Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense, de la protection de la population et des sports
armasuisse
Sciences et technologies

Cyber-Defence Campus

Rapport annuel 2021

Table des matières

IMPRESSUM

Éditeur : Cyber-Defence Campus, armasuisse, Feuerwerkerstrasse 39, CH-3602 Thoune

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

Crédit photo : sauf indication contraire : source VBS/DDPS, Pixabay, Adobe Stock

Avant-propos

À l'instar de l'année précédente, 2021 a été fortement marquée par la pandémie du COVID-19. Outre les répercussions négatives telles que la surcharge du système de santé ou l'augmentation des dépenses publiques, la pandémie a également entraîné une accélération rapide de la digitalisation. Les cybermenaces ont ainsi nettement gagné en importance et en complexité, impactant de plus en plus la sécurité de notre société.

Nos collaborateurs et partenaires du Cyber-Defence (CYD) Campus apportent chaque jour une contribution importante à la cybersécurité de la Suisse en s'engageant dans la recherche, l'innovation, la transmission de connaissances ou la formation de talents. Depuis sa création il y a trois ans, le CYD Campus a mis en œuvre plusieurs objectifs stratégiques du plan d'action pour la cyberdéfense, de la Stratégie cyber du DDPS et de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). En 2021, des progrès et des résultats significatifs ont notamment été obtenus dans les domaines ci-après.

La recherche systématique de nouvelles technologies et start-up a été étendue à six autres pays. Outre la veille des technologies et des marchés déjà établi en Suisse, aux États-Unis et à Singapour, les développements et tendances cyber font désormais l'objet d'un suivi actif au Royaume-Uni, en Allemagne, en Autriche, en France, en Israël et en Estonie en collaboration avec un réseau de partenaires internationaux. Les derniers développements dans ces régions sont régulièrement analysés et étudiés avec les services compétents de la Confédération dans le cadre d'études et de preuves de concept (« proof of concept »). Rien que l'année passée, une douzaine de preuves de concept ont ainsi été réalisées avec des partenaires. Un logiciel innovant d'une start-up du CYD Campus a par exemple été utilisé dans le cadre du premier projet pilote de la formation prémilitaire cyber de l'armée.

Sur le plan de la recherche, la collaboration avec des hautes écoles comme l'EPF Zurich, l'EPF Lausanne, la ZHAW ou encore l'université de Lausanne a été renforcée et étendue à de nouveaux domaines technologiques comme la cryptographie post-quantique, la lutte contre la désinformation ou la protection des infrastructures critiques afin de répondre aux besoins en matière de défense. L'organisation d'événements tels que les séminaires dînatoires, les hackathons, les conférences ou encore la nouvelle édition du Cyber Startup Challenge ont contribué par ailleurs à renforcer et développer la communauté de la cyberdéfense suisse. Je me réjouis du fait que cette année, dix étudiants d'universités suisses ont effectué leur travail de recherche en qualité de CYD Fellow et que 35 autres étudiants de hautes écoles ont effectué un stage ou un mémoire de master au sein du CYD Campus dans le cadre du programme d'encouragement des talents.

Le présent rapport annuel dresse un état des lieux des activités publiques non classifiées du CYD Campus en 2021.
Je vous souhaite une bonne lecture.

Thoune, le 31 décembre 2021

Dr Vincent Lenders
Directeur Cyber-Defence Campus

1 À propos du Cyber-Defence Campus

1.1 Intégration de la stratégie et principales missions

Face à un écosystème en mutation permanente et à la menace croissante des cyberattaques dans tous les domaines, le gouvernement suisse a fait de la cyber-sécurité un enjeu de sécurité nationale majeur. Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) renforce l'utilisation de ressources pour la cyberdéfense et en fait une priorité stratégique et opérationnelle. C'est pourquoi le premier plan d'action pour la cyberdéfense (PACD) a été élaboré en 2016. Eu égard au développement fulgurant des cybermenaces au cours des cinq dernières années, la nouvelle « Stratégie cyber DDPS », qui s'appuie sur le plan d'action, a été mise au point pour la période 2021-2024. Le plan d'action ainsi que la nouvelle « Stratégie cyber DDPS » sont coordonnés avec la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC).

Stratégie cyber DDPS 2021-2024

Dans le cadre du PACD et de la « Stratégie cyber DDPS », le DDPS développe et gère depuis trois ans le Cyber-Defence (CYD) Campus. Rattaché à l'Office fédéral de l'armement (armasuisse), le CYD Campus offre au DDPS une plateforme d'anticipation et de connaissances pour l'identification et l'évaluation des cyber-tendances technologiques, économiques et sociales. Afin de pouvoir collaborer le plus étroitement possible avec les hautes écoles, le DDPS et l'industrie, le CYD Campus est présent sur trois sites : sur le site principal à Thoune (armasuisse Sciences et technologies), à l'EPF Lausanne et à l'EPF Zurich. Cela lui permet de développer efficacement son savoir-faire et de fournir une cyber-expertise correspondant aux besoins de la Confédération suisse. Le CYD Campus fait ainsi le lien entre le secteur privé, l'administration publique et la science.

La cheffe du DDPS, la conseillère fédérale Viola Amherd, fixe les champs d'action et la répartition des tâches correspondante dans l'orientation de la « Stratégie cyber DDPS ». Actuellement, les trois principales missions du CYD Campus sont les suivantes:

Principales compétences du Cyber-Defence Campus

Identification précoce des tendances dans le domaine cyber: cette activité comprend une veille exhaustif des technologies et des marchés, la recherche de start-up à l'échelle internationale ainsi que l'entretien d'un réseau de coopération.

Recherche et innovation dans le domaine des cybertechnologies: la collaboration avec des hautes écoles et l'industrie permet d'identifier les cyberrisques émergents et de concevoir des solutions innovantes afin de contrer efficacement les menaces dans le cyberespace.
Le CYD Campus a également pour but d'assurer et de renforcer la sécurité et la résilience des systèmes cyber actuels.

Formation de cyber-spécialistes: le CYD Campus forme des talents de niveau master, doctorat et postdoc ainsi que des stagiaires de haute école pour les préparer à relever les défis de demain. Les experts du CYD Campus définissent et encadrent également un grand nombre de projets d'étudiants.

L'objectif de ce rapport annuel consiste à fournir une vue d'ensemble de la mise en œuvre des tâches susmentionnées en 2021 par le Cyber-Defence Campus. Il donne pour cela un bref aperçu de quelques temps forts de l'année 2021. Il présente également les activités publiques dans le cadre de projets de recherche, de mandats de clients et de démonstrateurs. Il aborde aussi les travaux de 2021 relatifs à l'extension des infrastructures des laboratoires et présente les activités de veille des technologies et des marchés. Les derniers chapitres de ce rapport donnent un aperçu des événements, des publications et des conférences, ainsi que des perspectives pour 2022.

1.2 Partenaires

Sur le plan organisationnel, le CYD Campus est rattaché à armasuisse Sciences et technologies (DDPS). Une cinquantaine d'autres organisations suisses et étrangères issues de la science, de l'industrie et du secteur public participent en qualité de partenaires.

Partenaires publics/Confédération

- Armée suisse
- Service de renseignement de la Confédération SRC
- Police fédérale fedpol
- Office fédéral de la statistique OFS
- Swisstopo
- Centre national pour la cybersécurité NCSC
- Office fédéral de l'aviation civile OFAC
- Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCDCoE)
- Laboratoire de recherche de l'armée de l'air américaine
- Laboratoire de recherche de l'armée américaine
- Armée luxembourgeoise
- Agence européenne de défense AED
- Office fédéral de la sécurité des technologies de l'information (BSI) Allemagne
- Swissnex

Hautes écoles

- EPF Lausanne
- Center for Digital Trust (C4DT)
- EPF Zurich
- Zurich Information Security and Privacy Center (ZISC)
- Académie militaire de l'EPFZ
- Université de Fribourg
- Université de Zurich
- Université de Lausanne
- Université de Neuchâtel
- Université d'Oxford, Royaume-Uni
- UCLouvain, Belgique
- IMDEA, Espagne
- Université de Murcie, Espagne
- Université Roi Juan Carlos, Espagne
- Université technique de Kaiserslautern, Allemagne
- ZHAW
- FHNW
- IDSIA
- Northeastern University, États-Unis
- HEIG-VD
- Université de Genève
- HES-SO
- HEPIA

Partenaires industriels

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

1.3 Personnes

La direction du CYD Campus est composée de collaborateurs spécialisés en Cybersécurité et en Data Science d'armasuisse S+T.

Direction du CYD Campus

Dr. Vincent Lenders

Directeur du CYD Campus et chef du domaine spécialisé

Stefan Engel

Responsable Business Development et directeur suppléant du CYD Campus

Dr. Gérôme Bovet

Responsable du programme de recherche et du groupe de Data Science

Dr. Colin Barschel

Responsable Innovation et collaborations industrielles

Giorgio Tresoldi

Responsable Relations internationales et du Scouting

Dr. Alain Mermoud

Responsable veille technologique et marchés

Monia Khelifi

Direction de l'assistance

Collaborateurs spécialisés en cybersécurité

Le Dr Martin Strohmeier est expert en sécurité de systèmes cyber-physiques et chef de projet scientifique

Daniel Hulliger est pentester, chercheur de vulnérabilité et chef de projet technique

Damian Pfammatter est pentester, chercheur de vulnérabilité et chef de projet scientifique

Llorenç Roma est pentester et chef de projet scientifique (arrivée en avril 2021)

Le Dr Daniel Moser est expert en sécurité des infrastructures critiques et des communications sans fil et chef de projet scientifique

Le Dr Miguel Keer est chef de projet scientifique

Le Dr Luca Gambazzi est auditeur de sécurité et chef de projet scientifique (départ en août 2021)

William Lacube est responsable de la collaboration avec le Centre d'excellence de cyberdéfense coopérative de l'OTAN en Estonie et chef de projet scientifique

Le Dr Carlo Matteotti est cryptologue et encadre les étudiants et les CYD Fellows en qualité de CYD Mentor

Collaborateurs spécialisés en Data Science

Le Dr Gérôme Bovet est responsable du groupe Data Science et directeur de programme de recherche

Le Dr Étienne Voutaz est Data Scientist et chef de projet scientifique

Le Dr Ljiljana Dolamic est experte en traitement automatique des langues et cheffe de projet scientifique

Le Dr Albert Blarer est Data Scientist et chef de projet scientifique

Le Dr Metin Feridun est spécialiste en big data et chef de projet scientifique

Le Dr Mathias Humbert est expert en apprentissage automatique et en protection de la vie privée ainsi que chef de projet scientifique (départ en novembre 2021)

Le Dr Raphael Meier est expert en traitement d'images et en apprentissage automatique ainsi que chef de projet scientifique (arrivée en mai 2021)

Thomas Sigrist est responsable des infrastructures informatiques et chef de projet technique (départ en décembre 2021)

Ivo Stragiotti est responsable des infrastructures des laboratoires et chef de projet technique (arrivée en juillet 2021)

Stagiaires de haute école

Afin d'accroître la cyber-expertise des étudiants et de renforcer à long terme la résilience de la Suisse face aux cybermenaces, le Cyber-Defence Campus propose des stages en haute école sur les trois sites de Thoune, Lausanne et Zurich. En 2021, 24 étudiants ont effectué un stage au Cyber-Defence Campus. Les stagiaires proviennent de différentes universités telles que l'EPF Lausanne, l'EPF Zurich ou l'université de Saint-Gall.

Huzar Marin, Septembre 21 - Février 22, Cybersécurité, Lausanne

Durussel Samad Emrys, Septembre 21 - Février 22, Data Science, Lausanne

Benjamin Kilian, Septembre 21 - Février 22, Cybersécurité, Lausanne

Eloi Garandel, Septembre 21 - Février 22, Data Science, Lausanne

Marie Reignier Tayar, Février 21 - Janvier 22, Data Science, Lausanne

Michael Tsesmelis, Juin 21 - Mai 22, Veille technologique et du marché, Lausanne

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

Sarah Frei, Avril 21 - Mars 22, Communication, Thun

William Lacube, Mars 21 - Décembre 21, Veille technologique et du marché, Lausanne

Valentyna Pavliv, Mars 21 - Août 21, Data Science, Lausanne

Eric Jolles, Mars 21 - Décembre 21, Veille technologique et du marché, Lausanne

Victor Cochard, Mars 21 - Août 21, Data Science, Lausanne

Caroline Violot, Février 21 - Julliet 21, Data Science, Lausanne

Anton Santiago Moreno, Février 21 - Julliet 21, Veille technologique et du marché, Lausanne

Valérian Rey, Octobre 20 - Mars 21, Data Science, Lausanne

Marc Kaufmann, Octobre 20 - Juin 21, Data Science, Zurich

Stéphanie Lebrun, Octobre 20 - Mars 21, Data Science, Lausanne

Etienne Bonvin, Octobre 20 - Mars 21, Data Science, Lausanne

Adrien Prost, Octobre 20 - Mars 21, Data Science, Lausanne

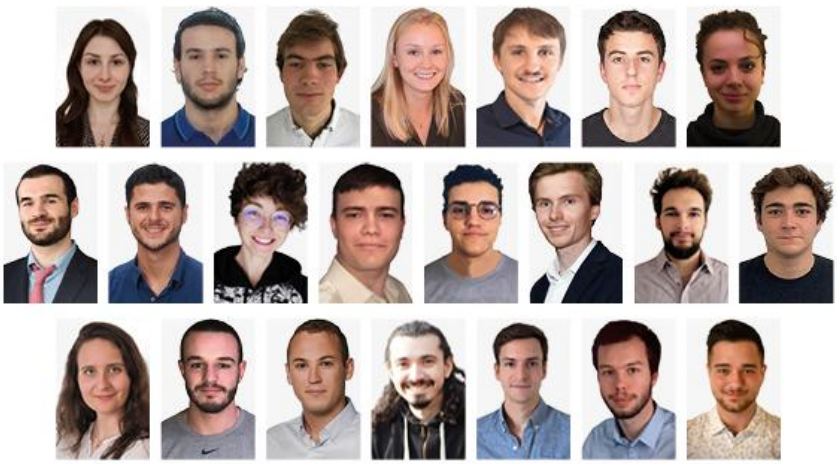
Benno Schneeberger, Septembre 20 - Février 21, Cybersécurité, Lausanne

Ejub Talovic, Septembre 20 - Février 21, Veille technologique et du marché, Lausanne

Edoardo Debenedetti, Août 20 - Janvier 21, Data Science, Lausanne

Robin Leurent, Août 20 - Janvier 21, Data Science, Lausanne

Llorenç Roma, Avril 20 - Mars 21, Cybersécurité, Thoune



CYD Fellows

En 2020, le CYD Campus a lancé un programme de Cyber-Defence (CYD) Fellowship en collaboration avec l'EPF Lausanne afin de permettre aux étudiants d'approfondir les thèmes de la cyberdéfense et d'y renforcer les compétences en Suisse. Les étudiants peuvent ainsi contribuer dès leurs études à la recherche sur la cyberdéfense pour la Suisse. Les CYD Fellowships constituent un programme d'encouragement des talents compétitif qui met à la disposition des étudiants un expert du CYD pour superviser leur travail de recherche. Les CYD Fellows sont inscrits dans une haute école suisse et mènent leurs recherches dans les locaux du CYD Campus à l'EPF Lausanne, à l'EPF Zurich ainsi qu'au siège à Thoune. Attribués plusieurs fois par an à des étudiants en master, à des doctorants ainsi qu'à des postdoctorants, les CYD Fellowships leur permettent de bénéficier d'un remboursement des frais de subsistance. En 2021, dix Fellows étaient actifs :

Lina Gehri, Master Thesis Fellow, ETHZ, Novembre 21 - Avril 22, intitulé de projet: *Analyzing and Comparing Defense Strategies in a Cyber Defense Exercise*, CYD mentor: Le Dr Vincent Lenders

Jan Urech, Master Thesis Fellow, ETHZ, October 21 - Avril 22, intitulé de projet: *Developing an Automated Defender for Cyber Security Exercises*, CYD mentor: Daniel Hulliger

Ksandros Apostoli, Master Thesis Fellow, EPFL, Septembre 21 - Février 22, intitulé de projet: *Privacy-Preserving Proof-of-Personhood Token*, CYD mentor: Le Dr Daniel Moser

Simran Tinani, PhD Fellow, UZH, Septembre 21 - Août 23, intitulé de projet: *Nonabelian Groups in Cryptography*, CYD mentor: Le Dr Carlo Matteotti

Louis Merlin, Master Thesis Fellow, EPFL, Mars - Août 21, intitulé de projet: *Recovering type information from compiled binaries to aid in instrumentation*, CYD mentor: Damian Pfammatter

Anita Mezzetti, Master Thesis Fellow, EPFL, Février - Juillet 21, intitulé de projet: *Modelling portfolios of cyber-related emerging technologies: a complex-system approach*, CYD mentor: Le Dr Alain Mermoud

Dr. **Andrei Kucharavy**, Postdoc Fellow, EPFL, Décembre 20 - November 22, intitulé de projet: *Evolutionary dynamics for improved GAN detection*, CYD mentor: Le Dr Ljiljana Dolamic

Dina Mahmoud, PhD Fellow, EPFL, Septembre 20 - Août 24, intitulé de projet: *ADHeS: Attacks and Defenses on FPGA-CPU Heterogeneous systems*, CYD mentor: Le Dr Vincent Lenders

Zuowen Wang, Master Thesis Fellow, ETHZ, Septembre 20 - Février 21, intitulé de projet: *Understanding and enhancing adversarial robustness for machine learning models*, CYD mentor: Le Dr Gérôme Bovet

Dr. **Dimitri Percia David**, Postdoc Fellow, UNIGE, Août 20 - Julliet 22, intitulé de projet: *Technology Forecasting and Market Monitoring for Cyber-Defence*, CYD mentor: Le Dr Alain Mermoud

Étudiants

Les collaborateurs du CYD Campus définissent et encadrent des projets d'étudiants au niveau bachelor, master et doctorat. Les étudiants réalisent leurs projets dans les locaux du CYD Campus à l'EPFL, à l'EPFZ ainsi que sur le campus de Thoune. En 2021, les travaux de onze étudiants ont été suivis par le CYD Campus.

Pedro Miguel Sanchez, Université de Murcia, Septembre 21 - Décembre 21,Tuteur: Le Dr Gérôme Bovet

Marco di Nardo, ETHZ, Septembre 21 - Février 22, Tuteur: Le Dr Daniel Moser

Dominique Portenier, ETHZ, Septembre 21 - Février 22, Tuteur: Le Dr Daniel Moser

Silvio Geel, ETHZ, Septembre 21 - Février 22, Tuteur: Le Dr Daniel Moser

Florian Lerch, ETHZ, Septembre 21 - Janvier 22, Tuteur: Le Dr Martin Strohmeier

Philippe Panhaleux, ETHZ, Mars 21 - Août 21, Tuteur: Le Dr Martin Strohmeier

Julian Huwyler, ETHZ, Mars 21 - Août 21, Tuteur: Le Dr Martin Strohmeier

Leeloo Granger, ETHZ, Mars 21 - Août 21, Tuteur: Le Dr Martin Strohmeier

Jannik Brun, ETHZ, Mars 21 - Août 21, Tuteur: Le Dr Martin Strohmeier

Michael Karpf, ETHZ, Mars 21 - Août 21, Tuteur: Le Dr Martin Strohmeier

Georg Baselt, ETHZ, Février 21 - Julliet 21,Tuteur: Le Dr Martin Strohmeier

2 Highlights

Car Hackathon

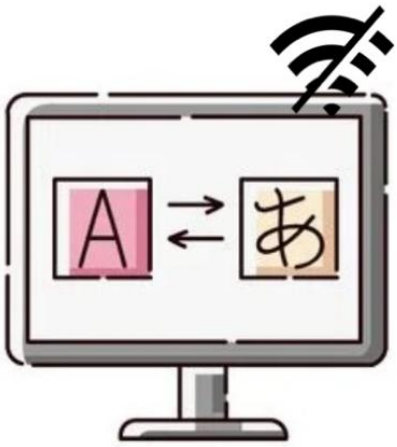
Les voitures sont de plus en plus intelligentes. Les nouvelles fonctions apportent certes plus de confort et de sécurité, mais engendrent également de nombreuses failles de cybersécurité. Celles-ci surviennent non seulement au niveau de systèmes potentiellement critiques tels que les freins ou le moteur, mais aussi au niveau de composants accessibles de l'extérieur, comme les interfaces sans fil du système multimédia. Ce danger est encore aggravé par l'introduction des véhicules électriques dans lesquels tous les systèmes sont généralement connectés sur un seul bus de données. L'infrastructure de recharge de ces véhicules soulève d'autres questions en matière de fiabilité et de sécurité (panne de la borne, échange de données entre la borne et le véhicule, etc.). Le nombre croissant de capteurs tels que les radars, les lidars, les caméras et leur dépendance à l'égard de l'intelligence artificielle pour analyser la grande quantité de données qu'ils génèrent engendrent également de nouvelles vulnérabilités.

Un hackathon de cinq jours a été organisé à Thoune en octobre 2021 afin de développer rapidement l'expertise du CYD Campus et de l'administration fédérale. Au total, 20 participants de l'EPF Zurich, de l'université d'Oxford, de fedpol, de l'armée et d'armasuisse ont décelé, avec le soutien d'experts de la société japonaise White Motion, des problèmes de sécurité potentiels sur sept véhicules différents (différents fabricants, militaires/civils, électriques/non électriques) et ont fait leurs premiers pas dans ce domaine de recherche. La composition des participants a permis un échange interdisciplinaire intensif et fructueux. De plus, plusieurs démonstrateurs qui interviendront au sein du CYD Campus ont été assemblés. Enfin, des données ont été collectées et seront utilisées pour la recherche en collaboration avec des universités dans les années à venir.

Formation avec des experts et analyse de vulnérabilités pendant le Car Hackathon à Thoune

Service de traduction hors ligne dans l'armée

Aujourd'hui, de nombreux programmes de traduction automatique sont disponibles en ligne. Ils permettent de traduire un grand nombre de langues avec une qualité de traduction variable qui dépend d'une part de l'outil proprement dit et d'autre part des langues concernées. Les services de traduction en ligne ont toutefois engendré de nombreux problèmes de sécurité, puisque des contenus impliquant des données personnelles ou confidentielles peuvent circuler vers l'extérieur. Dans le cadre d'un projet d'innovation, une validation de principe a été réalisée pour un outil de traduction automatique interne fonctionnant hors ligne et capable de fournir des traductions bidirectionnelles compréhensibles entre l'anglais et six autres langues. Avec l'allemand, le français, l'italien, le russe, l'arabe et le chinois comme langues source et cible, la faisabilité de cet outil a été démontrée pour une utilisation dans des systèmes de l'armée, indépendamment de la complexité linguistique ou du système d'écriture.



Le Dr Mathias Humbert est nommé professeur en cybersécurité à l'université de Lausanne

Le Dr Mathias Humbert, collaborateur scientifique du CYD Campus, a été promu professeur à l'université de Lausanne en novembre 2021. Au cours de ses deux années de travail au CYD Campus, Mathias Humbert a encadré de nombreux projets d'étudiants, acquérant ainsi de précieuses expériences pour ce nouveau défi. Professeur à l'université de Lausanne, il continuera de promouvoir la collaboration à long terme entre le CYD Campus et son département dans le domaine de la cybersécurité et de la protection des données. L'un des principaux objectifs stratégiques du CYD Campus est de promouvoir les cybertalents dans l'optique de renforcer la sécurité de la Suisse.

Failles de sécurité identifiées dans un logiciel VPN

Dans le cadre du programme Vulnerability Research, des solutions de logiciel VPN de différents fabricants ont été examinées afin d'identifier des vulnérabilités. Un chercheur du CYD Campus a notamment décelé une importante faille de sécurité dans le client VPN de la société américaine F5. Inconnue jusqu'alors, cette faille a été exploitée par des utilisateurs non autorisés pour obtenir les droits d'administrateur des systèmes clients Windows sur lesquels le logiciel VPN est installé. Le logiciel VPN concerné est utilisé par de nombreuses entreprises suisses pour permettre aux collaborateurs d'accéder à distance au réseau interne de l'entreprise. La pandémie de Covid-19 et le télétravail obligatoire qui en a découlé ont généralisé le recours aux VPN. La faille a pu être comblée grâce à un signalement rapide du CYD Campus au fabricant en février 2021.

La mise à jour de sécurité correspondante a été publiée le 1er juin 2021. Cette étape-clé illustre la pertinence et l'efficacité de la recherche en matière de vulnérabilités menée par le CYD Campus afin d'assurer la sécurité de la Suisse.

Conférence du CYD Campus et CRITIS

Le 28 septembre 2021, la conférence du CYD Campus s'est tenue au SwissTech Convention Center de l'EPFL à Lausanne et a été diffusée simultanément en ligne en raison de la pandémie en cours. La conférence a accueilli 130 participants sur place et 80 autres ont suivi l'événement en ligne. De nombreux experts du milieu académique, de l'administration fédérale et de l'économie sont intervenus, abordant des sujets-clés relatifs à la sécurité des infrastructures d'information critiques. L'événement a constitué une plateforme d'échange autour des défis et enjeux actuels et futurs du cyberespace. L'après-midi, à l'issue des pitchs des trois finalistes du Cyber Startup Challenge, la start-up zurichoise Decentriq a été élue gagnante. La conférence a été organisée en collaboration avec la 16e conférence internationale sur la sécurité des infrastructures d'information critiques (CRITIS 2021), qui s'est déroulée au même endroit du 27 au 29 septembre.

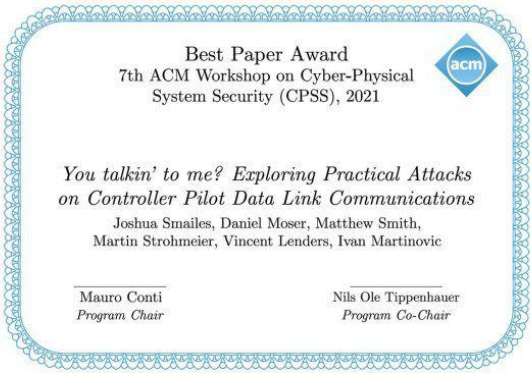
Participants à la conférence du CYD Campus et à CRITIS 2021 à Lausanne

Programme de la conférence – CRITIS 2021

CYD Campus Awards

Best Paper Award au Cyber-Physical System Security Workshop

Trois scientifiques du CYD Campus ont reçu, conjointement avec des chercheurs de l'université d'Oxford, le Best Paper Award du 7e ACM Cyber-Physical System Security (CPSS) Workshop. Dans le cadre de leur travail de recherche, les scientifiques démontrent qu'en prenant le contrôle de la liaison entre les contrôleurs aériens et l'équipage des avions, l'auteur d'une cyberattaque peut prétendre être un contrôleur légitime et donner de fausses instructions à l'avion-cible. Cette faille présenterait un risque significatif pour la sécurité des avions. Ils ont élaboré par ailleurs trois contre-mesures pour maîtriser ces risques de sécurité dans l'espace aérien. Ces contre-mesures vont d'un contrôle de plausibilité et du déclenchement d'une alarme à l'utilisation de signatures ou encore d'un chiffrement des données.


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

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

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

Mauro Conti, *Program Chair*

Nils Ole Tippenhauer, *Program Co-Chair*

Prix « Best Paper Award » de l'ACM

Vers la publication

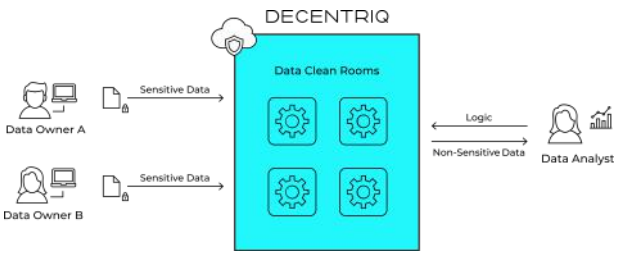
Stéphanie Lebrun présente son travail à la conférence CRITIS 2021, qui a été récompensé par le Young CRITIS Award

Young CRITIS Awards

Dans le cadre de la conférence CRITIS 2021, le Young CRITIS Award a été décerné afin d'encourager et de soutenir les jeunes scientifiques qui effectuent des recherches dans le domaine de la protection des infrastructures critiques. CRITIS 2021 a récompensé les meilleurs travaux de trois jeunes scientifiques. Santiago Anton Moreno et Stéphanie Lebrun, tous deux stagiaires de haute école au CYD Campus, se sont classés respectivement deuxième et troisième et ont obtenu un total de 1500 francs pour leurs contributions. Santiago Anton Moreno a développé des modèles permettant d'évaluer le marché et les technologies de cybersécurité afin de faciliter les décisions en matière d'investissements visant à garantir la sécurité des infrastructures critiques. Dans le cadre de son travail, Stéphanie Lebrun s'est penchée sur la sécurité des infrastructures GNSS.

Cyber Startup Challenge

Le Cyber Startup Challenge 2021 avait pour objectif de découvrir le paysage technologique des start-up autour du thème « Boostez votre centre de partage et d'analyse d'informations (Information Sharing and Analysis Center, ISAC) » et était axé sur la recherche de solutions innovantes dans le domaine de la détection de cybermenaces avec une focalisation sur la protection des infrastructures critiques. 38 start-up d'Europe, des États-Unis et d'Asie ont participé au challenge. Le jury, composé de cyber-experts du DDPS et d'armasuisse S+T, a sélectionné les trois finalistes Decentriq, Constella Intelligence et Pandora Intelligence, qui ont présenté un pitch lors de la conférence du CYD Campus le 28 septembre 2021. La start-up zurichoise Decentriq a finalement convaincu le jury avec sa plateforme Software as a Service (SaaS) innovante, qui propose des « data clean rooms » aux entreprises. Cette technologie permet aux acteurs internes et externes des infrastructures critiques d'échanger des données en toute sécurité et d'obtenir des aperçus agrégés et anonymes. Cela renforce leur cybersécurité sans compromettre la protection des données. En 2022, Decentriq va intégrer, conjointement avec le CYD Campus, une preuve de concept de sa technologie dans un environnement réel du DDPS.



Solution proposée par DECENTRIQ, lauréat du Cyber Startup Challenge 2021

3 Programme d'encouragement des talents du CYD

Les spécialistes du domaine de la cybersécurité et de la science des données sont rares en Suisse et dans de nombreux autres pays. La promotion et la formation de nouveaux cybertalents constituent par conséquent un défi majeur et font donc également partie des trois principales missions du CYD Campus. Le CYD Campus adopte différentes approches pour accroître les compétences des étudiants.

D'une part, il propose des stages de haute école sur les trois sites de Zurich, Lausanne et Thoune. D'autre part, des projets d'étudiants encadrés par des chercheurs du CYD Campus sont définis au niveau bachelor, master et doctorat. Inscrits dans l'université suisse de leur choix, ces étudiants sont encadrés par un mentor du CYD Campus. En outre, le CYD Campus a lancé en 2020, en collaboration avec l'EPFL, le programme CYD Fellowship afin de permettre et d'encourager les étudiants à étoffer leurs compétences dans le domaine de la cyberdéfense.

En 2021, 24 stagiaires de haute école ont été acceptés et onze travaux d'étudiants ont été supervisés par des scientifiques du CYD Campus. Par ailleurs, dix CYD Fellows étaient actifs.

L'objectif est de promouvoir une nouvelle génération de cybertalents. Le CYD Campus apporte ainsi une contribution significative à la lutte contre la pénurie de personnel qualifié dans le domaine hautement spécialisé de la cyberdefence, avec pour objectif à long terme de garantir les cyber-compétences nécessaires au gouvernement, à la science et à l'économie en Suisse.

Quelques CYD Fellows à Lausanne

Stagiaire de haute école lors de sa formation cyber au CYD Campus de Lausanne

4 Recherche

La recherche du CYD Campus est un investissement visant à garantir durablement l'expertise et les compétences scientifiques et techniques nécessaires à l'accomplissement des tâches et activités de la Confédération dans le domaine de la cyberdéfense. Partie intégrante de la gestion technologique, elle constitue également la base d'une solide planification des technologies futures et des projets d'innovation du DDPS. Elle contribue ainsi au développement des capacités opérationnelles de cyberdéfense qui seront nécessaires à l'avenir, ainsi qu'à l'étayage scientifique et technique des planifications et acquisitions du DDPS.

Les projets de recherche sont réalisés en collaboration avec les hautes écoles et les partenaires industriels.

4.1 Projets dans le domaine de la cybersécurité

Systèmes d'exploitation mobiles sécurisés

Les appareils mobiles (smartphones) sont indispensables pour travailler efficacement, mais leur mobilité et leur connectivité offrent de nombreuses possibilités d'attaques. La protection des informations confidentielles et sensibles s'avère donc particulièrement difficile. L'objectif est d'utiliser un appareil mobile disponible dans le commerce pour l'échange de données dans le cadre d'informations et d'applications sensibles. Cet appareil permet d'échanger des informations, que ce soit lors d'un appel, d'un message ou via une application, jusqu'au niveau « confidentiel ». Le principal défi consiste à trouver la meilleure architecture pour un système d'exploitation mobile sécurisé garantissant un équilibre entre sécurité, faisabilité et convivialité. Deux approches sont poursuivies pour protéger les données sensibles : la première consiste à compartimenter les risques. Autrement dit, la surface d'attaque est cloisonnée afin de minimiser l'impact d'une attaque. Pour ce faire, deux architectures ont été développées pour un système d'exploitation mobile sécurisé, analyse des risques comprise. La cybersécurité concerne non seulement le système d'exploitation mobile mais aussi le matériel, les composants cryptographiques et le durcissement de la séquence de démarrage (signatures). La deuxième approche tente de séparer l'exécution d'une application du système d'exploitation et du fabricant afin de garantir la souveraineté sur l'application et d'accroître la sécurité.

L'intelligence artificielle au service de la cyberdéfense : Blue Team Automation

En raison de la complexité et de la rapidité des attaques, il devient de plus en plus difficile de protéger les installations et les processus critiques. En réponse à cela, le projet Fast-Blue développe le modèle cognitif d'une équipe de cybersécurité. Le projet vise à mettre en place une méthodologie automatisée capable de corréler et d'analyser des flux de cyberdonnées et de permettre des enquêtes approfondies sur les menaces ainsi que des mesures de prévention. Ce modèle est alimenté par des flux de travail automatisés et un banc d'essai afin de proposer et de recommander des mesures de réaction et de protection. Le Blue Team doit sonder l'environnement, durcir les systèmes, et identifier et réagir aux activités du Red Team. Ce système de cyberdéfense entièrement automatisé n'aurait plus besoin d'assistance humaine pour identifier et combattre les attaques dans une infrastructure complexe. Le travail réalisé en 2021 s'est focalisé sur les mécanismes de détection et la corrélation des événements du système d'exploitation. La corrélation à l'aide de graphiques permet de remonter à l'origine de ces événements et ainsi de les identifier comme des attaques potentielles. La corrélation a été étendue à Windows et peut également détecter des mouvements transversaux entre Linux et Windows. Les détections sont basées sur des scénarios d'attaque prédéfinis, l'objectif étant qu'à l'avenir, le système soit en mesure de détecter les attaques de manière autonome.

Détection de vulnérabilités des logiciels et appareils : applications Microsoft Windows

La recherche sur les vulnérabilités dans le domaine des systèmes et applications basés sur Windows vise à déceler des failles de sécurité inconnues. En se concentrant sur les logiciels utilisés par les parties prenantes (organisations au sein du DDPS, mais aussi par le reste de l'administration fédérale), il en résulte, outre les activités de recherche, un avantage directement mesurable pour la sécurité informatique de l'administration fédérale.
Parallèlement au développement de compétences pour trouver et exploiter les points faibles, plusieurs failles de sécurité (dont certaines failles critiques) ont été identifiées l'année dernière et communiquées aux parties prenantes sous forme d'advisories. Les fabricants concernés ont été informés en détail sur les vulnérabilités et encouragés à y remédier le plus rapidement possible par la mise à disposition de validations de principe concernant des exploits pleinement fonctionnels.

Identification de vulnérabilités des logiciels et appareils : appareils IoT

Les appareils connectés, souvent appelés « Internet des Objets » (Internet of Things, IoT), sont aujourd'hui omniprésents et leurs applications sont souvent critiques en termes de sécurité. La détection de vulnérabilités potentielles dans de tels appareils est donc primordiale, mais représente souvent un défi. Notamment car un analyste n'a généralement pas accès au code source des programmes exécutés sur l'appareil, qui ne sont donc disponibles que sous forme de code binaire exécutable par la machine. Contrairement au code source, qui est plus facile à comprendre pour l'homme, de nombreuses abstractions (p. ex. noms de fonctions) ne sont plus disponibles, ce qui complique fortement l'analyse. En outre, le code binaire dépend de l'architecture du processeur en question, qui se différencie souvent davantage pour les appareils IoT (p. ex. ARM, MIPS) que pour les ordinateurs traditionnels (généralement x86). Dans le cadre de ce projet de recherche, des techniques d'analyse (semi-)automatisée de fichiers binaires IoT sont testées, et la faisabilité est démontrée à l'aide d'outils de validation de principe correspondants.

Identification de vulnérabilités des logiciels et appareils : noyau Linux

Le noyau du système d'exploitation Linux (en anglais : Linux kernel) constitue aujourd'hui la base de divers systèmes d'exploitation, qui sont utilisés à leur tour sur une multitude d'appareils (ordinateurs de bureau, systèmes de serveurs, petits appareils mobiles ou électroniques, etc.). Une approche pratique pour identifier les problèmes de sécurité potentiels dans le noyau Linux consiste à utiliser un « kernel fuzzer » (tests de noyau à données aléatoires), dont le but est d'identifier un éventuel comportement erroné dans le noyau sur la base d'entrées imprévues. Le plus connu de ces tests aléatoires pour le noyau Linux est syzkaller. Pour la version actuelle du noyau, une instance publique de syzkaller répertorie plus de 1000 comportements erronés de ce type, dont on ne sait toutefois pas s'ils sont effectivement exploitables, c.-à-d. s'il s'agit de véritables vulnérabilités. Dans le cadre de ce projet de recherche, on travaille à une procédure automatisée permettant d'évaluer cette exploitabilité. Cette procédure est essentielle pour évaluer la criticité des comportements erronés identifiés et pour pouvoir y remédier en fonction des priorités.

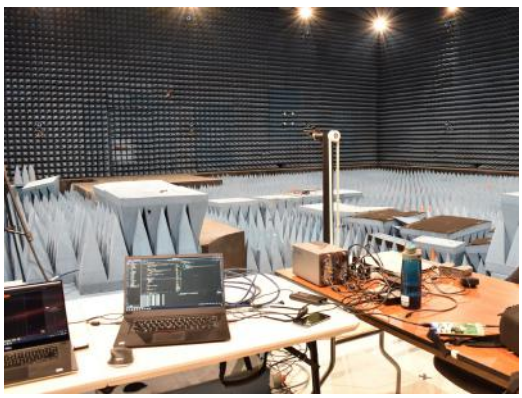
Plateformes d'information sur les cybermenaces

Les informations relatives à la cybersécurité sont généralement extrêmement sensibles et confidentielles, ce qui rend les organisations réticentes à partager ces données avec des tiers, même si une analyse agrégée des menaces communes présenterait des avantages considérables en termes de réactivité et d'adaptation. En réponse à ce conflit d'objectifs, les chercheurs du CYD Campus développent une plateforme offrant des garanties technologiques que les utilisateurs autorisés ne peuvent accéder qu'aux connaissances globales (modèles de cybermenaces) basées sur les données de l'ensemble du réseau. Chaque institution conserve ainsi le contrôle total de ses ensembles de données. Cela est rendu possible d'une part par le développement d'une architecture distribuée compatible avec la plateforme de partage de renseignements sur les menaces (Malware Information Sharing Platform, MISP) sans base de données centralisée, et d'autre part par l'intégration de techniques cryptographiques avancées basées sur le modèle de chiffrement homomorphe multipartite. Cela permet aux institutions de collaborer en toute sécurité autour de données sensibles importantes qui ne sont habituellement pas utilisées en commun, ouvrant la porte à des analyses et prédictions des menaces inédites et plus performantes.

Cryptographie à sécurité quantique

Les progrès de la recherche sur les ordinateurs quantiques posent des défis sur le plan de la cryptologie. Les normes de signature numérique (Digital Signature Schemes – DSS) ainsi que les systèmes de cryptographie asymétriques (Public Key Encryption – PKE) et les mécanismes d'encapsulation de clé (Key Encapsulation Mechanism – KEM) utilisés jusqu'à présent, qui sont sûrs par rapport aux « ordinateurs standards » existants, peuvent être cassés par les ordinateurs quantiques. C'est pourquoi l'Institut national des normes et de la technologie (National Institute of Standards and Technology, NIST) a commencé à sélectionner et à normaliser des successeurs à sécurité quantique pour les mécanismes classiques à clé publique. En juillet 2020, le troisième cycle d'évaluation a été lancé. Sept finalistes et huit candidats alternatifs ont été retenus parmi les candidats des tours précédents. Ce projet de recherche examine les candidats du dernier cycle d'évaluation qui sont basés sur un code (finaliste « Classic McEliece » et candidats alternatifs « BIKE » et « HQC ») ou sur des polynômes multivariés (finaliste « Rainbow » et candidat alternatif « GemSS »). Par ailleurs, des possibilités d'extension et d'adaptation des méthodes proposées sont développées et étudiées.

Piratage de mini-drones



Structure d'essai en laboratoire pour prendre le contrôle de drones via le spoofing GPS

Les aéronefs sans pilote (Unmanned Aerial Vehicles - UAV), également connus sous le nom de drones, représentent une révolution dans le domaine militaire et celui de la sécurité. Grâce aux récents progrès en matière de miniaturisation et à la baisse des coûts, les mini-drones sont également devenus très populaires dans le secteur civil. Ces drones sont généralement trop petits et pas assez puissants pour être équipés d'armes létales. Ils représentent néanmoins une menace pour l'armée et les autorités responsables de la sécurité car ils sont équipés de capteurs puissants et peuvent être utilisés à des fins d'infiltration ou de collecte de données au-dessus de zones interdites. L'armée et les autorités responsables de la sécurité cherchent donc à développer des capacités pour faire face à la menace des mini-drones. L'objectif de ce projet est d'explorer différentes techniques de blocage et de prise de contrôle de mini-drones afin de neutraliser la menace qu'ils représentent. Il s'agit notamment de déterminer s'il est possible d'utiliser pour cela les canaux de contrôle et de navigation sans fil par le biais d'attaques sophistiquées de brouillage, de spoofing et de manipulation de signaux. Cette année, l'accent a été mis sur la possibilité de prendre le contrôle de mini-drones via le canal GPS. La prise de contrôle par GPS a été démontrée avec succès en laboratoire.

Mise en place de réseaux étendus sécurisés

Face au besoin croissant en connexions sécurisées entre bureaux, partenaires et applications basées sur le cloud, les réseaux privés basés sur MPLS (Multiprotocol Label Switching), un réseau privé virtuel (Virtual Private Network, VPN) ou des technologies similaires ne sont plus une option viable pour la mise en place de réseaux étendus (Wide Area Networks, WAN) sécurisés. Ce projet examine des technologies alternatives telles que Scion d'Anapaya/EPFZ et des routeurs programmables pour permettre une communication sûre et fiable et transférer des informations entre les sites de l'entreprise, les partenaires de confiance et les fournisseurs de cloud. L'objectif est de développer et d'évaluer des techniques de routage sécurisées, notamment le routage explicite, l'attestation de routage sécurisée, la défense contre les attaques par déni de service distribué (Distributed Denial of Service, DDoS) et la dissimulation de trafic. Ces techniques sont démontrées dans le cadre d'un banc d'essai réunissant les sites du CYD Campus à Thoune, Lausanne et Zurich.

Sécurité des véhicules électriques et des infrastructures de recharge

Dans le cadre de la transition du DDPS vers des véhicules électriques, la sécurité des infrastructures de recharge existantes doit être vérifiée. Des travaux préparatoires ont déjà été effectués à cet égard, et ont montré que pour certains systèmes utilisant la Power Line Communication (PLC), le flux de données peut être intercepté sans fil à distance. Cela peut avoir diverses conséquences sur la sécurité et la protection des données des voitures et de l'infrastructure. Lors du Car Hackathon du CYD Campus à Thoune en octobre 2021, une attaque active a été développée sur un système de recharge, dans laquelle une attaque par déni de service (Denial of Service, DoS) discrète interrompt et met fin au processus de recharge sans fil. L'analyse de telles attaques et des contre-mesures possibles sera effectuée dans la suite de ce projet.

Formation avec des experts et analyse de vulnérabilités pendant le Car Hackathon à Thoune

Cybersécurité dans le domaine aéronautique et aérospatial

La cybersécurité dans le domaine aéronautique et aérospatial est un thème de recherche majeur depuis la création du CYD Campus. Dans l'aérospatiale, il existe de nombreux points communs fondamentaux, y compris dans le domaine de la cybersécurité. Ainsi, de nombreuses technologies anciennes sont utilisées, souvent inchangées depuis 20, voire 40 ans. Dans le domaine des technologies de communication sans fil en particulier, cela entraîne des problèmes de sécurité majeurs, le contenu n'étant ni chiffré ni authentifié. Mais même lorsque les contenus sont chiffrés, cela n'implique souvent pas des normes ouvertes et sûres mais des systèmes propriétaires faibles qui contredisent le principe de Kerckhoffs sur les cryptosystèmes sûrs. Dans le cadre de ses travaux sur la liaison de données avioniques ACARS (Aircraft Communication . Addressing and Reporting System), le CYD Campus a identifié cette année différents procédés de ce type, qui peuvent désormais être détectés de manière automatisée dans un projet de recherche ultérieur

Protection des systèmes avioniques non sécurisés

Le projet de recherche porte sur l'analyse de vulnérabilités du matériel avionique et des protocoles sans fil utilisés. En 2021, une attaque pratique contre FLARM, qui nécessite peu de ressources, a notamment été démontrée. Système d'alerte de collision utilisé dans les avions légers et les drones, FLARM a été développé en Suisse et a fait l'objet d'une attention et d'une diffusion mondiales. L'affichage du FLARM indique les avions à proximité selon la priorité de l'approche la plus dangereuse et soutient ainsi l'observation de l'espace aérien. En outre, des analyses de systèmes avioniques commerciaux ont été effectuées à l'aide du laboratoire d'avionique. Sur le plan théorique, le protocole de communications entre contrôleur et pilote par liaison de données (Controller-Pilot Data Link Communications, CPDLC) a été étudié et a permis d'identifier des vulnérabilités et de déterminer des possibilités d'amélioration. CPDLC est une méthode qui permet aux contrôleurs aériens de communiquer avec les pilotes via un système de liaison de données.

4.2 Projets dans le domaine «Data Science»

Capteurs IoT distribués: empreinte matérielle et analyse comportementale

Les appareils IoT (Internet des objets) sont aujourd'hui omniprésents dans de nombreuses applications, y compris dans le contexte militaire, ce qui en fait une cible attrayante pour les cyberattaques. Malheureusement, les fabricants ne mettent pas l'accent sur la sécurité lors du processus de développement, que ce soit au niveau matériel ou logiciel. Par exemple, les appareils Raspberry-Pi, très répandus, ne disposent pas d'un identifiant infalsifiable, ce qui les rend faciles à imiter. En observant les différences matérielles telles que la dérive d'horloge, les modèles d'apprentissage automatique sont entraînés à reconnaître les empreintes matérielles qui permettent d'identifier clairement un appareil IoT. À l'avenir, ces empreintes pourraient être utilisées comme une sécurité supplémentaire dans différentes applications. De même, des empreintes logicielles sont créées pour modéliser le comportement normal d'un appareil IoT. Les modèles d'apprentissage automatique sont entraînés à déterminer si un appareil se comporte de manière inattendue, ce qui permet de détecter des cyberattaques telles que des botnets ou des rançongiciels. Des indicateurs telles que les appels de processus et les allocations de ressources provenant du système d'exploitation sont utilisés à cette fin.

Capteurs IoT distribués : classification des modulations et IoT collaboratif

Le spectre électromagnétique est une ressource partagée et en même temps cruciale pour de nombreux systèmes tels que les télécommunications, les radars et la géolocalisation. Il doit donc être protégé contre les cyberattaques susceptibles d'affecter ces systèmes. Des algorithmes automatiques de classification des modulations tentent d'identifier ces dernières. Certains systèmes experts et les approches reposant sur l'apprentissage automatique donnent de bons résultats, mais rencontrent des problèmes en cas de paramètres inconnus comme le canal ou la fréquence d'échantillonnage, pour lesquels ils n'ont pas été entraînés. Ce projet examine les méthodes d'apprentissage par transfert qui permettent d'utiliser des radios logicielles à moindre coût. Grâce à l'apprentissage par transfert, le CYD Campus est en mesure de classer des modulations dans des conditions inconnues jusqu'à présent, qui entraînent généralement des erreurs de classification dans les approches traditionnelles.

Groupe de travail sur l'intelligence artificielle avec les États-Unis

Des représentants du CYD Campus et du département de la Défense des États-Unis ont échangé à plusieurs reprises en 2021 sur le thème de l'intelligence artificielle. Ces échanges ont notamment permis d'acquérir des connaissances de base communes dans ce domaine et d'identifier des applications correspondantes. Dans ce but, les possibilités techniques actuelles ont été examinées, des solutions technologiques possibles ont été développées et des activités communes ont été initiées. Des domaines d'intérêt identiques existent dans la surveillance des nouvelles technologies, l'Internet des objets (IoT) et l'apprentissage automatique décentralisé.
Le groupe de travail a été créé en 2020 dans le cadre d'un accord sur la recherche, le développement, l'expérimentation et l'évaluation. Cet accord a été signé en avril 2019 entre le département de la Défense des États-Unis (DoD) et le Département fédéral de la défense, de la protection de la population et des sports (DDPS).

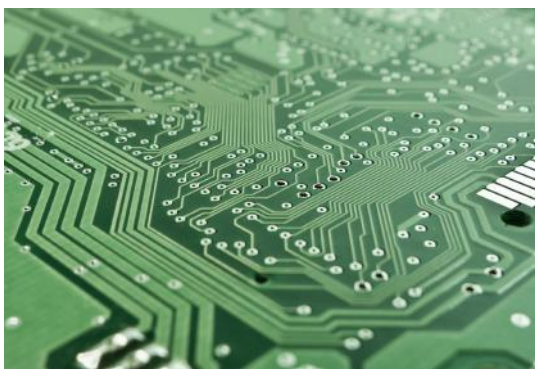
Collecte d'informations sur le cyberespace : stratosphère

Pour pouvoir analyser des données, il faut d'abord les obtenir. Bien que le cyberespace soit de fait une source de données, il n'a été considéré jusqu'à présent que comme un environnement virtuel lié aux technologies de l'information et de la communication. De nos jours, les cyberrisques peuvent toutefois avoir un impact sur l'espace aérien et spatial, par exemple sur les avions et les satellites. Il est donc important de considérer le cyberespace comme un environnement multidimensionnel. Dans le cadre de ce projet, l'intention est de recueillir des données à un endroit stratégique, à savoir la stratosphère. Celle-ci est particulièrement intéressante car elle se trouve entre les satellites et la Terre. Autrement dit, les chercheurs du CYD Campus sont en mesure de collecter des données de liaisons montantes et descendantes. Ils développent pour cela une plateforme à haute altitude portée par un ballon-sonde. La charge utile comprendra une radio logicielle capable d'intercepter les signaux et les communications et de localiser des émetteurs sur Terre ou dans l'espace.

Protection des données dans les appareils portatifs : détermination de caractéristiques personnelles

Les montres connectées représentent désormais une grande partie du marché de l'horlogerie. Elles offrent diverses fonctions telles que le comptage des pas et des battements cardiaques, et sont équipées de capteurs qui enregistrent les mouvements. Bien que ces montres soient jugées utiles par de nombreux propriétaires, ceux-ci ne sont pas conscients des problèmes potentiels qu'elles présentent en matière de protection des données. Les données générées par ces montres sont mises à la disposition d'applications tierces qui peuvent les réutiliser à différentes fins. Ce projet étudie la capacité à déterminer les caractéristiques personnelles des propriétaires de montres FitBit en évaluant leur ouverture d'esprit, leur conscienciosité, leur extraversion, leur agréabilité et leur névrosisme. L'entraînement de modèles d'apprentissage automatique avec les données collectées par ces montres a permis de dépasser la base de référence actuelle et de montrer que la personnalité peut effectivement être déterminée. Par ailleurs, les données permettent également de catégoriser les propriétaires en fonction de leur sexe et de leur religion, ce qui pourrait engendrer des problèmes de discrimination.

Analyse de données assistée par ordinateur : résistance des modèles d'apprentissage profond



Les modèles d'apprentissage automatique ont gagné en importance au cours des dernières années. Ils ne sont plus seulement utilisés dans des applications spécialisées mais se retrouvent dans de nombreuses applications, notamment dans les smartphones pour identifier les activités des utilisateurs. Cette observation soulève une question fondamentale : ces modèles sont-ils résistants face aux attaques ? Il semblerait que l'auteur d'une cyberattaque pourrait facilement venir à bout de la grande majorité des modèles. Comme cela pourrait avoir des conséquences désastreuses dans un contexte militaire, les modèles doivent être rendus résistants aux attaques adverses. Dans le cadre de ce projet, les collaborateurs du CYD Campus se penchent sur les modèles d'apprentissage profond et étudient des méthodes permettant d'accroître leur résistance. À cette fin, l'ensemble d'apprentissage est enrichi avec des échantillons contradictoires qui pourraient être réalisés par les auteurs de cyberattaques. Les résultats montrent que la résistance de modèles entraînés avec de tels schémas adverses augmente par rapport à la précision habituelle.

Protection des données dans les appareils portatifs : traçage de contacts COVID

En réponse à l'épidémie de COVID-19, de nombreux pays ont lancé une application de traçage de contacts. Ces applications ont été utilisées pour identifier des personnes susceptibles d'avoir été en contact avec des personnes infectées. Pour ce faire, l'application envoie régulièrement un signal via les Bluetooth du smartphone. Dans le cadre de ce projet, les collaborateurs du CYD Campus étudient la protection des données de certaines applications de traçage de contacts afin de déterminer par exemple s'il est possible d'identifier des utilisateurs individuels. Plusieurs campagnes de collecte de données ont donc été organisées dans les principales gares suisses. L'analyse des identifiants envoyés par les téléphones a permis de montrer les risques des applications de traçage de contacts.

Détection de fakes sur les réseaux sociaux : identification de la radicalisation

Les comportements suspects sur les réseaux sociaux sont présentés sous différentes appellations : fakes, désinformation, comptes compromis, usurpation d'identité, propagande, discours haineux ou radicalisation. Tous les comportements énumérés ont une caractéristique commune : L'intention de nuire. En se basant sur le cas spécifique de la radicalisation, ce projet identifie des points dans la chronologie des réseaux sociaux d'un utilisateur qui indiquent un changement d'attitude par rapport aux opinions extrémistes. Axée sur un tel objective, les influences auxquelles l'utilisateur a été exposé et qui ont pu conduire à ce changement de comportement sont modélisées à l'aide de modèles linguistiques de pointe. La reconnaissance des principales caractéristiques dans le flux d'informations permet de donner des signaux d'alerte en temps utile lorsqu'une intention de radicalisation peut être identifiée.

Arborescence de la propagation de tweets

d'infox

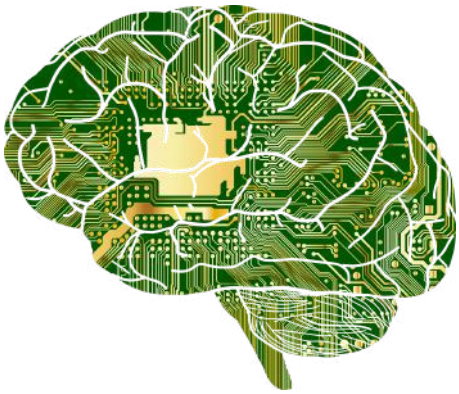
d'informations authentiques

- le nœud racine central indique un article d'actualité ;
- les nœuds marqués en noir signalent les utilisateurs très influents ;
- les nœuds marqués en rose correspondent à des retweets ;
- les nœuds marqués en jaune montrent des citations de l'article initial ou d'un retweet.

Détection de fakes sur les réseaux sociaux : informations erronées en lien avec le COVID

Dans le cas d'une pandémie qui se propage rapidement, il est nécessaire d'obtenir rapidement des informations pertinentes sur la maladie. Twitter est un réseau très populaire pour s'informer en temps réel sur les événements mondiaux. Mais il sert également à diffuser de fausses informations. La formation de chambre d'echo, le manque de contrôle et l'absence de vérification ou d'évaluation des informations sont des problèmes majeurs des réseaux sociaux. À l'ère de l'infodémie, il est essentiel de récolter les réactions des gens aux mesures de santé publique et de comprendre leurs préoccupations. Ce projet se concentre sur l'identification de publications sur les réseaux sociaux qui sont liées à une hypothèse erronée spécifique (Relatedness identification) en utilisant des modèles d'apprentissage automatique classiques tels que la régression logistique ou la machine à vecteurs de support (support-vector machine, SVM) ainsi que la similarité sémantique de textes. Les publications qui se rapportent à une hypothèse erronée sont ensuite classées en fonction des informations erronées qu'elles contiennent. Par ailleurs, l'hypothèse erronée comme sujet de discussion et les commentaires des utilisateurs permettent de déterminer si l'auteur est pour ou contre le sujet (reconnaissance d'attitudes).

Traduction automatique : identification de dialectes



L'identification de dialectes est une tâche très exigeante du point de vue de la linguistique et du traitement algorithmique du langage naturel. Au lieu de se concentrer uniquement sur la classification de langues ou de dialectes, ce projet de recherche tente de reconnaître la langue avant que l'énoncé ou le texte entier ne soit saisi. En d'autres termes : l'accent est mis sur une prédiction correcte à une longueur antérieure et plus courte. L'objectif est de trouver des critères pour raccourcir les données saisies qui déterminent et facilitent la prédiction du dialecte en fonction de l'échantillon et du modèle. Idéalement, la précision de prédiction globale de l'approche proposée doit atteindre, voire dépasser la performance initiale. Dans le cadre de ce projet, le CYD Campus se penche sur la tâche exigeante de la classification des dialectes et se concentre sur deux langues : le suisse allemand et l'indo-aryen. L'analyse expérimentale montre que dans la plupart des cas, la prédiction peut être effectuée à un moment antérieur. Ce processus repose sur des critères d'abréviation de saisie, qui se basent sur des probabilités calibrées et des cohérences d'étiquetage.

Traduction automatique : Universal Adversarial Perturbations

Ce projet a pour but d'étudier les Universal Adversarial Perturbations (UAP) qui tromperaient différents modèles modernes d'apprentissage profond pour le traitement du langage naturel (NLP) et en particulier pour la traduction de textes. Contrairement au traitement d'images, les attaques visant le NLP et les systèmes de traduction automatique neuronale (NMT) n'ont été que peu étudiées dans la littérature. Les systèmes NMT étant utilisés dans des applications hautement sensibles, l'étude des attaques, en particulier des UAP, est d'une importance cruciale pour le modèle NMT. En développant un algorithme de génération d'UAP, le projet tente d'analyser la vulnérabilité de systèmes NMT et de comprendre leur comportement en expliquant l'existence d'UAP.

Le projet s'intéresse aux attaques universelles contre les systèmes NLP et NMT. Prenons par exemple un scénario d'attaque en boîte blanche dans lequel les chercheurs ont accès aux paramètres du modèle, à sa structure et aux données d'apprentissage. Les attaques en boîte blanche sont plus intéressantes que les attaques en boîte noire car elles sont plus ciblées. Une attaque en boîte noire simule de manière réaliste l'attaque d'un hacker typique. Les attaques en boîte blanche désignent une attaque avec certaines connaissances détaillées sur le fonctionnement interne du système. Elles révèlent généralement davantage de vulnérabilités du modèle NMT car elles peuvent accéder aux paramètres du modèle.

Traduction automatique : familles de langues et de dialectes

La traduction automatique a fait des progrès considérables depuis l'introduction de modèles de réseaux neuronaux, et les transformers sont actuellement la norme pour les paires de langues avec de nombreuses données de traduction parallèles, appelées paires de langues riches en ressources. Pour les paires de langues pauvres en ressources ou en cas d'absence totale de données de traduction parallèles, des efforts supplémentaires sont nécessaires. Dans le cadre de ce projet, l'accent est mis sur des solutions permettant de gérer une langue pauvre en ressources lorsque des langues plus riches en ressources de la même famille sont disponibles. Pour l'entraînement des modèles de traduction initiaux, on a eu recours à l'apprentissage par transfert en utilisant différentes langues riches en ressources, qui ont été affinées par les chercheurs pour la langue pauvre en ressources donnée. Par ailleurs, la retraduction a été utilisée comme technique d'extension des données de traduction parallèles lorsque seules des sources monolingues sont disponibles. Il a été démontré que toutes ces techniques améliorent la qualité de la traduction dans des environnements pauvres en ressources.

Méthodes dans le domaine de la science des données pour la veille des technologies et des marchés

Le suivi de l'évolution des technologies et des marchés nécessite d'être en mesure d'identifier les technologies, de les distinguer et de comprendre leurs relations mutuelles. En utilisant les concepts liés à la technologie au sein du graphe de Wikipedia, le CYD Campus propose une méthode pour identifier la position effective d'un nouveau concept au sein d'une taxonomie existante en se basant sur des similitudes sémantiques et pertinentes. Par ailleurs, un cadre est mis en place pour la reconnaissance du concept lié à la technologie dans un texte non structuré en utilisant l'approche du « concept tagging », qui n'implique pas l'extraction de la forme exacte du texte brut. De cette manière, il devient possible de se concentrer sur le contenu sémantique d'un document plutôt que sur sa forme textuelle et d'identifier des concepts qui ne sont pas explicitement mentionnés dans le texte.

Signaux d'alerte précoce dans OSINT : anticipation de conflits

L'anticipation de conflits est une tâche essentielle pour les gouvernements et les forces armées. La connaissance d'instabilités ou de conflits potentiels peut fortement influencer la stratégie géopolitique et permettre une meilleure préparation. Récemment, plusieurs sources ouvertes ont commencé à collecter des données qui peuvent être d'une grande importance pour la prévision de conflits. À cet égard, on peut citer la base de données ACLED (The Armed Conflict Location & Event Data Project), qui contient de nombreux rapports quotidiens sur les manifestations, les émeutes et les victimes dans de nombreux pays. Grâce à des méthodes statistiques, les collaborateurs du CYD Campus peuvent identifier et prédire les «tipping points», des points de basculement qui indiquent un changement de direction. Il peut s'agir d'un coup d'État ou d'un autre changement politique majeur. En analysant des données provenant d'Inde et d'Irak, ils ont été en mesure de modéliser la dynamique d'instabilités dans ces pays et d'identifier ainsi les signaux d'alerte précoce correspondants.

Analyses causales

En statistique, des corrélations sont souvent utilisées pour mettre en évidence un lien entre deux variables. Les corrélations ne permettent toutefois pas de déterminer s'il existe ou non un lien de cause à effet entre les deux variables. L'objectif de l'analyse causale est de trouver la cause fondamentale d'un problème plutôt que d'examiner uniquement les symptômes. Cette technique permet de mettre en évidence les faits qui conduisent à une situation donnée. Ces dernières années, de nombreuses approches et méthodes avancées ont été développées pour le lien de causalité, notamment dans le domaine des statistiques. L'objectif de ce projet de recherche est de fournir un aperçu des méthodes modernes d'interprétation, d'identification et d'estimation des liens de causalité de données d'observation. La causalité pourrait par exemple être appliquée à l'observation et à la prévision de conflits, de telles méthodes pouvant fournir des informations sur la raison d'un changement dans la stabilité géopolitique.

5 Clients et répartition des moyens

Le dispositif cyber de la Confédération est divisé en trois domaines : cybersécurité (DFF), cyberdéfense (DDPS) et poursuite pénale de la cybercriminalité (DFJP). Le CYD Campus fournit en premier lieu des prestations pour le domaine de la cyberdéfense. Grâce aux synergies, notamment dans le domaine technologique, les deux autres domaines bénéficient toutefois aussi des prestations du CYD Campus. Des prestations directes sont fixées chaque année dans des conventions de prestations. En 2021, le CYD Campus a fourni des prestations pour le compte des acquisitions, de la défense et de l'administration.
Dans le détail, des commandes ont été passées aux organisations suivantes :

- armasuisse - domaine de compétences Conduite et exploration
- État-major de l'armée
- Base d'aide au commandement de l'arméeOrganisations de cybersécurité
- Défense Commandement des opérations
- Service de renseignement de la Confédération
- Département fédéral des finances – Centre national pour la cybersécurité NCSC
- Office fédéral de la police fedpo

Prestations contractuelles	Répartition 2021
Analyses de sécurité, tests d'intrusion, conseil en sécurité	29 %
Analyses de sécurité et tests d'intrusion	16 %
Concepts de sécurité et conseil	13 %
Recherche de vulnérabilités	2 %
Recherche de vulnérabilités	2 %
Conseil, transformations technologiques	21 %
Soutien consultatif Data Science	3 %
Transformation technologique	18 %
Démonstrateurs	29 %
Conception de démonstrateurs technologiques	5 %
Conception de démonstrateurs d'innovation	24 %
Création et participation aux études	19 %
Réalisation d'études d'aptitude	2 %
Réalisation d'études de base	2 %
Collaboration aux études de base	11 %
Création d'études technologiques	4 %

Tableau 1: répartition des mandats 2021 du CYD Campus

La prestation globale du CYD Campus, répartie par domaines, est présentée dans l'illustration 1. Les principales prestations concernent la recherche, les contributions à l'innovation et le soutien aux activités d'acquisition. Une liste plus détaillée dans le Tableau 1 montre la répartition des mandats traités en 2021.

Remarque: Pour des raisons de classification, les prestations contractuelles ne peuvent pas être décrites plus en détail dans le rapport annuel.

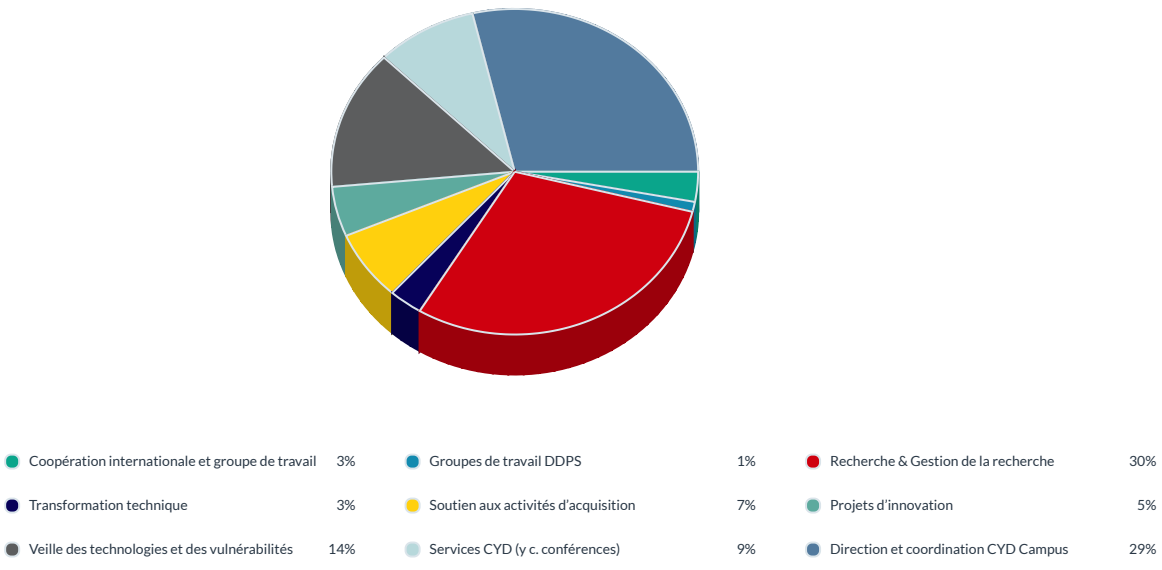


Illustration 1 : prestation globale 2021 du CYD Campus

6 Innovation

Le CYD Campus soutient les innovations technologiques pour les unités administratives et la défense avec un niveau de maturité technologique (TRL) de 4 à 6.

L'objectif des projets d'innovation est de mettre en œuvre chez le client ou le mandant les résultats de la recherche ou de nouveaux besoins sous forme de démonstrateurs et de démontrer l'applicabilité pratique de la technologie chez le client.
En 2021, des rapports d'innovation ont été réalisés pour les organisations suivantes :

- Base d'aide au commandement BAC
- Office fédéral de la police fedpol
- Service de renseignement de la Confédération – MELANI

Les rapports d'innovation ont été réalisés pour la plupart dans le cadre d'un atelier d'une journée sur place à Thoune. En raison des restrictions en vigueur en lien avec le COVID-19, il a fallu renoncer à la présence de l'ensemble des participants, mais les événements ont été organisés de manière hybride – à l'aide de vidéoconférences – dans le respect de la sécurité de l'information.

6.1 Résultats des projets d'innovation

Pour des raisons de classification, il n'est pas possible de présenter de résultats explicites, raison pour laquelle un aperçu générique d'une sélection de résultats est présenté.

Application de l'intelligence artificielle à des problématiques actuelles

Les systèmes de détection d'intrusions dans les réseaux (Network Intrusion Detection - NIDS) sont des composantes importantes des réseaux sécurisés modernes qui contribuent à détecter les signes de cyberattaques dans un réseau. De telles attaques sont de plus en plus complexes et visent le nombre croissant d'appareils connectés, dont les objets de l'Internet des objets (IoT). Les systèmes IoT actuels génèrent déjà une grande partie du trafic Internet, mais la sécurité informatique des appareils reste faible, ce qui entraîne un nombre élevé d'attaques fructueuses. L'introduction de systèmes innovants pour la détection d'attaques de réseau doit être améliorée par de nouvelles techniques d'apprentissage automatique (ML). Dans le cadre du projet d'innovation, les performances de nouveaux modèles de ML pour les NIDS ont été étudiées sur différents ensembles de données de réseau IoT et de nouvelles techniques d'extracteurs de caractéristiques de réseau ont été vérifiées sur le terrain.

Introduction de méthodes pour protéger la sphère privée

Ce projet a examiné comment les protocoles de protection de la sphère privée tels que Private Set Intersection (PSI) ou Private Membership Test (PMT) peuvent être utilisés pour empêcher les connexions illicites de collaborateurs identifiés à distance. Différentes primitives cryptographiques ont été utilisées, comme le chiffrement homomorphe (HE), les « oblivious pseudorandom functions » (OPRF) et les « garbled Bloom filters » (GBF). Les résultats montrent que les calculs du protocole OPRF PSI nécessitent moins de 200 ms pour 4000 collaborateurs, tandis que les coûts de transmission des données sont inférieurs à 1 Mo. En utilisant l'approche OPRF pour PMT, les calculs prennent 14 ms et le protocole exige des parties qu'elles transmettent moins de 20 Ko.

Transfert de connaissances dans le domaine Data Science

Le transfert de connaissances du monde académique aux clients du CYD Campus s'effectue à plusieurs niveaux. Grâce à des formations et des stages dans le domaine de la science des données, des collaborateurs transmettent des bases statistiques et mathématiques à différentes organisations du DDPS. Les contenus d'apprentissage transférés sont adaptés aux domaines spécifiques des clients ainsi qu'aux analyses actuelles.

Travail exploratoire

Outre l'expertise scientifique, des innovations techniques sont également transmises aux clients du CYD Campus. À titre d'exemple de transfert de connaissances technologiques, citons la transmission de savoir-faire en matière de gestion et de maintenance de données dans les architectures de type «lacs de données».

Accompagnement lors de l'introduction de structures de données et du traitement de grandes quantités de données, mégadonnées et lacs de données

Au cours des dernières années, le Big Data a favorisé le développement de diverses technologies. Parmi les exemples de ces technologies de Big Data figurent les nouvelles technologies de stockage de grandes quantités de données et des formats de données les plus divers (p. ex. formats de données structurés et non structurés), le traitement de flux de données en temps réel ou le calcul dans des systèmes distribués. Le CYD Campus conseille et soutient les clients du DDPS dans le cadre de la mise en place de systèmes dotés d'architectures de type « lacs de données », qui utilisent principalement les technologies de Big Data.
Une part importante du savoir-faire du CYD Campus provient de la mise en place du Data Science Lab, une plateforme spécialement conçue et exploitée pour le stockage et le traitement de Big Data.

Introduction d'une plateforme novatrice pour le suivi de la situation en termes de cybermenaces, y compris l'échange de données

La compréhension et la protection contre les cybermenaces deviennent de plus en plus complexes étant donné l'évolution rapide des tactiques, techniques et procédures d'attaque. L'objectif du projet de suivi de la situation des cybermenaces (CBL) est de développer une validation de principe pour une plateforme de renseignement sur les menaces (Threat Intelligence Platform, TIP). La plateforme développée utilise des éléments open source existants tels que MISP, OpenCTI et TheHive, chaque outil ayant une fonction spécifique.
La plateforme a été largement testée et améliorée avec des fonctions spécifiques telles que l'analyse de documents (analyse syntaxique). Par ailleurs, l'architecture et l'installation élaborée ont été documentées. Différentes approches possibles pour résoudre le problème, comme d'autres outils disponibles, la disponibilité future et la flexibilité, ont également été prises en compte. En outre, une architecture finale idéale a été décrite dans le cadre de l'étude. L'objectif est de présenter la meilleure structure productive possible en tenant compte des coûts, des risques et du fonctionnement à long terme.

Introduction d'une plateforme de traduction automatique hors ligne pour les opérations tactiques

Le projet a démontré que dans le cas de textes généraux, il est possible d'entraîner des modèles à fournir une traduction complète indépendamment de la langue source ou cible. Il s'est toutefois avéré que les données utilisées pour l'entraînement peuvent avoir une influence considérable sur la qualité de la traduction. Des données variées provenant de sources différentes permettent une grande fiabilité du modèle de langue et de traduction assimilé par rapport aux variations linguistiques. En outre, les modèles entraînés pour une traduction générale peuvent être optimisés sur des ensembles de données internes afin de couvrir des cas d'application plus spécifiques. Ces ensembles de données utilisés pour l'entraînement interne peuvent également provenir de sources classifiées.

Conception d'une architecture pour des systèmes d'exploitation mobiles sécurisés

Les projets open source ou commerciaux manquent d'une architecture de sécurité complète pour un système d'exploitation mobile. En effet, l'architecture de sécurité devrait compartimenter les risques afin de protéger les données confidentielles et les communications contre des attaques ou des accès non autorisés. Par ailleurs, les utilisateurs devraient être en mesure d'exécuter des applications non sécurisées sur un appareil parallèlement à des applications fiables, tout en travaillant avec des informations confidentielles. Deux architectures ont été développées dans le but de mettre en place une telle architecture de sécurité. Le système sous-jacent est basé sur un concept d'hyperviseur pour l'exécution de plusieurs noyaux et instances Android. Les pilotes sont également virtualisés, les noyaux n'ayant pas d'accès direct au matériel.

Partage automatisé de vulnérabilités

En 2021, le CYD Campus collabore pour la première fois avec l'Office fédéral allemand de la sécurité des technologies de l'information (BSI) dans le domaine de l'innovation. Cette collaboration comprend la mise à disposition d'applications logicielles open source permettant de créer et de gérer des recommandations de sécurité dans un format exploitable par les machines. Les informations sur les vulnérabilités peuvent ainsi être partagées plus facilement, ce qui améliore la cybersécurité.

6.2 Cyber Startup Challenges

2020: Détection de cybermenaces

Les start-up ont souvent des idées innovantes et révolutionnaires, et peuvent proposer des technologies qui offrent un avantage technologique par rapport aux auteurs de cyberattaques. C'est pour cette raison que le CYD Campus a lancé le Cyber Startup Challenge en 2020.

En 2020, la start-up CounterCraft a convaincu le jury avec sa solution novatrice dans le domaine de la détection de cybermenaces. En 2021, l'entreprise a mis en œuvre une validation de principe sur mesure.

Le scénario d'usurpation décrit un petit réseau de contrôle industriel avec un nombre réduit d'automates programmables industriels (API) actifs. Il peut s'agir d'une petite installation isolée, à l'instar d'une sous-station ou d'une station de pompage. Le réseau est contrôlé par le biais d'une interface homme-machine (IHM), les données de contrôle étant stockées dans une base de données en réseau. L'installation est commandée à partir d'un centre de contrôle.

La validation de principe a été testée en 2021 du point de vue de l'auteur d'une cyberattaque et du défenseur avec les unités opérationnelles de l'armée. Il a été possible de comparer les tactiques, techniques et procédures générées (tactics, techniques and procedures - TTP) avec la réaction de la plateforme.

2021: Boostez votre centre de partage et d'analyse d'informations (ISAC)

Le Cyber Startup Challenge 2021 avait pour objectif de découvrir le paysage technologique des start-up sous la devise « Boostez votre centre de partage et d'analyse d'informations (Information Sharing and Analysis Center, ISAC) » et recherchait des solutions innovantes dans le domaine du renseignement sur les cybermenaces en mettant notamment l'accent sur la protection des infrastructures critiques.

Au total, 38 start-up d'Europe, des États-Unis et d'Asie ont répondu à l'appel. Le jury, composé de cyber-experts du DDPS et d'armasuisse S+T, a sélectionné les trois finalistes Decentriq, Constella Intelligence et Pandora Intelligence, qui ont présenté un pitch lors de la conférence du CYD Campus le 28 septembre 2021. La start-up zurichoise Decentriq a convaincu le jury avec sa plateforme innovante Software as a Service (SaaS), qui propose des « data clean rooms » aux entreprises. Les « data clean rooms » sont des environnements sécurisés et protégés dans lesquels les données personnelles sont nettoyées et traitées afin de pouvoir être utilisées à diverses fins d'analyse de données. La plateforme permet ainsi aux acteurs internes et externes d'infrastructures critiques de partager des cyberdonnées en toute sécurité et d'obtenir des connaissances agrégées et anonymes. De cette manière, la cybersécurité est améliorée sans compromettre la protection des données.
En 2022, Decentriq va travailler, en collaboration avec le CYD Campus, à l'intégration d'une validation de principe de sa technologie dans un environnement réel du DDPS.

7 Audits de sécurité, tests d'intrusion et conseil en sécurité

En 2021, des collaborateurs du CYD Campus ont examiné la sécurité d'une douzaine de systèmes militaires traités dans le cadre d'achats d'armement et de systèmes informatiques au DDPS. Les contrôles ont pris la forme d'audits de sécurité, de tests d'intrusions ou de conseils en matière de cybersécurité. Dans la plupart des cas, les mandants étaient les services d'achat centraux d'armasuisse.

L'accent a été mis sur les domaines suivants :

- Plateformes Windows
- Plateformes Linux
- Applications Web
- Middlewares
- Réseaux informatiques
- Technologies VPN et solutions de chiffrements
- Systèmes d'information de contrôles
- Drones
- Véhicules
- Systèmes de communication sans fil (voix et données)
- Aviation et systèmes de communication par satellite

Les analyses et audits ont débouché sur des mesures de sécurité qui ont ensuite été mises en œuvre dans des projets d'acquisition ou qui sont alors pris en compte lors de prises de décision dans le cadre du concept de sécurité de l'information et de protection des données (SIPD).

Remarque: Pour des raisons de classification, les analyses de sécurité, tests d'intrusion et conseils en sécurité ne peuvent pas être décrits plus en détail dans le rapport annuel.

8 Démonstrateurs

Démonstrateur de réalité mixte pour la simulation de formation

La réalité mixte (RM) décrit le mélange du monde physique réel avec une réalité virtuelle, c.-à-d. avec un environnement interactif généré par ordinateur. Un démonstrateur a été développé afin d'utiliser également cette réalité mixte dans le cadre de formations.

L'objectif du démonstrateur est d'apporter une innovation dans la simulation en formation, de vérifier les affirmations conservatrices de l'industrie, de montrer le potentiel de la réalité mixte dans la formation en simulateur ainsi que d'estimer et d'évaluer les limites de la technologie. La simulation porte sur la conduite d'un char.

Utilisation du démonstrateur pour des tests avec des personnes

Les potentiels de la RM sont entre autres:

- Augmentation de la reconnaissance physique et opérationnelle de la situation
- Réduction des coûts de formation et d'entraînement
- Meilleures préparations à l'entraînement et à l'engagement
- Flexibilité et mobilité (partielle) dans les entraînements, la formation et les préparations à l'engagement
- Meilleur soutien (maintenance, logistique, troupes sanitaires, etc.)
- Action combinée (capteurs, renseignement, conduite) plus efficace
- Préservation du matériel et de l'environnement
- Réalisation de scénarios qui ne sont pas ou difficilement réalisables dans le monde réel (scénarios d'urgence dans des véhicules, réalisation d'exercices de grande envergure, interventions en zone urbaine, etc.)

Démonstrateur réalité mixte pour la simulation de formation

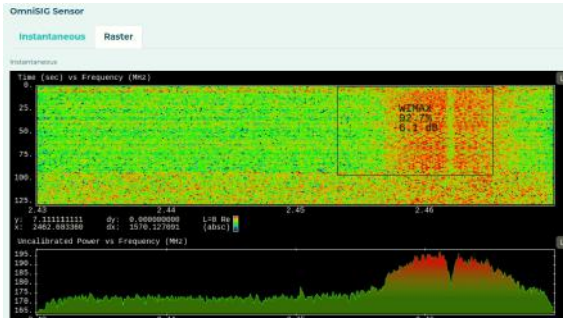
L'utilisation de la technologie comporte certains risques, notamment:

- Mal du virtuel ou cybercinétose
- Surcharge de données et d'informations
- Forte dépendance de la RM en cours d'engagement
- Forte dépendance des ressources informatiques
- Sécurité (intégrité des systèmes, disponibilité des services, confidentialité des données)
- Fort impact possible dans la doctrine, notamment dans la formation
- Juxtaposition de la formation, de l'entraînement et du déploiement
- Manque d'interopérabilité et de frameworks
- Faible maturité du marché
- Faible niveau de maturité de la RM pour les applications militaires

Les premiers résultats obtenus avec le démonstrateur montrent qu'il existe certes un grand potentiel, mais que regrouper les différentes composantes et surmonter les risques constituent un défi.

Démonstrateur de classification de signaux

La cyberguerre et la guerre électromagnétique étaient généralement considérées comme des domaines distincts. Nous assistons aujourd'hui à une convergence de ces deux domaines vers une compréhension et une utilisation intégrées des technologies. Cela se manifeste également dans le contexte des opérations modernes de guerre hybride, où il devient de plus en plus important de pouvoir classifier des signaux dans le spectre électromagnétique avec une puissance de calcul limitée et une flexibilité croissante. Il existe aujourd'hui plusieurs approches de recherche qui utilisent les techniques d'apprentissage profond pour classifier les données du spectre. Les collaborateurs du CYD ont identifié une start-up américaine prometteuse, capable de classer des signaux en utilisant des données de magnitude et signal de phase grâce à des méthodes d'apprentissage profond. Le logiciel offre une interface utilisateur simple ainsi que des options avancées et repose sur une technologie de pointe en constante évolution. Il peut également être utilisé avec du matériel informatique bon marché disponible dans le commerce. Les capteurs à l'origine de l'inférence ne nécessitent qu'une puissance de calcul limitée et peuvent fonctionner sur une petite plateforme intégrée avec une unité de traitement graphique. Ce démonstrateur montre l'importance et le potentiel de cette technologie, qui n'en est qu'à ses débuts.



Le démonstrateur utilise des modèles d'apprentissage automatique pour classifier le spectre électromagnétique en temps réel

Démonstrateur de spoofing GPS pour drones

Le spoofing GPS est une attaque qui consiste à utiliser un émetteur radio à proximité de la cible pour simuler un signal GPS légitime. Étant donné que les drones dépendent de signaux GPS pour déterminer leur position, ils sont également concernés par ce type d'attaque. Il a déjà été possible de montrer comment un drone transmet sa position falsifiée au pilote. Les travaux se concentrent maintenant sur la manière de prendre le contrôle d'un drone à l'aide de cette attaque. L'idée consiste à falsifier en permanence des emplacements à proximité et à simuler un mouvement réel, de sorte que le drone se déplace et que l'auteur d'une cyberattaque ait un contrôle total sur le mouvement du drone. Le spoofing GPS pourrait donc être utilisé par l'auteur d'une cyberattaque pour prendre le contrôle de drones commerciaux appartenant à des particuliers afin d'effectuer des actes malveillants à leur insu, p. ex. faire s'écraser le drone contre une cible précise ou voler le drone pour accéder à des données personnelles.

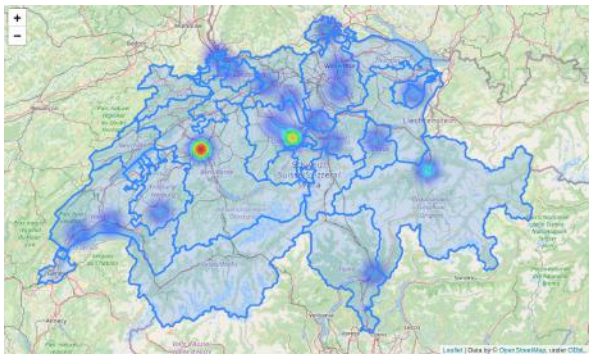
Démonstrateur de réalité augmentée pour la sécurité

La réalité augmentée (RA) permet à une personne d'interagir avec son environnement réel, qui est augmenté par des informations et des objets virtuels. Pour ce démonstrateur, l'applicabilité de la RA comme outil d'aide aux utilisateurs pour se défendre contre les cyberattaques telles que l'hameçonnage est prise en considération. Les lunettes de RA peuvent simuler un expert en cybersécurité qui « regarde par-dessus l'épaule » de l'utilisateur et l'aide à se défendre contre des attaques. Cette approche permet une bien meilleure défense contre l'hameçonnage et les attaques par hameçonnage ciblé par rapport aux méthodes traditionnelles.

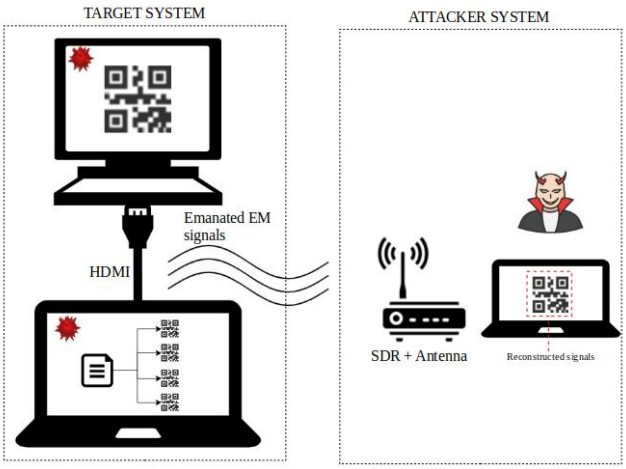
Évaluation de la réalité augmentée pour une meilleure défense contre l'hameçonnage à l'aide du démonstrateur

Démonstrateur d'état des lieux des réseaux sociaux

La communication au 21e siècle est marquée par trois technologies : Internet, les appareils mobiles et les réseaux sociaux. Il n'est donc pas surprenant que cette infrastructure soit utilisée par certains acteurs tels que des services de renseignement étrangers pour la diffusion ciblée de fausses informations. Un démonstrateur pour l'analyse automatisée de contenus de comptes Twitter est donc en cours d'élaboration. Tous les messages rédigés par le compte cible sont téléchargés via l'API officielle de Twitter. Il est ensuite possible d'effectuer une analyse des données textuelles, graphiques et vidéo qu'ils contiennent. L'utilisation d'expressions ordinaires permet d'extraire des tweets des indications concernant la date et l'heure, associées aux localités mentionnées. Les contenus peuvent ainsi être placés dans un contexte temporel et géographique, ce qui permet de générer un état des lieux. Le contenu textuel des tweets est ensuite analysé en fonction des fréquences de mots et des localités mentionnées. Cela permet de se faire une première idée du point de vue dominant d'un compte Twitter et de son rapport avec des événements définis dans le temps et l'espace. Par ailleurs, les données graphiques sont analysées à l'aide de méthodes d'apprentissage profond modernes (réseaux de neurones convolutifs), ce qui permet de distinguer des mèmes image/texte d'autres données graphiques. Les mèmes image/texte constituent un outil efficace pour la diffusion d'idées et le contrôle de contenus en ligne, ce qui les rend attrayants pour des campagnes de désinformation.



Heatmap du nombre de tweets référençant des localités en rapport avec la pandémie COVID19



Exploitation du rayonnement des câbles vidéo HDMI pour exfiltrer des données sensibles d'un ordinateur infecté

Demonstrator TEMPEST Datenabfluss

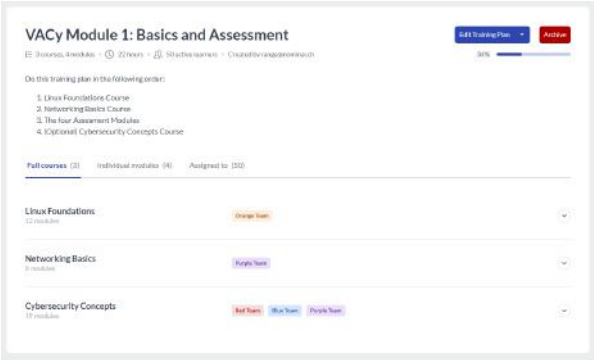
Tout appareil électronique génère des émissions électromagnétiques. Les signaux électromagnétiques générés sont liés au fonctionnement interne des composants électroniques émetteurs. L'auteur d'une cyberattaque peut écouter ces signaux et les examiner afin d'obtenir des informations sur l'appareil émetteur. La pratique de l'interception et de la protection contre l'interception et son contrôle est résumée dans un cadre connu sous le nom de TEMPEST.

Dans le cas de moniteurs vidéo, les signaux diffusés peuvent être utilisés pour reconstruire le contenu. Il a déjà été démontré comment l'auteur d'une cyberattaque peut utiliser les signaux du câble de connexion entre un PC et un moniteur vidéo pour extraire des informations internes du moniteur. Dans cette démonstration, le CYD Campus montre comment un code QR peut être utilisé pour exfiltrer des données internes à l'aide de ces signaux émis par le moniteur vidéo.

Étant donné que de nombreuses entreprises s'appuient sur les réseaux informatiques comme système de communication pour transférer différents types d'informations entre des serveurs et des postes de travail, on peut s'attendre à ce que ces réseaux constituent une cible intéressante pour les auteurs de cyberattaques, certaines de ces informations pouvant contenir des secrets commerciaux et être hautement confidentielles.

Démonstrateur de ludification de la cyberformation

On sait qu'il y a une pénurie systématique de main-d'œuvre qualifiée dans le domaine de la cybersécurité ; une solution possible à ce problème consiste à attirer davantage de personnes vers la formation dans ce domaine. Pour cibler efficacement les jeunes, il convient de proposer quelque chose d'intéressant. La ludification dans le cadre de la cyberformation peut apporter une contribution importante à cet égard. La ludification consiste à appliquer des éléments ludiques typiques dans un contexte qui ne s'y prête pas forcément. Afin de tester différents scénarios et hypothèses, des collaborateurs du CYD Campus ont consulté les produits de plusieurs start-up et en ont testé deux avec un groupe de jeunes. L'expérience acquise lors de ce premier essai a permis de passer à un test de plus grande envergure. Les cinquante jeunes qui feront partie du premier projet pilote de la formation prémilitaire cyber (qui débutera en novembre 2021) ont pu utiliser le logiciel innovant d'une des start-up sélectionnées.



Environnement logiciel du démonstrateur pour la formation prémilitaire cyber

Démonstration de l'exploitation des failles de sécurité de véhicules électriques pour intercepter les communications

Démonstrateur de «car hacking»

Lors du Hackathon autour de voitures à Thoune, décrit dans le chapitre Temps forts, les participants ont conçu plusieurs démonstrations d'attaques pouvant être menées contre des voitures. Dans un cas, le raccordement d'une interface au bus CAN (interface de communication) d'une voiture électrique a permis de déclencher des comportements intempestifs tels que des lumières clignotantes, l'ouverture et la fermeture des fenêtres ou d'influencer la direction assistée. Compte tenu de la forte tendance à la mobilité électrique, il a également été démontré que le processus de charge de véhicules électriques pouvait être perturbé et interrompu à distance.

Démonstrateur de visualisation d'attaques contre des infrastructures critiques

Lors d'exercices de capture de drapeau ou du type Live-Fire, il est souvent difficile pour les experts en cybersécurité et les décideurs de comprendre l'impact de cyberactions sur l'infrastructure physique. En effet, contrairement aux attaques contre les systèmes cyber-physiques tels que les installations de production d'électricité ou les systèmes (d'armes) militaires, il est relativement facile de détecter si un site Internet ne se charge pas, si des courriels malveillants arrivent ou si un rançongiciel est introduit sur un ordinateur. Afin de déterminer les meilleurs outils de cyberformation pour l'armée suisse, un démonstrateur a été conçu pour illustrer ces incidences. Il se compose d'un modèle de terrain de 2,4 x 1,2 m, modulaire et facile à déplacer, montrant un aéroport à usage mixte (civil et militaire) ainsi que des infrastructures critiques, une production d'énergie et des systèmes militaires. Cette installation a été testée avec succès en 2021 dans le cadre d'un exercice Live-Fire-Cyber de l'armée suisse. Elle sera développée l'année prochaine en étant connectée à de véritables automates programmables (API) et intégrée dans un environnement SCADA (Supervisory Control and Data Acquisition) réaliste qui pourra être utilisé pour la recherche et les exercices.

Visualisation de cyberattaques sur une base aérienne

Démonstrateur de cyber-range hybride

Les cyber-range sont des infrastructures composées de plusieurs ordinateurs et réseaux, qui peuvent être utilisées pour la recherche ou des exercices. En règle générale, la majeure partie de l'infrastructure est virtualisée ; autrement dit, il n'y a pas de véritables postes de travail, ceux-ci fonctionnant sur des serveurs dans un centre de calcul. Toutefois, les réseaux réels ne se composent pas uniquement de serveurs et de postes de travail, mais comprennent également des composants physiques utilisés pour surveiller et piloter les processus techniques. Le projet consistait à tester des composants qui ont permis aux collaborateurs du CYD Campus d'intégrer de véritables systèmes de surveillance industriels (SCADA) dans un cyber-range. Ils ont été utilisés avec succès dans le cadre d'exercices et d'autres essais.

Système de commande industriel avec écran de visualisation (en haut) et espace cyber mobile (en bas)

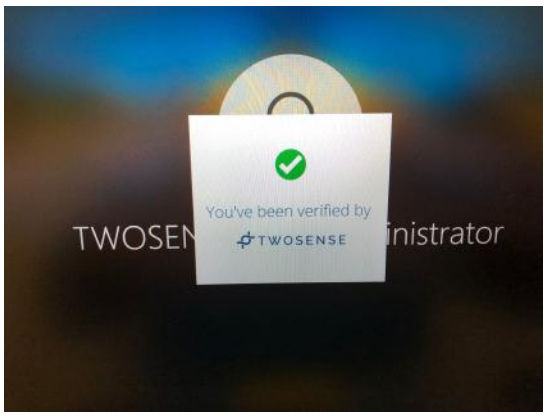
Démonstrateur de traduction hors ligne

L'échange d'informations dans différentes langues est désormais une nécessité. Les outils de traduction automatique sont également devenus une partie intégrante de notre travail quotidien. Cependant, ces outils de traduction en ligne comportent également des risques importants pour la sphère privée, notamment en ce qui concerne les informations sensibles. Il est donc impératif que la traduction automatique puisse être utilisée sans que les informations ne soient divulguées à l'extérieur. Le démonstrateur de traduction hors ligne propose à cet effet une traduction de texte hors ligne automatique bidirectionnelle entre l'anglais et six autres langues, à savoir l'arabe, l'allemand, le français, l'italien, le russe et le chinois. Afin d'éviter les erreurs causées par une mauvaise utilisation de la langue, une fonction de reconnaissance de langue est également intégrée. L'outil de traduction peut être utilisé via une interface graphique et une API REST.

Exemple de traduction du chinois vers l'anglais avec un système hors ligne

Démonstrateur d'authentification continue

Les demandes de mot de passe ou les contrôles biométriques uniques tels que les lecteurs d'empreintes digitales ou les scanners d'iris permettent aux utilisateurs d'accéder au système après une authentification mais ne vérifient pas régulièrement les comportements malveillants ou le changement d'utilisateur. Ces méthodes permettent p. ex. des attaques dites de midi, où l'auteur d'une cyberattaque utilise un poste de travail auquel un utilisateur légitime est encore connecté mais qui n'a pas été verouillé. De même, les données de mot de passe peuvent être volées en cas de fuites, d'espionnage par-dessus l'épaule ou d'attaques de hameçonnage et laisser la voie libre dans le système ciblé. Ce comportement s'oppose à l'authentification continue (AC) qui consiste à observer un utilisateur sur une longue période et à accorder ou, le cas échéant, révoquer sans cesse l'authentification. L'AC authentifie donc le comportement de l'utilisateur, même lorsqu'il est connecté, généralement à l'aide de caractéristiques biométriques telles que le suivi du regard ou la surveillance de l'environnement comme les capteurs de proximité capacitifs sans fil. Le démonstrateur automatise la protection de l'identité au moyen de l'authentification biométrique des utilisateurs, de sorte qu'ils ne soient plus obligés de s'authentifier manuellement. Le démonstrateur permet à jusqu'à dix utilisateurs de se connecter à deux ordinateurs gérés à l'aide du logiciel d'authentification automatique afin de démontrer la capacité d'authentification continue.

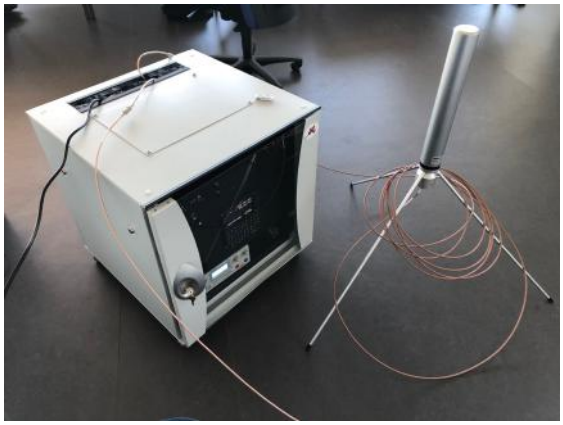


Vérification comportementale de l'utilisateur par le démonstrateur

Démonstrateur de spoofing des communications d'un aéronef

Dans les années 2010, des scientifiques et des hackers ont démontré de nombreuses vulnérabilités dans les technologies sans fil utilisées par les avions et les contrôleurs aériens. Jusqu'à présent, ce type de spoofing a été démontré avec des moyens limités comme des radios logicielles exclusivement sur ordinateur avec du matériel et des logiciels simulés.

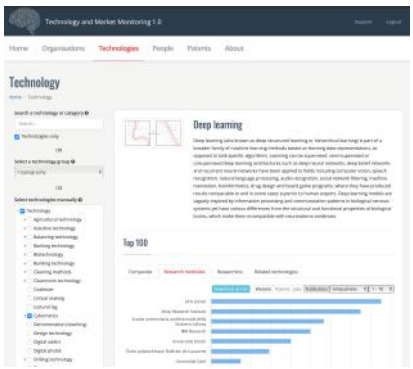
Ce démonstrateur utilise une représentation proche de la réalité de systèmes avioniques réalistes (matériel et logiciels) tels qu'ils sont installés dans les avions. L'accès complet à ces systèmes à des fins de tests d'intrusion permet aux chercheurs du CYD Campus de montrer des attaques par radiofréquence (RF) sans fil sur les systèmes de GPS, Automatic Dependent Surveillance - Broadcast (ADS-B) et d'alerte de trafic et d'évitement de collision (Traffic Alert and Collision Avoidance System, TCAS).



Démonstration de spoofing au Cyber Avionics Lab

Démonstrateur de veille des technologies et des marchés

Sur la base de données open source, le démonstrateur propose aux utilisateurs une liste d'entreprises pertinentes en Suisse correspondant au cluster technologique recherché. Par ailleurs, des informations sur les postes vacants, le nombre de brevets et le nombre de publications sont disponibles dans le démonstrateur, et les entreprises peuvent être trouvées avec des informations telles que les produits, services et technologies proposés. Ces entreprises sont par conséquent visibles tant comme fournisseurs (ou sous-traitants) potentiels que comme partenaires de compensation éventuels dans le cadre d'acquisitions.



Extrait de l'outil TMM sur les technologies d'apprentissage profond

9 Veille technologique et du marché

Le CYD Campus agit comme une plateforme d'anticipation des cyber-évolutions et des cyber-tendances. À travers ce domaine d'activité, le DDPS veut être en mesure de découvrir les innovations des cybertechnologies pour comprendre en temps voulu les opportunités et les risques qui en découlent. Pour détecter les dernières tendances sur le marché, le CYD Campus s'appuie sur une veille quantitatif et qualitatif des technologies et des marchés (Technology and Market Monitoring, TMM). La plateforme TMM permet d'une part de découvrir des cybertechnologies et des ensembles de celles-ci émergents grâce à une évaluation quantitative de données accessibles au public, et d'autre part de repérer des start-up prometteuses grâce à une recherche qualitative et d'un programme international de veille technologique.

Technologies de cybersécurité

Pour découvrir des technologies de cybersécurité pertinentes sur le marché, il est indispensable d'avoir accès à des sources de données contenant des informations actuelles et fiables sur les technologies proposées sur le marché. Le CYD Campus utilise pour cela sa propre plateforme de veille technologique et du marché (TMM) ainsi que d'autres sources.
Cette année, des chercheurs du CYD Campus ont rédigé un rapport donnant un aperçu des tendances et des activités en Suisse et à l'étranger dans le domaine des technologies de cybersécurité. Les conclusions ont été présentées le 2 décembre 2021 sur le site du CYD Campus à l'EPF de Lausanne.

Présentation de l'écosystème suisse de cybersécurité

Une étude dans le cadre de la plateforme TMM a été réalisée en collaboration avec l'ACAMIL à l'EPF Zurich. Il s'agissait de modéliser les écosystèmes publics, privés et académiques en lien avec le domaine cyber en Suisse. Plusieurs cartes sur les réseaux et une représentation géographique des principaux acteurs ont été développées. Une partie de ce projet a été publiée sur le site Internet du NCSC en mettant à disposition une liste des formations académiques disponibles en Suisse dans le domaine de la cybersécurité.
Lien vers la Swiss Cyber Map:

Scouting

Grâce à la recherche qualitative, le CYD Campus repère des start-up et des partenaires intéressants en Suisse et à l'étranger qui répondent aux exigences du DDPS. Le programme s'adresse principalement à des entreprises émergentes, mais aussi occasionnellement à des entreprises établies qui peuvent proposer des produits innovants. Un réseau a déjà été établi avec différents partenaires tels que Swissnex, Swisscom, PlugandPlay, divers accélérateurs de start-up et sociétés de capital-risque, ainsi qu'avec des ambassades et d'autres acteurs institutionnels, afin d'examiner systématiquement les marchés importants à la recherche de nouvelles tendances dans le domaine des cyber-technologies. D'un point de vue géographique, l'accent est mis sur les régions où se trouvent des start-up performantes.
Elles comprennent:

- Suisse: Trust Valley, Crypto Valley et Inno-Raum Zurich.
- États-Unis: pôles urbains autour de la Silicon Valley, Washington DC, Boston, New York, Seattle et Austin.
- Israël: une unité de l'armée fait émerger 8200 grands talents dans le domaine de la cybersécurité.
- Royaume-Uni: des universités renommées et un budget de défense important contribuent au paysage des start-up.
- France: le Pôle d'excellence cyber de Rennes encourage les travaux dans le domaine de la cybersécurité.
- Allemagne: promotion par des organisations telles que l'Institut de cyberdéfense de l'Université de la Bundeswehr à Munich.
- Estonie : site du Centre d'excellence de cyberdéfense coopérative de l'OTAN ainsi qu'un État avec un haut niveau de digitalisation.
- Singapour : l'État dispose d'une des dépenses de défense par habitant les plus élevées au monde.

Approche générale

Dans le cadre de l'activité de scouting, les ressources de chaque entreprise, le problème qu'elle tente de résoudre ainsi que la solution qu'elle propose sont analysés. On examine en outre pour quelles parties prenantes (armasuisse, autres autorités fédérales au sein et en dehors du DDPS) l'entreprise et sa solution pourraient s'avérer intéressantes. Le service concerné de l'administration fédérale peut également formuler une demande concrète et le CYD Campus s'efforcera de trouver, grâce à son réseau, les entreprises les plus innovantes et les mieux à même de relever un défi donné. Si nécessaire, une évaluation plus approfondie ou une preuve de concept sera lancée.

2021: 300 START-UP
dont 60 présentations techniques
dont 20 orientées vers des services compétents au sein de l'AF
8 preuves de concept mises en œuvre
12 partenaires de scouting actifs

Activités en 2021

Royaume-Uni

En avril 2021, le CYD Campus a effectué un repérage des entreprises de cybersécurité au Royaume-Uni. Le Swiss Business Hub (SBH) à Londres a joué un rôle déterminant dans l'identification des entreprises intéressantes et a établi, avec l'aide d'experts locaux et de toute l'équipe de l'ambassade, une longue liste d'une centaine de start-up et d'entreprises britanniques. Au Royaume-Uni, l'équipe de recherche a rencontré un grand nombre d'entreprises que l'on peut classer dans les grandes catégories suivantes : sécurité de la chaîne d'approvisionnement, analyse de données, réponse à la détection de réseau, systèmes de contrôle industriels, infrastructure et analyse des menaces.

Allemagne et Autriche

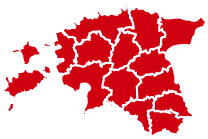
Un processus similaire à celui du Royaume-Uni a été mis en œuvre fin 2021 pour l'Allemagne et l'Autriche, ce qui a également permis d'identifier des entreprises intéressantes.

France

Le CYD Campus a participé au Forum international de la cybersécurité à Lille ainsi qu'à la semaine européenne de la cybersécurité et de la cyberdéfense à Rennes, au cours desquelles plusieurs nouveaux contacts ont été établis.

Estland

Une visite à Tallinn a été effectuée afin d'avoir un premier aperçu de l'écosystème de la cybersécurité local. Il y a quelques entreprises très intéressantes, notamment dans le domaine de la cyberformation. L'écosystème local de soutien aux start-up en termes de connaissances, de ressources financières et de ressources humaines est bien développé, mais le nombre absolu de start-up disruptives et matures est faible.



USA

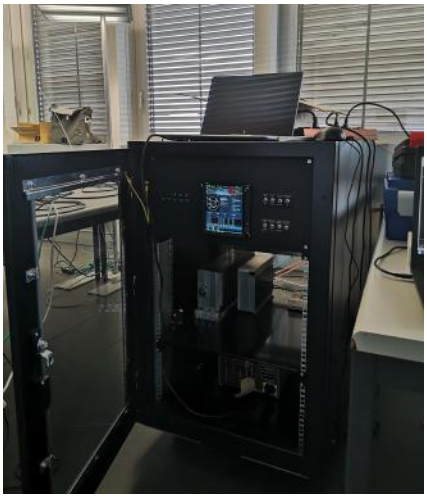
En 2019 et 2020, le paysage de la cybersécurité a fait l'objet d'une analyse approfondie pour trouver des technologies intéressantes. Compte tenu de la rapidité des évolutions et de l'ampleur du marché, un voyage aux États-Unis a été organisé en août 2021, ce qui a permis de rencontrer plusieurs entreprises supplémentaires et d'échanger des informations avec des partenaires-clés.

10 Infrastructures de laboratoire

Les installations de laboratoire du CYD Campus sont aménagées pour le développement collectif des connaissances. En plus du laboratoire de cybersécurité existant, des travaux ont été menés en 2021 pour développer les infrastructures de laboratoire, qui sont abordées plus en détail dans les sections suivantes.

Laboratoire de cyber-avionique étendu

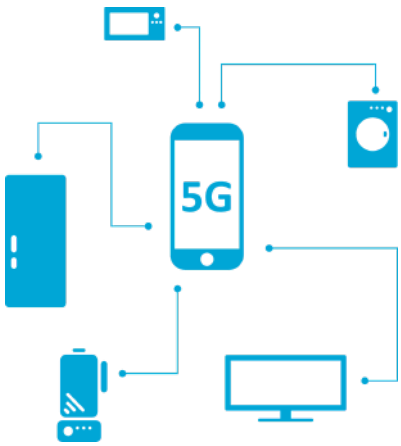
Le laboratoire d'avionique du CYD Campus a déjà soutenu avec succès les essais et les contrôles de sécurité des technologies aéronautiques, et les résultats ont notamment été publiés dans l'Aviation Village de la convention DEF CON. Le laboratoire s'enrichit désormais de la technologie de communications entre contrôleur et pilote par liaison de données (Controller-Pilot Data Link Communi-cations, CPDLC). Le système CPDLC est une liaison de données par laquelle des instructions critiques pour la sécurité sont échangées entre l'avion et les contrôleurs aériens. Les travaux de recherche du CYD Campus ont déjà montré que le système CPDLC n'est pas sûr sans authentification et que des attaques de type Man-in-the-Middle sont par exemple possibles. Il s'agit à présent d'expérimenter cela dans la pratique, dans un environnement de laboratoire avec du matériel certifié.



Extension du Cyber Avionik Lab avec communications entre contrôleur et pilote par liaison de données (CPDLC)

Laboratoire 5G en construction

Les connaissances techniques et les compétences dans le domaine de la technologie 5G sont faibles en Suisse, notamment dans le domaine de la sécurité et du cœur de réseau. La plupart des opérateurs externalisent la construction et même l'exploitation de l'infrastructure, et les institutions académiques n'ont pas accès à des laboratoires de recherche pour former les étudiants. Un laboratoire de recherche 5G en Suisse est d'une grande importance pour le DDPS et la BAC. Les infrastructures critiques auront de plus en plus recours à la technologie 5G à l'avenir. Le laboratoire de recherche 5G apportera les connaissances manquantes aux différentes organisations du DDPS et explorera le large éventail d'aspects liés à la sécurité.



Laboratoire Satcom

Un laboratoire Satcom sera mis en place pour compléter les plateformes d'expérimentation improvisées actuelles par de petites antennes satellites. Au centre de ce laboratoire se trouve une antenne parabolique de 2,5 m de diamètre, montée sur une plateforme motorisée. Celle-ci permet aux collaborateurs du CYD Campus d'orienter la parabole vers les satellites via une plateforme de configuration et, dans le cas de satellites non géostationnaires, de suivre leur orbite. Le récepteur de la parabole est conçu pour recevoir une grande variété de fréquences, ce qui permet aux chercheurs d'utiliser plusieurs bandes de fréquences simultanément. L'achèvement du laboratoire est prévu pour l'été 2023.

Satcom Cyber Security Lab à Zurich

Data Science Lab

Les algorithmes d'apprentissage profond nécessitent une grande capacité de calcul. Les processeurs graphiques (GPU) sont particulièrement optimisés pour le type d'opérations mathématiques effectuées par ces algorithmes. Afin de mettre à la disposition des chercheurs du CYD Campus des ressources de calcul suffisantes, un cluster de GPU a été mis en place dans le Data Science Lab. Celui-ci comprend une trentaine de GPU qui peuvent être mis à disposition de manière dynamique. Les utilisateurs n'ont qu'à soumettre leur tâche (code), qui sera automatiquement exécutée sur un processeur graphique libre. Il est ainsi possible de soumettre plusieurs tâches en même temps. Le contrôleur du processeur graphique gère l'attribution des tâches sur les différents processeurs graphiques. Cette infrastructure facilite l'utilisation et le partage des processeurs graphiques par les utilisateurs, p. ex. pour la traduction automatique, la détection de Fakes ou la prédiction de séries temporelles. Par ailleurs, un serveur FPGA a été mis en place cette année pour compléter les GPU et les CPU du laboratoire.

Scion

Afin de démontrer le potentiel des nouvelles technologies de réseau pour sécuriser le trafic de données sur des réseaux étendus (Wide-Area Networks, WAN), un laboratoire réseau est mis en place entre les trois sites du CYD Campus (Thoune, Lausanne et Zurich). Les sites seront reliés par la nouvelle technologie Scion de l'EPF Zurich afin de permettre un routage sécurisé et contrôlable. De plus, des commutateurs programmables sur les sites offrent la possibilité de mettre en œuvre de nouvelles méthodes de dissimulation du trafic de données sur le réseau et d'en étudier l'efficacité. Cette infrastructure de laboratoire est utilisée par les chercheurs et les partenaires du CYD Campus pour des projets de recherche et d'innovation.

La topologie du réseau Scion permet un routage efficace selon différents critères (source : anapaya.net)

11 Événements

Conférences

Du 16 au 18 novembre 2021 Semaine européenne de la cybersécurité et de la cyberdéfense à Rennes

Plus de 4000 acteurs publics et privés ainsi que 84 partenaires du domaine de la cybersécurité se sont réunis à Rennes pour identifier et anticiper les évolutions technologiques. Le CYD Campus y a participé pour nouer des liens avec des acteurs pertinents.

Du 27 au 29 septembre 2021 Conférence CYD & CRITIS

La conférence du CYD Campus s'est déroulée le 28 septembre 2021 au SwissTech Convention Center de l'EPFL à Lausanne (participation également possible à distance). La conférence a porté principalement sur la sécurité des infrastructures d'information critiques. Elle a été organisée en collaboration avec la 16e conférence internationale sur la sécurité des infrastructures d'information critiques (CRITIS 2021), qui s'est déroulée du 27 au 29 septembre.

Du 7 au 9 septembre 2021 Forum International de la cybersécurité à Lille en France

L'un des plus grands événements annuels en Europe consacrés à la cybersécurité, le Forum offre aux parties prenantes la possibilité de nouer des liens dans l'écosystème européen de la cybersécurité. En 2021, la Suisse était représentée pour la première fois par le CYD Campus et une douzaine d'autres entreprises. L'objectif principal de la participation du CYD Campus était de trouver des entreprises ayant des idées innovantes dans le domaine de la cybersécurité.

10 et 11 mars 2021 Swiss Cyber Security Days

Le Dr Vincent Lenders, le Dr Luca Gambazzi et Giorgio Tresoldi ont réalisé une vidéo sur le thème de l'exercice Locked Shields, diffusée dans le cadre de la conférence.

Challenges & Hackathons

Du 11 au 15 octobre 2021 Car Hackathon

Une vingtaine de personnes d'armasuisse, de l'industrie, de hautes écoles, de la BAC et de fedpol ont participé au Car Hackathon. La cybersécurité de divers véhicules a été examinée et des exploits ont été testés sur certaines vulnérabilités. Des voitures électriques, des véhicules à essence classiques et un Duro ont été testés.

28 septembre 2021 Cyber Startup Challenge

Sous la devise « Boostez votre centre de partage et d'analyse d'informations (Information Sharing and Analysis Center - ISAC) », cette édition du challenge avait pour objectif de trouver des solutions technologiques innovantes dans le domaine du renseignement sur les cybermenaces en mettant notamment l'accent sur la protection des infrastructures critiques. L'entreprise zurichoise gagnante, Decentriq, a été désignée lors de la conférence du CYD Campus le 28 septembre 2021.

Data Science Challenges

8 novembre 21:	Meme Classification
24 septembre 21:	Dialect Identification + GPU cluster
21 juin 21:	FitBit Data
10 mai 21:	IoT Device Fingerprints
29 mars 21:	Tipping Points
15 janvier 21:	Early Warning Signals

Discours introductif du directeur du CYD Campus lors de la conférence du CYD à Lausanne

Car Hackathon à Thoune

Forum International de la cybersécurité à Lille

Séminaires dînatoires

En raison de la pandémie persistante, de nombreux séminaires ont dû être annulés cette année. Lors de ces événements d'information, des conférences sont organisées par un certain nombre d'intervenants sur des thèmes techniques spécifiques du CYD pour les clients de la défense et de l'administration fédérale.

15 novembre 21: Quantum-Resistent Edge. Intervenant: Stiepan Aurélien Kovac, itk.swiss

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

19 mai 21: Tutoriel: Running programs at terabits per second in network switches (P4 and Intel Tofino), Intervenant: Roland Meier, ETH Zurich

3 mai 21: Séminaire Start-up: Avec trois start-up de Tech 4 Trust (Swiss Startup acceleration program in the field of digital trust and cybersecurity).

Intervenants:

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

Retraites

28 juin - 2 juillet 2021: Retraite Cyber Alp

Des chercheurs du CYD Campus et un certain nombre de partenaires de recherche ont donné des conférences sur des thèmes-clés de la cybersécurité et de la science des données. L'événement a rassemblé des acteurs du DDPS, de l'industrie et des sciences afin d'échanger sur les défis et les enjeux actuels et futurs du cyberespace.

Rapports de recherche

Les rapports annuels servent à rendre compte des thèmes de recherche en cours à l'intention des mandants et des services intéressés. Les rapports ont eu lieu sous une forme hybride et ont accueilli à chaque fois près de 80 invités. Certains participants étaient issus de l'État-major de l'armée, de la BAC, du SG-DDPS et du SRC.

3 juin 21: Rapport de recherche 3a Cyberspace

10 août 21: Rapport de recherche 3b Data Science

Séminaire dînatoire sur le thème Quantum-Resistent Edge à Thoune

Rapport de recherche Data Science à Thoune

Retraite Cyber-Alp 2021 à Gstaad

Visites

16 novembre 21: Visite de la Military Aviation Authority, Thoune

10 novembre 21: Visite du chef de l'armée, Thoune

1er novembre 21: Visite des stagiaires suivant la cyber-formation 2021 de l'armée, Thoune

15 octobre 21: Présentation de la Data Science aux étudiants EPF Zurich

8 september 21: Visite de la haute école de Lucerne et ICT Warriors, Thoune

Événement TMM

2 décembre 21: Technologies de la cybersécurité, CYD Campus Lausanne

Échanges professionnels d'étudiants

Un mardi sur deux, des étudiants et des stagiaires du CYD discutent des résultats de leurs projets de recherche. À cette occasion, tous les collaborateurs des sites concernés se rencontrent en ligne pour échanger sur des travaux de recherche et des conclusions.

Plateforme de recrutement d'étudiants

8 octobre 2021 Forum EPFL:

Cette année, le CYD Campus était présent au Forum de l'EPFL afin d'aller à la rencontre des étudiants, de leur donner un aperçu des activités du CYD Campus et de leur parler des diverses possibilités offertes par le CYD Campus pour acquérir une expérience pratique.

Atelier CYD Fellowship pour les candidats:

5 août 21

26 janvier 21

Visite des stagiaires en cyberformation de l'armée

Événement TMM sur les technologies de cybersécurité à Lausanne

Échanges sur les projets des étudiants à Thoune

12 Conférences

- 9 novembre 21 — *Collaboration EPFL-CYD Campus: Manager's Lunch*, EPFL Innovation Park, Lausanne, le Dr Vincent Lenders
- 25 octobre 21 — *Table ronde*, *Workshop on Systems Challenges in Reliable and Secure Federated Learning, ACM SOSP*, le Dr Gérôme Bovet
- 15 octobre 21 — *Panel on the future of digital trust*, Digital Trust 2025, Genève, le Dr Vincent Lenders
- 8 octobre 21 — *EPFL Forum*, Salon des carrières, Lausanne, le Dr Mathias Humbert
- 30 septembre 21 — *Security and Privacy in Wireless Communication Systems*, séance de clôture du groupe d'experts en cybersécurité du DDPS, le Dr Daniel Moser
- 3 septembre 21 — *Comprendre les cybermenaces*, DSC Security Week, le Dr Daniel Moser
- 27 août 21 — Vidéo deepfake de la Conseillère fédérale Viola Amherd, Kadertag VBS, le Dr Gérôme Bovet
- 26 août 21 — *Fusion von OSINT und SAR-IMINT - NATO/PfP Research Program SET-279*, séance d'information sur les satellites radar, armasuisse, Thoune, le Dr Albert Blarer
- 7 julliet 21 — *Présentation du CYD Campus*, visites des secrétaires généraux de la Confédération à l'EPFL», le Dr Vincent Lenders
- 9 juin 21 — *Voyage ministériel numérique de la Rhénanie-du-Nord-Westphalie en Suisse - Table ronde: Cyber Security*, le Dr Vincent Lenders
- 1 juin 21 — *Machine Learning for Intrusion Detection Systems: Challenges and Opportunities*, FUB TechTalk, le Dr Mathias Humbert
- 30 avril 21 — *Présentation CYD Campus*, Palais fédéral, visite de la ministre de la Défense, Autriche, le Dr Vincent Lenders
- 21 avril 21 — *Analyzing Cybersecurity Risks with and in Machine Learning*, SDSC (EPFZ/EPFL) & ZISC (EPFZ), le Dr Mathias Humbert
- 7 avril 21 — *Fake News in Social Media: How to fight them?* , Kdo Op - armasuisse S+T, le Dr Ljiljana Dolamic et le Dr Vincent Lenders
- 25 mars 21 — *Wireless Security in Critical Infrastructures: Legacy Debt and Opportunities*, ZISC (ETF), le Dr Martin Strohmeier
- 18 mars 21 — *Secure and Fast Satellite Broadband*, CySat, Davos, le Dr Vincent Lenders
- 10 mars 21 — *The role of AI in Cyberdefence*, Swiss Cyber Security Days, Fribourg, Le Dr Vincent Lenders
- 25 février 21 — *Cyber-Defence Campus: Bilan après 2 ans*, Sous-commission DFAE/DDPS du Conseil des États, Palais fédéral, le Dr Vincent Lenders
- 17 février 21 — *Cyberdefence Research and Innovation: The Swiss Approach*, UK-Swiss Cyber Seminar, Berne, le Dr Vincent Lenders
- 10 février 21 — *Research on Aviation Cyber Security*, BAZL, le Dr Martin Strohmeier
- 21 janvier 21 — *How (not) to do wireless security*, Eurocontrol, le Dr Martin Strohmeier
- 20 janvier 21 — *Deception technologies*, FUB TechTalk, le Dr Luca Gambazzi

13 Documents scientifiques

13.1 Publications

Décembre

Classi-Fly: Inferring Aircraft Categories from Open Data

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

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

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

Adaptive Uplink Data Compression in Spectrum Crowdsensing Systems

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

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

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

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

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

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

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

Novembre

Federated Learning for Malware Detection in IoT Devices

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

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

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

When Machine Unlearning Jeopardizes Privacy

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

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

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

Septembre

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

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

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

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

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

Août

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

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

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

Juin

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

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

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

Mai

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

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

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

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

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

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

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

Avril

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

Mars

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

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

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

Février

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

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

Crowdsourced Air Traffic Data from the OpenSky Network 2019–20

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

13.2 Travaux d'étudiants

CYD Fellows

Postdoc

Le Dr **Andrei Kucharavy**	*Evolutionary Dynamics for Improved GAN Detection*	EPF Lausanne
Le Dr **Dimitri Percia David**	*Technology Forecasting and Market Monitoring for Cyber-Defence*	Université de Genève

PhD

Alessandro Stolfo	*Privacy-Preserving Learning of Neural Language Models*	EPF Zurich
Simran Tinani	*Nonabelian Groups in Cryptography*	Université de Zurich
Dina Mahmoud	*ADHeS: Attacks and Defenses on FPGA-CPU Heterogeneous Systems*	EPF Lausanne

Master

Adalsteinn Jonsson	*PE Malware Detection with Deep Neural Model*	EPF Zurich
Lina Gehri	*Analyzing and Comparing Defense Strategies in a Cyber Defense Exercise*	EPF Zurich
Jan Urech	*Developing an Automaten Defender for Cyber Security Exercises*	EPF Zurich
Ksandros Apostoli	*Privacy-Preserving Proof-of-Personhood Token*	EPF Lausanne
Louis Merlin	*Recovering Type Information from Compiled Binaries to Aid in Instrumentation*	EPF Lausanne
Anita Mezzeti	*Modelling Portfolios of Cyber-Related Emerging Technologies: a Complex-System Approach*	EPF Lausanne
Zuowen Wang	*Understanding and Enhancing Adversarial Robustness for Machine Learning Models*	EPF Zurich

Étudiants et stagiaires

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

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

14 Communication

@Cyber-Defence Campus

@cydcampus

Publications sur Internet

- 20.12.2021, Collaboration fructueuse entre le Cyber-Defence Campus et l'office fédéral allemand de la sécurité des technologies et de l'information (BSI)
- 02.11.2021, Un collaborateur scientifique du CYD Campus obtient une chaire à l'Université de Lausanne
- 06.10.2021, Intelligence artificielle : vers une reconnaissance automatique des fake news ?
- 30.09.2021, Rencontrez les finalistes du Cyber Startup Challenge 2021
- 08.09.2021, Conférence du Cyber-Defence Campus 2021
- 27.07.2021, Le CYD Campus démontre de nouvelles formes d'attaque menaçant les infrastructures critiques
- 23.07.2021, Chercheurs du Cyber-Defence Campus récompensés par le Best Paper Award
- 23.06.2021, Le Cyber-Defence Campus identifie une faille de sécurité critique dans un logiciel VPN
- 10.06.2021, Appel au Cyber Startup Challenge 2021
- 25.05.2021, Le Cyber-Defence Campus à la conférence CyCon de l'OTAN à Tallinn, Estonie
- 21.05.2021, Le Cyber-Defence Campus, véritable force d'innovation

Communiqués de presse

- 20.12.2021, Collaboration fructueuse entre le Cyber-Defence Campus et l'office fédéral allemand de la sécurité des technologies et de l'information (BSI)
- 30.09.2021, , «Cyber Startup Challenge 2021» : la start-up Decentriq a convaincu le jury
- 25.05.2021, Projets de recherche du Cyber-Defence Campus du DDPS dans le cadre de la conférence Cyber Conflict de l'OTAN
- 22.03.2021, Nouvelle équipe du Campus Cyber-Defence du DDPS pour la détection des vulnérabilités logicielles

Armafolio

- Édition de décembre, L'intelligence artificielle au service de la désinformation sur les réseaux sociaux (en allemand)

Medien

- 15.10.2021, Der Schlüssel für eine effektive Cyber Defence liegt im Teamwork, Smart Media, Canal de distribution, Tagesanzeiger (en allemand)

15 Perspectives pour 2022

L'année prochaine, la collaboration du CYD Campus avec les hautes écoles et l'industrie sera étendue, notamment dans les domaines de la digitalisation, de l'intelligence artificielle et de l'innovation. Dans ces trois domaines, le DDPS, mais aussi l'ensemble de l'administration fédérale, sont confrontés à des défis technologiques majeurs. Il convient également de mentionner les étapes de développement suivantes et les activités prévues du CYD Campus, qui doivent être mises en œuvre en 2022 conformément à la Stratégie cyber DDPS:

- Élever le CYD Campus au niveau de compétences techniques national pour la cyberdéfense avec des hautes écoles et l'industrie. Il s'agit notamment d'étendre le soutien aux services de la Confédération actifs dans le domaine cyber en dehors du DDPS, comme les exploitants d'infrastructures critiques.
- Soutien à la mise en place du commandement Cyber. En particulier pour les projets de centre de cyberformation (Cyber Training Center, CTC), les moyens cyber mobiles (MCM), la formation prémilitaire et le stage de formation cyber.
- Développement d'un radar à technologie automatisé (TMM 2.0), qui utilise des bases de données et des sites Internet pour identifier rapidement les tendances et les technologies et évaluer leur importance pour la Suisse. Cet instrument doit soutenir les activités de scouting et de veille du CYD Campus, mais aussi à mieux gérer la base technologique et industrielle importante pour la sécurité (BTIS) de la Suisse.
- Extension du site d'antennes du CYD Campus à Zurich. Pour des raisons de place, le CYD Campus de l'EPF Zurich doit déménager dans des locaux plus grands à l'été 2022. Le nouveau site fournira des postes de travail et permettra également d'organiser des séminaires et des ateliers.
- Un nouveau concept de communication sera mis en œuvre en 2022. Le site Internet du CYD Campus subira une refonte complète avec davantage de contenus et d'actualités sur la cyberdéfense
- Les infrastructures des laboratoires du CYD Campus doivent continuer à être développées, notamment pour les projets dans le domaine de la sécurité 5G, de la sécurité SATCOM, de la sécurité des véhicules électriques et de l'Internet du futur.
- Développement du programme CYD Fellowship afin d'identifier et d'encourager dès que possible les cybertalents scientifiques. Un nouveau Fellowship pour les preuves de concept doit encourager la capacité d'innovation des jeunes talents et mieux les intégrer dans les processus d'innovation du DDPS.
- Envoi d'une personne au CCDCoE à Tallinn (Estonie). Un collaborateur du CYD Campus sera placé en permanence à Tallinn auprès du CCDCoE à partir de 2022 afin de promouvoir de manière ciblée la coopération avec l'OTAN dans le domaine de la technologie et de la recherche.

Contact
Cyber-Defence Campus
Feuerwerkerstrasse 39
CH-3602 Thoune

Zollstrasse 62
CH-8005 Zurich

EPFL Innovation Park, Bâtiment I
CH-1015 Lausanne

cydcampus@armasuisse.ch
+41 58 480 59 34

Plus d'informations:
https://cydcampus.ch