Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence, Civil Protection and Sport
armasuisse
Science and technology

Research Program 3a
Secure in cyberspace

Dr. Bernhard Tellenbach
Feuerwerkerstrasse 39
CH-3602 Thun
Tel +41 58 467 21 59
bernhard.tellenbach@armasuisse.ch

Cyberspace has become a military domain of operations, and an increasing number of nations are preparing to use it. This development requires essential adjustments in the Armed Forces, which are comparable with the expansion of warfare into airspace around 100 years ago. However, in cyberspace, as in the air, it is not merely a matter of preparing for a conflict, but about maintaining the constant availability, integrity and confidentiality of the functions on which we are dependent. The hitherto prevailing approach of reactive, selective action must be replaced by a logic of anticipation and resilience, in order to cope with major events which could increasingly take place simultaneously.

The constant further development and penetration of digitalisation in society are making cyberspace a key area for modern conflicts and wars. The likelihood of cyberspace attacks occurring in Switzerland is very high, yet it is hard to predict how much damage could be caused.

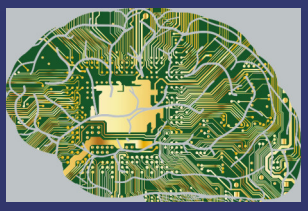
The goal of the programme is to build up and secure technological expertise in order to identify, assess and reduce risks in cyberspace. Due to the very short technology cycles and the rapidly changing level of threat, the research focuses are guided agilely by the current trends and the needs of the Swiss Armed Forces at the Cyber Defence Campus. Concepts are being developed which recognise anomalies in data traffic in own networks and thus detect attacks which can be displayed on an operational picture of the cyber domain of operations. To protect own networks, competences will be built up to support operations for active defence against attacks or to deceive enemy players in cyberspace. Specifi c vulnerability analyses in critical infrastructures and mobile devices, cyber security in aerospace as well as post-quantum cryptography round off the portfolio.

Modern laboratory infrastructures are being used to examine research results in a realistic military environment. In addition to a cyber security lab for researching the security of software and hardware components in an isolated environment, domain-specific labs exist to examine the security of future vehicle, aircraft, satellite, internet and 5G communication.

Competence areas

Cyber protection

Digitalisation leads to the fact that information and communication infrastructures are increasingly being abused for criminal, intelligence, power-political or terrorist purposes. In order to detect threats early and increase our resilience in cyberspace, new security technologies and cyber defence methods are being developed.



Cyber operational capabilities

Cyber operations and actions in cyber space are gaining in military significance. The response capability of restricting possible consequences during incidents, if necessary even defence against cyber attacks by active defence countermeasures is being examined here.

Cyber operational pictures

The cyber threat situation is characterised by several possible threats. These vary with regard to the purpose of an attack, the participants behind the attacks and those affected. New approaches and procedures are being examined in order to present an overall operational picture of the activities and threats in cyberspace.

Robust and highly secure cyber infrastructures

In order for the Armed Forces, but also critical infrastructures, to remain operational in emergency situations and crises, they must have access to functioning and secure information and control systems at all times. This requires highly secure, robust and autonomous cyber infrastructures. Automated methods for fi nding and eliminating vulnerabilities are being examined for this purpose.

Technology priorities

- Secure mobile operating systems
- Deception in cyberspace
- Security of future vehicles and charging infrastructures
- 5G security
- Artificial intelligence in cyber defence
- Quantum-secure cryptology
- Cyber security in aerospace
- Identification of software and device vulnerabilities
- Defence of deployment systems with programmable
- networks
- Cyberspace operational picture
- Cyber training

Network

The requisite professional skills build on a broad network of partners from business, universities (including universities of applied science) and other research units in Switzerland and abroad. To ensure that these skills are properly developed, there is close contact and an ongoing exchange of information with users and with planning, procurement and testing units within the DDPS.

State partners / federal government

- National Cyber Security Centre NCSC
- Federal Offi ce of Civil Aviation FOCA
- NATO CCDCoE
- US Air Force Research Lab
- US Army Research Lab
- Luxembourg Army

Universities, universities of applied sciences/ industry

- ETH Zurich
- EPFL
- University of Zurich
- University of Neuchâtel
- University of Oxford
- IBM Research
- Noser Engineering
- Ad Novum
- Astrocast