aircraft trajectories
Lukas Baege, Patrick Schaller, Vincent Lenders & Martin Strohmeier, Opensky Symposium, Toulouse, Frankreich

Sentinel: an aggregation function to secure decentralized federated learning
Chao Feng, Alberto Huertas Celdran, Janosch Baltensperger, Enrique Tomas Martinez Beltran, Gérôme Bovet & Burkhard Stiller, arXiv

SKYPOS: Real-world evaluation of self-positioning with aircraft signals for IoT devices
Yago Lizarribar, Domenico Giustiniano, Gérôme Bovet & Vincent Lenders, IEEE Journal on Selected Areas in Communications 2023;42(1):134-145

Stealth Spectrum Sensing Data Falsification Attacks Affecting IoT Spectrum Monitors on the Battlefield
Pedro Miguel Sánchez Sánchez, Enrique Tomás Martínez Beltrán, Alberto Huertas Celdrán, Robin Wassink, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM), Boston, USA

September

A Relaxed Optimization Approach for Adversarial Attacks Against Neural Machine Translation Models
Sahar Sadrizadeh, Clément Barbier, Ljiljana Dolamic & Pascal Frossard, 31st European Signal Processing Conference (EUSIPCO), Helsinki, Finnland

A novel algorithm for informed investment in cybersecurity companies and technologies
Anita Mezzetti, Loïc Maréchal, Dimitri Percia David, William Blonay, Sébastien Gillard, Michael Tsesmelis, Thomas Maillart & Alain Mermoud, In: Cyberdefence: The Next Generation (S. 87-101)

Anticipating cyberdefense capability requirements by link prediction analysis
Santiago Anton Moreno, Dimitri Percia David, Alain Mermoud, Thomas Maillart & Anita Mezzetti, In: Cyberdefence: The Next Generation (S. 135-145)

Cybersecurity Ecosystems: A network study from Switzerland
Cédric Aeschlimann, Kilian Cuche & Alain Mermoud, In: Cyberdefence: The Next Generation (S. 123-134)

Decentralized Federated Learning: fundamentals, state of the art, frameworks, trends, and challenges
Enrique Tomás Martínez Beltrán, Mario Quiles Pérez, Pedro Miguel Sánchez Sánchez, Sergio López Bernal,Gérôme Bovet, Manuel Gil Pérez, Gregorio Martínez Pérez & Alberto Huertas Celdrán, IEEE Communications Surveys and Tutorials 25(4):2983-3013

Identification of future cyberdefense technology by text mining
Dimitri Percia David, William Blonay, Sébastien Gillard, Thomas Maillart, Alain Mermoud, Loïc Maréchal & Michael Tsesmelis, In: Cyberdefence: The Next Generation (S. 69-86)

Identifying emerging technologies and influential companies using network dynamics of patent clusters
Michael Tsesmelis, Ljiljana Dolamic, Marcus M. Keupp, Dimitri Percia David & Alain Mermoud, In: Cyberdefence: The Next Generation (S. 103-122)

Social media influence operations
Raphael Meier, arXiv

August

CyberForce: a federated reinforcement learning framework for malware mitigation
Chao Feng, Alberto Huertas Celdran, Pedro Miguel Sanchez Sanchez, Jan Kreischer, Jan von der Assen, Gérôme Bovet, Gregorio Martinez Perez & Burkhard Stiller, arXiv

FABRID: Flexible Attestation-Based Routing for Inter-Domain Networks
Cyrill Krähenbühl, Marc Wyss, David Basin, Vincent Lenders, Adrian Perrig & Martin Strohmeier, 32nd USENIX Security Symposium, Anaheim, USA

Network fingerprinting via timing attacks and defense in software defined networks
Beytüllah Yiğit, Gürkan Gür, Fatih Alagöz & Bernhard Tellenbach, Computer Networks 2023; 232:109850

Juli

Byzantine-Resilient Learning Beyond Gradients: Distributing Evolutionary Search
Andrei Kucharavy, Matteo Monti, Rachid Guerraoui & Ljiljana Dolamic, GECCO '23 Companion: Companion Conference on Genetic and Evolutionary Computation, Lissabon, Portugal

Evolutionary Algorithms in the Light of SGD: Limit Equivalence, Minima Flatness, and Transfer Learning
Andrei Kucharavy, Rachid Guerraoui & Ljiljana Dolamic, The 2023 Conference on Artificial Life, Sapporo, Japan

LWHBench: a low-level hardware component benchmark and dataset for single board computers
Pedro Miguel Sánchez Sánchez, José María Jorquera Valero, Alberto Huertas Celdrán, Gérôme Bovet, Manuel Gil Pérez & Gregorio Martínez Pérez, Internet of Things 2023;22:100764

Mitigating communications threats in decentralized federated learning through moving target defense
Enrique Tomás Martínez Beltrán, Pedro Miguel Sánchez Sánchez, Sergio López Bernal, Gérôme Bovet, Manuel Gil Pérez,Gregorio Martínez Pérez & Alberto Huertas Celdrán, arXiv

Moving Target Defense Strategy Selection against Malware in Resource-Constrained Devices
Jan Von der Assen, Alberto Huertas Celdrán, Nicolas Huber, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venedig, Italien

Juni

A Federated Defense Framework Using Cooperative Moving Target Defense
Chao Feng, Jan von der Assen, Alberto Huertas Celdrán, Steven Näf, Gérôme Bovet & Burkhard Stiller, 8th International Conference on Smart and Sustainable Technologies (SpliTech), Split, Kroatien

A Trustworthy Federated Learning Framework for Individual Device Identification
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, JNIC Cybersecurity Conference, Vigo, Spanien

Building Collaborative cybersecurity for Critical Infrastructure Protection: Empirical evidence of Collective intelligence information sharing Dynamics on ThreatFox
Eric Jollès, Sébastien Gillard, Dimitri Percia David, Martin Strohmeier & Alain Mermoud, In: Critical Information Infrastructures Security. CRITIS 2022. Lecture Notes in Computer Science, vol 13723 (S.140-157)

FedStellar: a platform for decentralized federated learning
Enrique Tomás Martínez Beltrán, Ángel Luis Perales Gómez, Chao Feng, Pedro Miguel Sánchez Sánchez, Sergio López Bernal, Gérôme Bovet, Manuel Gil Pérez, Gregorio Martínez Pérez & Alberto Huertas Celdrán, arXiv

Forecasting Labor Needs for Digitalization: A bi-partite graph Machine learning approach
Dimitri Percia David, Santiago Anton Moreno, Loïc Maréchal, Thomas Maillart & Alain Mermoud, World Patent Information 73:102193

From scattered sources to Comprehensive Technology Landscape: A recommendation-based retrieval approach
Chi Thang Duong, Dimitri Perica David, Ljiljana Dolamic, Alain Mermoud, Vincent Lenders & Karl Aberer, World Patent Information 73:102198

GraphINC: Graph Pattern mining at network speed
Rana Hussein, Alberto Lerner, Andre Ryser, Lucas David Bürgi, Albert Blarer & Philippe Cudre-Mauroux, Proceedings of the ACM on Management of Data. 2023;1(2):1-28

LLM-Based Entity Extraction is Not for Cybersecurity
Maxime Würsch, Andrei Kucharavy, Dimitri Percia-David & Alain Mermoud, Joint Workshop of the 4th Extraction and Evaluation of Knowledge Entities from Scientific Documents and the 3rd AI + Informetrics (EEKE- AII2023), New Mexico, USA

MTFS: a Moving Target Defense-Enabled file system for malware mitigation
Jan von der Assen, Alberto Huertas Celdrán, Rinor Sefa, Gérôme Bovet & Burkhard Stiller, arXiv

RansomAI: AI-powered ransomware for stealthy encryption
Jan von der Assen, Alberto Huertas Celdrán, Janik Luechinger, Pedro Miguel Sánchez Sánchez, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, arXiv

Single-board device individual authentication based on hardware performance and autoencoder transformer models
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet & Gregorio Martínez Pérez, arXiv

Targeted Adversarial Attacks Against Neural Machine Translation
Sahar Sadrizadeh, AmirHossein Dabiri Aghdam, Ljiljana Dolamic & Pascal Frossard, ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Rhodos, Griechenland

Mai

A Framework for Wireless Technology Classification using Crowdsensing Platforms
Alessio Scalingi, Domenico Giustiniano, Roberto Calvo-Palomino, Nikolaos Apostolakis & Gérôme Bovet, IEEE INFOCOM 2023 - IEEE Conference on Computer Communications, New York, USA

A lightweight moving target defense framework for multi-purpose malware affecting IoT devices
Jan von der Assen, Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Jordan Cedeño, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, arXiv

A Simplified Training Pipeline for Low-Resource and Unsupervised Machine Translation
Àlex R. Atrio, Alexis Allemann, Ljiljana Dolamic & Andrei Popescu-Belis, Proceedings of the The Sixth Workshop on Technologies for Machine Translation of Low-Resource Languages (LoResMT 2023), Dubrovnik, Kroatien

Capturing Trends Using OpenAlex and Wikipedia Page Views as Science Indicators: The Case of Data Protection and Encryption Technologies
Sarah Ismail, Alain Mermoud, Loic Marechal, Samuel Orso & Dimitri Percia David, 27th International Conference on Science, Technology and Innovation Indicators (STI 2023), Leiden, Niederlande

Contrastive learning with self-reconstruction for channel-resilient modulation classification
Erma Perenda, Sreeraj Rajendran, Gérôme Bovet, Mariya Zheleva & Sofie Pollin, IEEE INFOCOM 2023 - IEEE Conference on Computer Communications, New York, USA

Early Detection of Cryptojacker Malicious Behaviors on IoT Crowdsensing Devices
Alberto Huertas Celdrán, Jan von der Assen, Konstantin Moser, Pedro M. Sánchez Sánchez, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, USA

Evaluating the security of power conversion systems against electromagnetic injection attacks
Marcell Szakály, Sebastian Köhler, Martin Strohmeier & Ivan Martinovic, arXiv

Evolutionary algorithms in the light of SGD: limit equivalence, minima flatness, and transfer learning
Andrei Kucharavy, Rachid Guerraoui, Ljiljana Dolamic & arXiv

FirmwareDroid: Towards Automated Static Analysis of Pre-Installed Android Apps
Thomas Sutter & Bernhard Tellenbach, 2023 IEEE/ACM 10th International Conference on Mobile Software Engineering and Systems (MOBILESoft), Melbourne, Australien

Modeling 5G Threat Scenarios for Critical Infrastructure Protection
Gerrit Holtrup, William Blonay, Martin Strohmeier, Alain Mermoud, Jean-Pascal Chavanne & Vincent Lenders, 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia

Optimizing the Size of Subword Vocabularies in Dialect Classification
Vani Kanjirangat, Tanja Samardžić, Ljiljana Dolamic & Fabio Rinaldi, Tenth Workshop on NLP for Similar Languages, Varieties and Dialects (VarDial 2023), Dubrovnik, Kroatien

Satellite Spoofing from A to Z: On the Requirements of Satellite Downlink Overshadowing Attacks
Edd Salkield, Marcell Szakály, Joshua Smailes, Sebastian Köhler, Simon Birnbach, Martin Strohmeier & Ivan Martinovic, WiSec '23: Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Guildford, UK

SecBox: A Lightweight Container-based Sandbox for Dynamic Malware Analysis
Jan von der Assen, Alberto Huertas Celdrán, Adrian Zermin, Raffael Mogicato, Gérôme Bovet & Burkhard Stiller, NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, USA

Towards Generalizing Machine Learning Models to Detect Command and Control Attack Traffic
Lina Gehri, Roland Meier, Daniel Hulliger & Vincent Lenders, 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia

April

Data in Transit Security
Roland Meier, In: Trends in Data Protection and Encryption Technologies (S. 135-139)

Differential Privacy
Valentin Mulder & Mathias Humbert, In: Trends in Data Protection and Encryption Technologies (S. 157-161)

Electronic Voting
Louis-Henri Merino, In: Trends in Data Protection and Encryption Technologies (S. 129-133)

Hardware Acceleration
Dina Mahmoud, In: Trends in Data Protection and Encryption Technologies (S. 109-114)

Identity-Based Cryptography
Bernhard Tellenbach, In: Trends in Data Protection and Encryption Technologies (S. 59-64)

In Pursuit of Aviation Cybersecurity: Experiences and lessons from a Competitive approach
Martin Strohmeier, Mauro Leonardi, Sergei Markochev, Fabio Ricciato, Matthias Schäfer & Vincent Lenders, IEEE Security & Privacy 2023; 21(4):61-73

Robust and explainable identification of logical fallacies in natural language arguments
Zhivar Sourati, Vishnu Priya Prasanna Venkatesh, Darshan Deshpande, Himanshu Rawlani, Filip Ilievski, Hông-Ân Sandlin & Alain Mermoud, Knowledge-Based Systems 266:11041

Scientometric and Wikipedia Pageview Analysis
Alexander Glavackij, Sarah Ismail & Percia David Dimitri, In: Trends in Data Protection and Encryption Technologies (S. 243-252)

Secure Multi-Party Computation
Louis-Henri Merino & José Cabrero-Holgueras, In: Trends in Data Protection and Encryption Technologies (S. 89-92)

Secure Operating System
Llorenç Romá & Bernard Tellenbach, in: Trends in Data Protection and Encryption Technologies (S. 115-120)

Secure Positioning and Localization
Martin Strohmeier, In: Trends in Data Protection and Encryption Technologies (S. 187-192)

TaxoComplete: Self-Supervised Taxonomy Completion Leveraging Position-Enhanced Semantic Matchin
Ines Arous, Ljiljana Dolamic & Philippe Cudré-Mauroux, Proceedings of the ACM Web Conference 2023 (WWW '23), Austin, USA

März

A methodology to identify identical single-board computers based on hardware behavior fingerprinting
Pedro Miguel Sánchez Sánchez, José María Jorquera Valero, Alberto Huertas Celdrán, Gérôme Bovet, Manuel Gil Pérez & Gregorio Martínez Pérez, Journal of Network and Computer Applications 212:103579

Channel and hardware impairment data augmentation for robust modulation classification
Erma Perenda, Gérôme Bovet, Mariya Zheleva & Sofie Pollin, TechRxiv

CyBERSPEC: Behavioral fingerprinting for intelligent attacks detection on crowdsensing spectrum sensors
Alberto Huertas Celdrán, Pedro Miguel Sánchez Sánchez, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, IEEE Transactions on Dependable and Secure Computing

Early warning signals of social instabilities in Twitter data
Vahid Shamsaddini, Henry Kirveslahti, Raphael Reinauer, Wallyson Lemes de Oliveira, Matteo Caorsi & Etienne Voutaz, arXiv

Fundamentals of Generative large language Models and Perspectives in Cyber-Defense
Andrei Kucharavy, Zachary Schillaci, Loïc Maréchal, Maxime Würsch, Ljiljana Dolamic, Remi Sabonnadiere, Dimitri Percia David, Alain Mermoud & Vincent Lenders, arXiv

Measuring Security Development in Information Technologies: A Scientometric framework using ARXIV e-Prints
Dimitri Percia David, Loïc Maréchal, William Lacube, Sébastien Gillard, Michael Tsesmelis, Thomas Maillart & Alain Mermoud, Technological Forecasting and Social Change 188:122316

Februar

A deep learning approach to predict collateral flow in stroke patients using radiomic features from perfusion images
Giles Tetteh, Fernando Navarro, Raphael Meier, Johannes Kaesmacher, Johannes C. Paetzold, Jan S. Kirschke, Claus Zimmer, Roland Wiest & Bjoern H. Menze, Frontiers in Neurology; 14

FederatedTrust: a solution for trustworthy federated learning
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Ning Xie, Gérôme Bovet, Gregorio Martínez Pérez & Burkhard Stiller, arXiv

Large-scale transient peri-ictal perfusion magnetic resonance imaging abnormalities detected by quantitative image analysis
Manuel Köstner, Michael Rebsamen, Piotr Radojewski, Christian Rummel, Baudouin Jin, Raphael Meier, Uzeyir Ahmadli, Kaspar Schindler & Roland Wiest, Brain communications;5(2)

QPEP in the Real World: A Testbed for Secure Satellite Communication Performance
Julian Huwyler, James Pavur, Giorgio Tresoldi & Martin Strohmeier, Workshop on Security of Space and Satellite Systems (SpaceSec) 2023

Spoofing Earth Observation Satellite Data through Radio Overshadowing
Edd Salkield, Sebastian Kohler, Simon Birnbach, Richard Baker, Martin Strohmeier & Ivan Martinovic, Workshop on Security of Space and Satellite Systems (SpaceSec) 2023, San Diego, USA

TransFool: an adversarial attack against neural machine translation models
Sahar Sadrizadeh, Ljiljana Dolamic & Pascal Frossard, arXiv

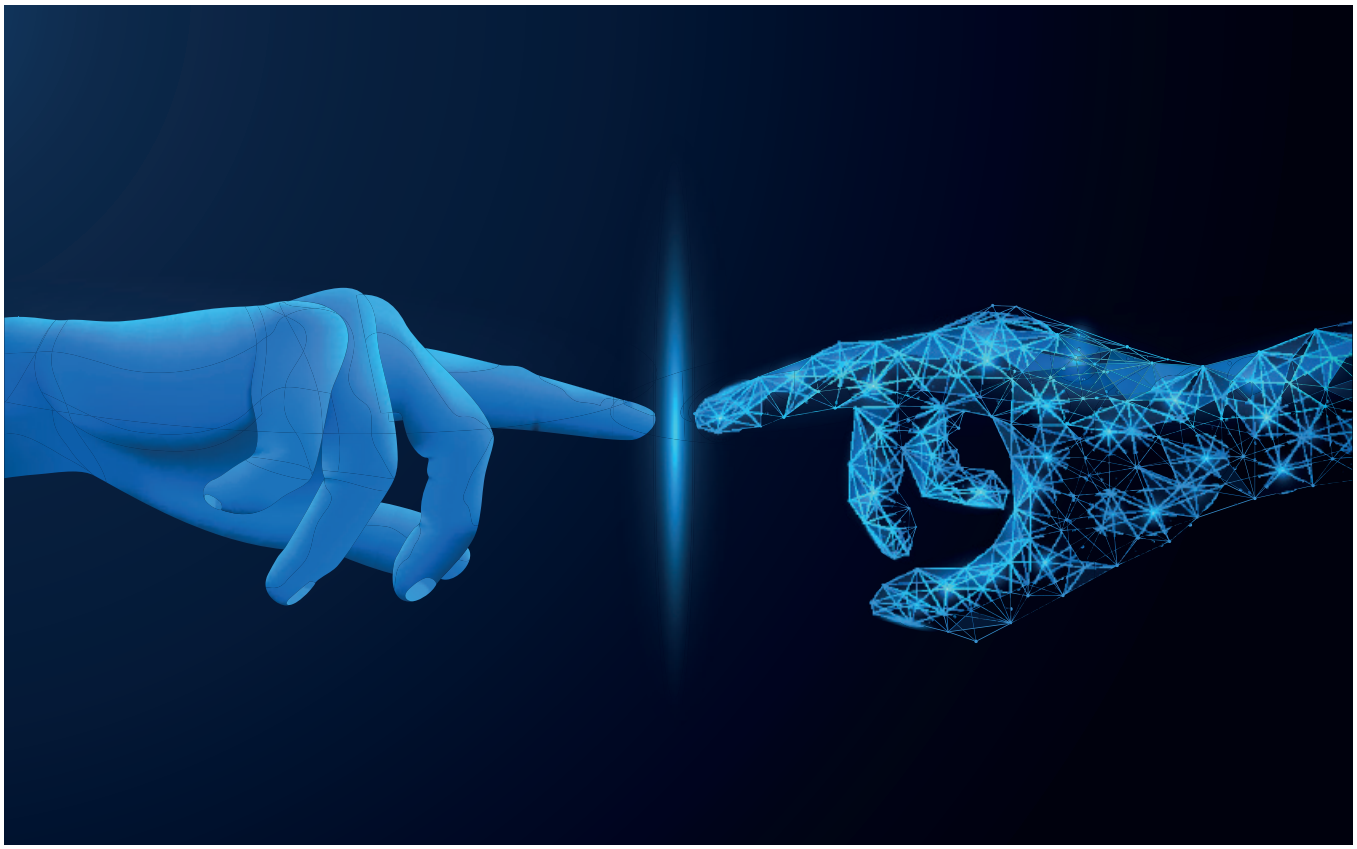
Januar

Adaptive uplink data compression in spectrum crowdsensing systems
Yijing Zeng, Roberto Calvo-Palomino, Domenico Giustiniano, Gérôme Bovet & Suman Banerjee, IEEE ACM Transactions on Networking

Analysis of GNSS disruptions in European airspace
Michael Felux, Benoit Figuet, Manuel Waltert, Patric Fol, Martin Strohmeier & Xavier Olivé, Proceedings of the Institute of Navigation. International Technical Meeting, Long Beach, UBA

Case-Based reasoning with language models for classification of logical fallacies
Zhivar Sourati, Filip Ilievski, Hông-Ân Sandlin & Alain Mermoud, arXiv

Robust federated learning for execution time-based device model identification under label-flipping attack
Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, José Rafael Buendía Rubio, Gérôme Bovet & Gregorio Martínez Pérez, Cluster Computing



16. Kommunikation

Die Bedeutung der Kommunikation im Cyberbereich kann nicht genug betont werden. Die rasante Entwicklung von Technologien, wie beispielsweise im Bereich von AI Tools mit ChatGPT, erfordert eine kontinuierliche Berichterstattung. Von Bedeutung ist unter anderem die Aufklärung der Öffentlichkeit über potenzielle Gefahren, wie auch die Förderung des Austausches zwischen Cyberfachleuten sowie zwischen Bund, Industrie, Armee und Hochschulen.

Eine proaktive Kommunikation spielt für den CYD Campus eine zentrale Rolle, um die Öffentlichkeit für Cyber-Themen zu sensibilisieren und den Cyberbereich national sowie international zu fördern. Im vergangenen Jahr konnten wir bedeutende Kommunikationsmassnahmen erfolgreich umsetzen, um das Bewusstsein für die Cyber-Verteidigung in der Schweiz, aber auch global, zu stärken.

Stärkung unserer Publikationstätigkeit

Im Jahr 2023 haben wir eine beachtliche Anzahl von 80 Fachartikeln und zwölf öffentliche Mitteilungen veröffentlicht, die sich mit aktuellen Herausforderungen und Entwicklungen im Bereich der Cybersicherheit in der Schweiz und auf der ganzen Welt befassen.

Wachstum auf Social Media

Durch kontinuierlich veröffentlichte Inhalte auf unseren Social-Media-Kanälen konnten wir unsere Onlinesichtbarkeit gezielt steigern. Auf LinkedIn konnten wir fast 2'100 neue Followerinnen und Follower gewinnen und unsere Reichweite in der Cyber-Community auf über 5'000 Followerinnen und Follower vergrössern.

Neue Website live geschaltet

Im September 2023 konnten wir unsere Website cydcampus.admin.ch liveschalten. Darauf bieten wir umfassende Einblicke in unsere vielfältigen Projekte und Programme über Publikationen, Kooperationen, bis hin zu verschiedenen Veranstaltungen am CYD Campus.

Medienmitteilungen

Die Veröffentlichung von Internet- und Medienmitteilungen war wichtig, um interne als auch externe Zielgruppen über wichtige Ereignisse und Entwicklungen am CYD Campus zu informieren. Wir nutzen Mitteilungen, um Einblicke in neue Studien zu geben, um Veranstaltungen wie Hackathons oder Konferenzen anzukündigen und über unsere Cyber Trainings zu berichten.

Auswahl öffentlicher Mitteilungen

Medienmitteilungen

- Erfolgreiche Zusammenarbeit zwischen dem VBS und dem Schweizer Finanzsektor zum Schutz der Privatsphäre, 28.04.23
- Cyber-Defence Campus lanciert Cyber Startup Challenge 2023, 08.06.23
- Cyber Startup Challenge 2023: Das Startup Ostorlab überzeugt das VBS, 26.10.23

Webmitteilungen

- Kollaborativer Ansatz zur Beseitigung von Cyber-Sicherheitslücken, 27.02.23
- Der Cyber-Defence Campus veröffentlicht seinen Jahresbericht 2022, 03.03.23
- CYD Proof of Concept Fellowship, 16.04.23
- Aufruf für die Cyber Startup Challenge 2023, 08.06.23
- Neuer Cyber-Defence Campus Webauftritt, 20.09.23
- CYD Campus durchleuchtet die Cybersecurity Forschungslandschaft der Schweiz, 29.09.23
- Cyber-Defence Campus Hackathon zu Forensik in Energiesystemen, 24.10.23
- Sicherheit im Zeitalter der KI: Chancen und Risiken, 02.11.23
- Cyber Bedrohungen der generativen Künstlichen Intelligenz, 22.11.23

Besuchen Sie uns auf:

Unserer Website

LinkedIn

Twitter

Das Kommunikationsteam des CYD Campus bei der Arbeit

Ausblick 2024

Im Jahr 2024 wird der Cyber-Defence Campus sein fünfjähriges Jubiläum feiern. Nach fünf Jahren werden wir uns weiterhin darauf fokussieren, die Zusammenarbeit mit der Wirtschaft, Hochschulen sowie Partnerinnen und Partnern im In- und Ausland zu vertiefen. Wir setzen uns zum Ziel, in der fortschreitenden Digitalisierung einen aktiven Beitrag an die Sicherheit zu leisten, Innovationen im Bereich der Cyberverteidigung voranzutreiben sowie wichtige Grundlagen zu erarbeiten. Ziel ist es, das Schweizer Cyberdispositiv und die Armee für die Zukunft zu rüsten.

Der Cyber-Defence Campus wird sich im Jahr 2024 auf die Umsetzung der Strategie Cyber des Departements VBS, der nationalen Cyberstrategie NCS des Bundes und der Gesamtkonzeption Cyber der Armee fokussieren. Dazu gehören unter anderem:

Ausbildung von Expertinnen und Experten und Vorantreiben von Innovationen: Zum gezielten Vorantreiben von Innovationen und zur Ausbildung von Fachleuten im Cyberbereich werden erneut wichtige Anlässe stattfinden. Eine Cyber-Defence Konferenz für das Jahr 2024 sowie verschiedene Cyber Trainings und Hackathons sind bereits in Planung. Auch Studierende können im Rahmen unserer Programme und attraktiven Angebote auf verschiedenen Ebenen profitieren.

Überwachung technologischer Trends: Aufgrund der rasanten Entwicklung im Cyberbereich ist es relevant, technologische Trends und Entwicklungen frühzeitig zu erkennen, um gegen potenzielle Risiken effizient vorzugehen. Der Cyber-Defence Campus wird deshalb den Ausbau seiner Technologie Monitoring Plattform (TMM 2.0) weiterhin vorantreiben. Ziel ist es, bestehende Datenbanken, Websites und Verzeichnisse effizienter zu durchsuchen, um Cyber-Technologien und -Trends frühzeitig zu identifizieren und deren Potenziale für die Schweiz einzustufen.

Stärkung der internationalen Kooperationen: Im Fokus der Tätigkeit des Cyber-Defence Campus steht wie in den vorhergehenden Jahren die Stärkung internationaler Kooperationen. Die internationale Zusammenarbeit im Bereich Cybersicherheit, Künstliche Intelligenz und disruptive Technologien wird eine unserer Prioritäten darstellen, sei es über bilaterale Beziehungen oder über multinationale Gremien (EDA, NATO, etc.).

Ausbau der Kommunikation: Ein weiteres Ziel besteht darin, die Kommunikationskanäle des Cyber-Defence Campus aktiver zu nutzen, um zentrale Erkenntnisse und Publikationen zu teilen und durch den Austausch mit Fachleuten die Cyber Community zu stärken. Expertenmeinungen und Technologieempfehlungen sollen einem breiteren Publikum zugänglich gemacht werden, um die Cyber Resilienz in der Schweiz zu stärken.

Forschung an aufkommenden und disruptiven Technologien: Der Cyber-Defence Campus wird sich mit aufkommenden und disruptiven Technologien wie beispielsweise 5G/6G, Künstliche Intelligenz, zukünftige Netzwerktechnologien, Weltraum, oder Quantum Technologien beschäftigen, um deren Potenzial für die Schweizer Cyber-Defence und für die Schweizer Armee zu untersuchen.

Zusammenarbeit mit der Armee: Der Cyber-Defence Campus plant 2024 die Kooperation mit dem Kommando Cyber und dem Cyber Bataillon 42 weiter zu vertiefen. Ziel ist es, den Fähigkeitsaufbau des neu gegründeten Kommando Cyber im Rahmen der Gesamtkonzeption Cyber zu unterstützen und gemeinsam mit dem bereits 2022 ins Leben gerufenen Bataillon 42 und mit Angehörigen der Armee Synergien zu schaffen.

Dr. Vincent Lenders blickt schon gespannt auf das kommende Jahr am CYD Campus

IMPRESSUM

Herausgeber: Cyber-Defence Campus, armasuisse Wissenschaft und Technologie, Feuerwerkerstrasse 39, CH-3602 Thun
Kontakt: +41 58 462 99 00, cydcampus@armasuisse.ch
Bildernachweis: Wo nicht anders vermerkt: Quelle VBS/DDPS, Pixabay, Adobe Stock, iStock

Kontakt

Cyber-Defence Campus
Feuerwerkerstrasse 39
CH-3602 Thun

Zollstrasse 62
CH-8005 Zürich

EPFL Innovation Park, Bâtiment I
CH-1015 Lausanne

cydcampus.admin.ch
cydcampus@armasuisse.ch
+41 58 462 99 00