Forschungsprogramm 3a
Cyberspace

Dr. Vincent Lenders
Feuerwerkerstrasse 39
CH-3602 Thun
Tel +41 58 468 27 68
vincent.lenders@armasuisse.ch

Der Cyber-Raum ist zu einer militärischen Operationssphäre geworden, und immer mehr Staaten bereiten sich darauf vor, dieses zu nutzen. Diese Entwicklung erfordert in Streitkräften grundlegende Anpassungen, welche mit der Ausdehnung der Kriegführung in den Luftraum vor rund 100 Jahren vergleichbar ist. Im Cyber-Raum geht es jedoch, wie auch in der Luft, nicht nur darum, sich auf einen Konflikt vorzubereiten, sondern die ständige Verfügbarkeit, Integrität und Vertraulichkeit der Funktionen zu wahren, von denen wir abhängig sind. Die bislang vorherrschende Denkweise eines reaktiven, punktuellen Handelns muss einer Logik der Antizipation und Widerstandsfähigkeit weichen, um grosse Ereignisse zu bewältigen, die vermehrt gleichzeitig stattfinden können.

Die stete Weiterentwicklung und die Durchdringung der Digitalisierung in der Gesellschaft machen den Cyberspace zu einem zentralen Raum für moderne Konflikte und Kriege. Angriffe aus dem Cyberspace sind heute in der Schweiz sehr wahrscheinlich und mit einem schwer abschätzbaren Schadenspotential verbunden.

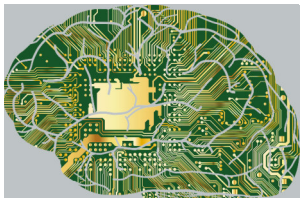
Ziel des Programms ist der Aufbau und die Sicherstellung von technologischen Fachkompetenzen zur Identifikation, Beurteilung und Reduktion von Risiken im Cyberspace. Aufgrund der sehr kurzen Technologiezyklen und der sich schnell ändernden Bedrohungslage, werden die Forschungsschwerpunkte agil entlang der Trends und dem Bedarf der Armee beim Cyber-Defence Campus geführt. Es werden Konzepte entwickelt, welche Anomalien im Datenverkehr auf den eigenen Netzen erkennen und so Angriffe detektieren und auf einem Lagebild der Operationssphäre Cyber darstellbar machen. Zum Schutz der eigenen Netzwerke werden Kompetenzen aufgebaut, welche Operationen zur aktiven Abwehr von Angriffen oder zur Täuschung von gegnerischen Akteuren im Cyberraum unterstützen. Gezielte Schwachstellenanalysen in kritischen Infrastrukturen und mobilen Geräten, Cybersicherheit in der Raum- und Luftfahrt sowie Post-Quantum-Kryptografie runden das Portfolio ab.

Moderne Laborinfrastrukturen werden eingesetzt um Forschungsresultate in einem praxisnahen Militärumfeld zu untersuchen. Nebst einem Cyber Sicherheit Lab zur Erforschung der Sicherheit von Software und Hardwarekomponenten in einer isolierten Umgebung, sind domänenspezifische Labs vorhanden für die Untersuchung der Sicherheit von zukünftigen Fahrzeug-, Flugzeug-, Satelliten-, Internet,- oder 5G-Kommunikation.

Kompetenzfelder

Cyber Schutz

Die Digitalisierung führt dazu, dass Informations- und Kommunikationsinfrastrukturen für kriminelle, nachrichtendienstliche, machtpolitische oder terroristische Zwecke vermehrt missbraucht werden. Zur frühzeitigen Erkennung von Bedrohungen und zur Erhöhung der Widerstandsfähigkeit im Cyberspace werden neue Sicherheitstechnologien und Cyber-Abwehrmethoden entwickelt.

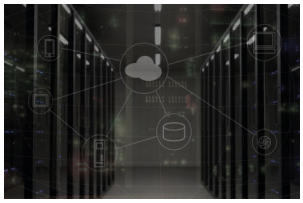


Cyber Operationsfähigkeiten

Cyber Operationen und Aktionen im Cyberspace gewinnen an militärischer Bedeutung. Die Reaktionsfähigkeit, um mögliche Folgen bei Vorfällen zu begrenzen, wenn nötig auch die Abwehr von Cyber-Angriffen durch Gegenmassnahmen zur aktiven Verteidigung wird hier untersucht.

Cyber Lagebilder

Die Cyber-Bedrohungslage ist durch eine Vielzahl von möglichen Bedrohungen geprägt. Diese unterscheiden sich hinsichtlich des Zwecks eines Angriffs, der Akteure, welche hinter den Angriffen stehen und des Kreises der Betroffenen. Neue Ansätze und Verfahren werden untersucht um ein Gesamtlagebild der Aktivitäten und Bedrohungen im Cyberraum darzustellen.



Robuste und hochsichere Cyber Infrastrukturen

Damit die Armee aber auch kritische Infrastrukturen in Notlagen und Krisen einsatzfähig bleiben, müssen sie jederzeit über funktionierende und sichere Informations- und Steuersysteme verfügen können. Dies erfordert hochsichere, robuste und autonome Cyber Infrastrukturen. Dafür werden automatisierte Methoden zum Auffinden und Beheben von Schwachstellen untersucht.

Technologieschwerpunkte

- **Sichere mobile Betriebssysteme**
- **Täuschung im Cyberspace**
- **Sicherheit von zukünftigen Fahrzeugen und Ladeinfrastrukturen**
- **5G Sicherheit**
- **Künstliche Intelligenz in der Cyberabwehr**
- **Quantum-sichere Kryptologie**
- **Cyber Sicherheit in der Luft- und Raumfahrt**
- **Identifikation von Software und Geräteschwachstellen**
- **Abwehr von Einsatzsystemen mit programmierbaren Netzen**
- **Lagebild Cyberspace**
- **Cyber Training**

Netzwerk

Für den Aufbau von Fachkompetenzen wird ein aktives und breites Netzwerk von Partnern aus Wirtschaft, Hochschulen, Universitäten und anderen Forschungsstellen im In- und Ausland eingesetzt und gepflegt. Zur Sicherstellung der Fähigkeitsorientierung findet ein enger Kontakt und Informationsaustausch zu Nutzern, Planungs-, Beschaffungs- und Erprobungsstellen des VBS statt.

Staatliche Partner / Bund

- Nationales Zentrum für Cybersicherheit NCSC
- Bundesamt für Luftfahrt BAZL
- NATO CCDCoE
- US Air Force Research Lab
- US Army Research Lab
- Luxemburgische Armee

Universitäten, Fachhochschulen / Industrie

- ETH Zürich
- EPFL
- Universität Zürich
- Universität Neuchâtel
- University of Oxford
- IBM Research
- Noser Engineering
- Ad Novum
- Astrocast
- Swisscom