



Bern, 10. Dezember 2021

---

# **Die Zusammenarbeit des CYD Campus mit den Hochschulen, der Wirtschaft und den Kantonen**

## **Bericht des VBS an den Bundesrat**

---

## Inhaltsverzeichnis

1	Einführung .....	3
2	Zusammenarbeit mit den Hochschulen.....	3
3	Einbindung der Wirtschaft.....	4
4	Leistungen zuhanden der Kantone .....	5
5	Synergien innerhalb der Bundesverwaltung.....	5
6	Internationale Zusammenarbeit.....	6
7	Zukünftige Ausrichtung .....	7
8	Fazit .....	7

# 1 Einführung

Am 12. Mai 2021 hat der Bundesrat das VBS damit beauftragt, ihm bis Ende 2021 in einem Bericht darzulegen, wie der Cyber-Defence Campus (CYD Campus) mit den Hochschulen, der Wirtschaft und den Kantonen zusammenarbeitet (EXE 2021.1029). Mit dem vorliegenden Bericht kommt das VBS diesem Auftrag nach.

Der rasante Technologiewandel und die Digitalisierung führen dazu, dass immer mehr Systeme und Infrastrukturen miteinander vernetzt sind. Es werden zunehmend grössere Datenmengen generiert und öffentlich zugänglich gemacht. Aufgrund der Zunahme von Cyberrisiken und den Erfahrungen mit konkreten Angriffen baut das VBS seine Vorkehrungen zum Schutz vor Cyberangriffen laufend aus. Aus diesem Grund entstand im Jahr 2016 der erste Aktionsplan für Cyberdefence (APCD<sup>1</sup>). Angesichts der rapiden Weiterentwicklung der Cyberbedrohungslage wurde für den Zeitraum 2021–2024 die neue Strategie Cyber VBS 2021–2024<sup>2</sup> erarbeitet, die auf dem APCD aufbaut. Der Aktionsplan wie auch die neue «Strategie Cyber VBS» sind mit der übergeordneten Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS<sup>3</sup>) abgestimmt.

Im Januar 2019 wurde der Cyber-Defence Campus gegründet, um Cyber-Entwicklungen schneller zu antizipieren. Er ist heute integraler Teil der Strategie Cyber VBS 2021–2024 und bildet das Bindeglied zwischen VBS, der Industrie und der Wissenschaft in Forschung, Entwicklung und Ausbildung für die Cyberabwehr. Der CYD Campus ist ein Netzwerk wichtiger Cyber-Akteure sowie Organisationen mit Standorten in Thun (armasuisse W+T), Zürich (ETHZ) und Lausanne (EPFL). Zentral ist die Zusammenarbeit mit Partnern aus der Wissenschaft, den Leistungserbringern innerhalb des VBS, der Verwaltung – beispielsweise dem Nationalen Zentrum für Cybersicherheit (NCSC) – sowie der sicherheitsrelevanten Technologie- und Industriebasis (STIB) der Schweiz.

Der CYD Campus gehört zum Bundesamt für Rüstung (armasuisse) und erfüllt folgende drei Hauptaufgaben:

- Früherkennung der Entwicklungen im Cyber-Bereich: Dazu gehören ein umfassendes internationales Technologie- und Markt-Monitoring, der Aufbau eines Kollaborationsnetzwerks sowie die Führung eigener VBS-Forschungsprogramme.
- Entwicklung und Prüfung von Cyber-Technologien: Zusammen mit der Industrie und der Wissenschaft werden neue Lösungsansätze untersucht sowie bestehende Systeme auf ihre Sicherheit und Effizienz geprüft.
- Ausbildung von Cyber-Fachkräften: Beim CYD Campus werden Talente auf Master-, PhD- und Postdoc-Stufe sowie Hochschulpraktikantinnen und Hochschulpraktikanten für zukünftige Herausforderungen ausgebildet.

## 2 Zusammenarbeit mit den Hochschulen

Die Schweizer Hochschulen gehören zur Weltspitze in Wissenschaft, Innovation und Ausbildung. Die eidgenössischen technischen Hochschulen in Zürich (ETHZ) und Lausanne (EPFL) haben in den letzten Jahren erhebliche Anstrengungen unternommen, um Ausbildung und Forschung im Cyber-Bereich auszubauen. So bieten sie beispielsweise seit 2019 einen gemeinsamen Master-Studiengang in Cybersicherheit an und haben ihre Kompetenzen beim *Zurich Information Security and Privacy Center (ZISC)* an der ETHZ und beim *Center for Digital Trust (C4DT)* an der EPFL gebündelt und stark erweitert.

Der CYD Campus ist ein Partner des ZISC sowie des C4DT und bearbeitet mit diesen auf Cyberdefence ausgerichtete Forschungsprogramme. Damit werden unter anderem die Bedürfnisse des Departements an wissenschaftlichen und technischen Grundlagen gemäss der Strategie Cyber VBS 2021–2024 und der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018–2022 abgedeckt. Mit den CYD Campus Standorten an den beiden ETH, die 2019 durch armasuisse Wissenschaft und Technologie aufgebaut worden sind, ist eine noch engere Zusammenarbeit zwischen dem VBS und den Hochschulen ermöglicht worden. Diese Standorte bieten eine Kollaborationsplattform für den Bund und die Hochschulen. Bereits heute arbeiten an diesen Standorten

<sup>1</sup> Aktionsplan Cyber-Defence VBS (APCD) vom 9. November 2017. Abrufbar auf der [Website des VBS](#).

<sup>2</sup> Strategie Cyber VBS 2021–2024 vom März 2021. Abrufbar auf der [Website des VBS](#).

<sup>3</sup> Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018–2022 vom April 2018. Abrufbar auf der [Website des VBS](#).

## Die Zusammenarbeit des CYD Campus mit den Hochschulen, der Wirtschaft und den Kantonen

auch Experten aus der Wirtschaft mit. Diese Form von Zusammenarbeit im Bereich der Cyberdefence ist innerhalb der Schweiz einmalig.

Gemeinsam mit der EPFL hat der CYD Campus 2020 ein Cyberdefence Fellowship Programm lanciert. Das Programm bietet Unterstützung für Masterarbeiten, Promotionen und Studienaufenthalte für Kandidatinnen und Kandidaten mit herausragenden akademischen und beruflichen Leistungen. Dadurch werden Forschungsarbeiten gefördert, die für die Cyberdefence von Bedeutung sind und die Studierenden können einen Forschungsbeitrag zuhanden der Cyberabwehr der Schweiz leisten. Pro Jahr werden rund zehn Fellowships für die Durchführung einer Master-, PhD- und Postdoc-Forschungsarbeit am CYD Campus vergeben.

Weiter werden vom CYD Campus pro Jahr rund zwanzig Praktikumsstellen oder Masterarbeitsthemen für die Gewinnung und Ausbildung von Cyber-Talenten ausgeschrieben und von den Studierenden der Schweizer Hochschulen genutzt. Zu diesem Zweck hat der CYD Campus zwei Forschungsprogramme in den Bereichen Cyberspace und Datenwissenschaft etabliert, an welchen mehr als zwanzig nationale und internationale Hochschulen partizipieren. Das Ziel dieser Programme besteht darin, im Rahmen von Forschungskollaborationen neues Wissen und damit wichtige Erkenntnisse für die Cyberdefence in der Schweiz zu erschliessen. Aufgrund gewonnener Forschungserkenntnisse ist 2021 beispielsweise das EPFL-Spin-off Tune Insight AG entstanden, das im Bereich sichere Zusammenarbeit mit sensitiven Daten tätig ist. Gleichzeitig werden die notwendigen Kompetenzen für die Verwaltung und die operativen Einheiten sichergestellt. Als weiteres Beispiel für die erfolgreiche Zusammenarbeit mit der Wissenschaft dient ein ehemaliger Hochschulpraktikant von armasuisse, der heute die Koordinationsfunktion für die Schweiz am NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) in Tallinn wahrnimmt. Diese Tätigkeit belegt, dass es gelingt, eigens ausgebildete Wissenschaftler ins Cyber-Ecosystem einzubinden.

### 3 Einbindung der Wirtschaft

Die Schweizer Wirtschaft ist hinsichtlich Innovation und Entwicklung sowie Nutzung von Schlüsseltechnologien sowohl ein wichtiger Treiber als auch ein zuverlässiger Lieferant. Die Integration neuer Technologien und Methoden erfordert ein flexibles und vernetztes Vorgehen aller Beteiligten.

Der CYD Campus betreibt ein Technologie- und Markt-Monitoring, unter anderem über ein automatisiertes Web-Informationssystem, sowie ein aktives Technologiescouting zur Früherkennung der technischen Entwicklungen und zur Identifikation von wichtigen Akteuren im Cyber-Bereich. Werden neue Schlüsseltechnologien identifiziert, werden diese als Teil des Innovationsprozesses von armasuisse (Proof of Concepts) durch die Industrie im Auftrag des CYD Campus weiterentwickelt. Beispielhaft kann der Themenbereich *Künstliche Intelligenz* genannt werden: Neu entwickelte Algorithmen werden zur automatischen Klassifizierung von Signalen eingesetzt. Damit können Cyber-Angriffe schneller bemerkt werden. Ebenso werden neu entwickelte Technologien in kontrollierten, interaktiven Technologieumgebungen (sogenannten *Cyber Ranges*<sup>4</sup>) zur Ausbildung zukünftiger Experten eingesetzt. Zur gemeinsamen Entwicklung neuer Lösungen werden Partnerschaften mit Wirtschaftsunternehmen und Startups geschlossen. So wurde das Netzwerk in den Jahren 2020 und 2021 unter anderem mit Firmen wie Swisscom AG, IBM Research, Noser Engineering, Kudelski SA und Astrocast<sup>5</sup> erweitert. Diese Kooperationen fördern die Innovationskraft und erlauben einen Know-how- sowie Informationstransfer zwischen der Bundesverwaltung und der Privatwirtschaft, der angesichts der rasanten Entwicklungen im Cyber-Bereich notwendig ist.

In regelmässigen Abständen werden zudem sogenannte «Hackathons» zu aktuellen Herausforderungen<sup>6</sup>, Startup Challenges<sup>7</sup> und gemeinsame Übungen in Zusammenarbeit mit der Industrie organisiert. Diese Veranstaltungen dienen dem Kompetenzaufbau, der Konzeptüberprüfung (*Proof of Concept*) und der Erweiterung des Expertennetzwerks. Im Rahmen der Zusammenarbeit mit Start-ups wurden im Verlauf der letzten zwei Jahre eine Vielzahl von Demonstratoren aufgebaut und zahlreiche Anlässe organisiert. Unter anderem wurde ein Algorithmus entwickelt, der heute im Cyber Fusion Center der

<sup>4</sup> In dieser Umgebung können angehende Cybersicherheitsexperten lernen, wie sie Cyberangriffe erkennen und abwehren können, indem sie dieselbe Art von Ausrüstung benutzen, die sie auch bei ihrer künftigen Arbeit verwenden werden. In Cyber Ranges werden Angriffe auf IT-Infrastrukturen, Netzwerke, Softwareplattformen und Anwendungen simuliert.

<sup>5</sup> Schweizer Unternehmen für Satellitenkommunikation mit Sitz in Lausanne.

<sup>6</sup> z.B. zu Themen wie Darkweb, der Sicherheit von Aviatik- und Drohnensystemen, oder der Sicherheit von Elektrofahrzeuge und Ladeinfrastrukturen.

<sup>7</sup> "Cyber-Defence Campus lanciert Cyber Startup Challenge 2021", [Medienmitteilung vom 25.06.2021](#).

## **Die Zusammenarbeit des CYD Campus mit den Hochschulen, der Wirtschaft und den Kantonen**

Gruppe Verteidigung im operationellen Einsatz steht, ebenso wird ein Instrument für den NDB im Bereich der Lagerdarstellung evaluiert, welches für die Umsetzung der NCS 2 erforderlich ist.

Dank den hochspezialisierten CYD Campus Labors in Thun und den mit den Hochschulen geteilten Räumlichkeiten an den Aussenstandorten in Lausanne und Zürich können Projekte in enger Zusammenarbeit zwischen Bund, Industrie und den Hochschulen durchgeführt werden. Dieses neue Modell der offenen Zusammenarbeit (Open Labs und Open Innovation) hat sich sehr bewährt und fördert das gemeinsame Verständnis sowie das gemeinschaftliche Handeln.

## **4 Leistungen zuhanden der Kantone**

Insbesondere im Bereich kritischer Infrastrukturen erbringt der CYD Campus Leistungen zuhanden der Kantone. Kritische Infrastrukturen wie Stromversorgung, Telekommunikation, Luftraumsicherung und Spitäler werden weltweit zunehmend zur Zielscheibe von Cyberangriffen. Die Schweiz ist bisher grösstenteils von schwerwiegenden Cyberattacken verschont geblieben, muss sich aber der verschärften Bedrohungslage stellen.

Der CYD Campus schafft in diesem Zusammenhang Grundlagen, die dem Schutz kritischer Infrastrukturen dienen. Dadurch unterstützt der CYD Campus auch die Massnahme 5 zur Förderung der Grundlagenforschung im Rahmen der nationalen Strategie zum Schutz kritischer Infrastrukturen 2018-2022 (EXE 2017.2427 oder 8. Dezember 2017). So werden die Erkenntnisse des CYD Campus über Cyberisiken, -schwachstellen und -technologien mit den Betreibenden von kritischen Infrastrukturen geteilt. Dies erfolgt im Rahmen bilateraler Partnerschaften und regelmässiger Austauschplattformen wie Workshops, Hackathons oder Konferenzen.

In Zusammenarbeit mit dem Nachrichtendienst des Bundes (NDB), dem Nationalen Zentrum für Cybersicherheit (NCSC) und internationalen Partnern – etwa dem Bundesamt für Sicherheit in der Informationstechnik BSI Deutschland – entwickelt der CYD Campus neue Plattformen und Standards für den Austausch von Informationen zwischen den Betreibern kritischer Infrastrukturen zu Verwundbarkeiten und Sicherheitsempfehlungen. So organisierte der CYD Campus im September 2021 beispielsweise die dreitägige 16. Internationale Konferenz über die Sicherheit kritischer Infrastrukturen (CRITIS 2021) in Lausanne. An der Konferenz kamen Expertinnen und Experten aus der Bundesverwaltung sowie Vertreterinnen und Vertreter der Kantone, der Industrie und der Hochschulen zusammen, um sich über die neuesten Trends bezüglich der Sicherheit kritischer Infrastrukturen auszutauschen.

## **5 Synergien innerhalb der Bundesverwaltung**

Das Cyber-Dispositiv des Bundes gliedert sich in drei Bereiche: Cybersicherheit (EFD), Cyberdefence (VBS) und Cyberstrafverfolgung (EJPD). Der CYD Campus erbringt primär Leistungen für den Bereich Cyberdefence. Dank verschiedener Synergien, insbesondere im technologischen Bereich, profitieren auch die anderen beiden Bereiche von den Leistungen des CYD Campus. Direkte Leistungen werden jährlich in Dienstleistungsvereinbarungen (DLV) festgehalten. So führt der CYD Campus derzeit das Technologie- und Markt-Monitoring sowie die internationale Technologie-Trendanalyse unter anderem auch für das NCSC (EFD) durch. Für das EJPD werden Innovationsprojekte im Bereich Cybersicherheit und Datenwissenschaft bearbeitet.

Weitere Behörden der Bundesverwaltung wie das Bundesamt für Zivilluftfahrt BAZL (UVEK) und das Bundesamt für Statistik BFS (EDI) profitieren in den Bereichen Cybersicherheit und Datenwissenschaft aktiv von der Kompetenz des CYD Campus.

Obwohl die Forschungsprogramme des CYD Campus primär auf die Bedürfnisse der Armee und der Nachrichtendienste ausgerichtet werden, sind zahlreiche Themen für verschiedenste staatliche Akteure (siehe oben) verwertbar, wie nachfolgende Liste der Forschungsprojekte des CYD Campus verdeutlicht:

## Die Zusammenarbeit des CYD Campus mit den Hochschulen, der Wirtschaft und den Kantonen

Forschungsprojekt	militärisch	dual-use <sup>8</sup>
Sichere mobile Betriebssysteme		X
Erkennung von Software- und Geräteschwachstellen		X
Cyber-Täuschung	X	
5G Sicherheit		X
Künstliche Intelligenz für die Automatisierung von Cyberdefence Teams	X	
Cyber-Training		X
Quantensichere Kryptographie		X
Aufklärungsplattformen für Cyber-Bedrohungen		X
Cyber in der Luft- und Raumfahrt		X
Drohensicherheit und Abwehr		X
Netzwerk-Sicherheit		X
Resiliente und sichere verteilte Systeme (distributed computing)		X
Backdoors und Side-Channel Angriffe		X
Sicherheit von elektrischen Fahrzeugen und Ladeinfrastrukturen		X
Erweiterte und virtuelle Realität für die Simulation	X	
Datenwissenschaftliche Methoden zur Technologie- und Marktbeobachtung		X
Schwarmintelligenz	X	
Maschinelles Übersetzen		X
Erkennung von Fakes in soziale Medien		X
Big Data Technologien		X
Early Warning Signals in OSINT (Open Source Intelligence)		X
Kausalanalysen		X
Blockchain Anwendungen und Analyse		X
Verteilte IoT (Internet of Things) Sensoren		X
Datenschutz bei tragbaren Geräten		X
Robustheit und Störfestigkeit von maschinellem Lernen		X

## 6 Internationale Zusammenarbeit

Die Strategie Cyber VBS 2021–2024 und die NCS 2018–2022 weisen der nationalen und internationalen Zusammenarbeit eine wichtige Rolle zu, die künftig weiter gestärkt werden soll. Dabei nimmt der CYD Campus eine Führungsrolle im Rahmen der internationalen Zusammenarbeit im Bereich der Forschung und Innovation von Cybertechnologien ein.

Ein internationales Scouting mit verschiedenen Partnern wie Swissnex, Swisscom, PlugandPlay oder Crunchbase – allesamt wichtige Akteure im Bereich der Innovation – wurde etabliert, um wichtige Märkte wie beispielsweise das Silicon Valley, die USA generell, Israel, Grossbritannien oder China systematisch auf neue Trends im Bereich der Cyber-Technologien zu prüfen. Zudem wurden verschiedene bilaterale – unter anderem mit den USA (US Air Force Research Labs und Army Research Labs) und Luxemburg – sowie multilaterale Kollaborationen (NATO Cooperative Cyber Defence Centre of Excellence CCDCoE, European Defence Agency EDA etc.) eingegangen. Im Zuge dieser Kollaborationen werden regelmässig Mitarbeiterinnen und Mitarbeiter für den Know-how-Transfer entsendet. Im Rahmen dieser Entsendungen werden gemeinsame Forschungsprojekte durchgeführt.

Auch mit Hochschulen im Ausland werden Forschungskollaborationen gepflegt (zurzeit werden rund zehn internationale Forschungsprojekte an verschiedenen Hochschulen durchgeführt). Diese Projekte sollen Wissen über neue Technologien in die Schweiz transferieren und Lücken in der nationalen Forschungslandschaft schliessen.

<sup>8</sup> Dual-use beschreibt die prinzipielle Verwendbarkeit von Technologien oder Gütern zu zivilen als auch zu militärischen Zwecken.

## 7 Zukünftige Ausrichtung

In den kommenden Jahren soll die Zusammenarbeit des CYD Campus mit Hochschulen, der Wirtschaft und den Kantonen weiter ausgebaut werden, dies insbesondere in den Bereichen der Digitalisierung, der künstlichen Intelligenz und der Innovation. In diesen drei Bereichen steht das VBS, aber auch die gesamte Bundesverwaltung, vor grossen technologischen Herausforderungen. Daher ist es besonders wichtig, die Vernetzung und die Zusammenarbeit innerhalb des Bundes zu fördern und departementsübergreifende Synergien zu nutzen. Dies geschieht beispielsweise bereits heute mit dem Kompetenzzentrum für Datenwissenschaft des BFS und dem Kompetenzzentrum für Digitalisierung bei der Bundeskanzlei (Digitale Transformation und IKT-Lenkung DTI). Der Cyber-Defence Campus plant, seine Ressourcen primär so einzusetzen, dass die Bedürfnisse des VBS abgedeckt sind, wobei aber – wo sinnvoll – auch andere Bundesstellen von den Erkenntnissen profitieren sollen.

## 8 Fazit

Cyberdefence ist eine Verbundaufgabe, weswegen die nationale Zusammenarbeit zwischen Bund, Hochschulen, Wirtschaft und Kantonen von entscheidender Bedeutung ist. Der Cyber-Defence Campus hat sich innert kurzer Zeit als nationales Kompetenznetzwerk etabliert, welches Cyber-Akteure und Organisationen in der Schweiz miteinander verbindet. Der CYD Campus schafft mittels Forschung neue Erkenntnisse und generiert somit einen hohen Mehrwert für alle Beteiligten. Das VBS ist deshalb überzeugt, dass die neuen Zusammenarbeitsmodelle inkl. Open Labs, die der Cyber-Defence Campus in den letzten zwei Jahren realisiert hat, eine tragfähige Basis zur Bewältigung der komplexen zukünftigen Herausforderungen im Cyber-Bereich darstellt. Dieser Weg soll auch in Zukunft weiterverfolgt werden.