Research Program 3
Cyberspace and Information

Dr. Vincent Lenders
Feuerwerkerstrasse 39
CH-3602 Thun
Tel +41 58 468 27 68
Fax. +41 58 468 28 41
vincent.lenders@armasuisse.ch

The armed forces operational capabilities in cyberspace are becoming increasingly important. The ‚Cyberspace and Information' research program is developing the necessary expertise so as to extend traditional military capabilities in the areas of intelligence and command and control into the operational domain of cyberspace. This is achieved through research projects, demonstrators in laboratory environements, and experiments in real-life environments.

The constant growth of information technologies (IT) and the extent to which they have permeated society have made cyberspace a focus for contemporary conflicts and wars. Attacks against Switzerland from cyberspace are highly likely today and their potential to cause damage is very difficult to estimate. At the same time, however, cyberspace, seen as a military domain of influence, offers new opportunities for acquiring available information in a form that is more up-to-date, more comprehensive and of better quality.

The aim of the program is to develop expertise in new information technologies for acquiring, managing and analysing information from cyberspace as well as identifying and assessing the associated risks. Because of the very short technology cycles and the rapidly changing threat landscape, the main emphasis of research is conducted flexibly in line with technological trends and the current needs of the armed forces. At present, research activities are concentrated on four areas of expertise: cyber defence, information acquisition, information management, and fusion and visual representation.

In order to protect our own networks, expertise is built up to support the MilCert in repelling attacks. For example, concepts are developed to identify data traffic anomalies in our own networks and proactively combat attacks.

Thanks to today's communication media, cyberspace has become a place containing a wealth of information that can also be exploited for military operations. Social media and the internet of things, for example, provide comprehensive real-time information.

By managing and analysing large volumes of unstructured data (big data), specific information can be produced and visualized in a way which meets the requirements of decision makers. This requires combining expert military knowledge with basic technical and scientific principles. Assisted by a broad-based international network of experts comprising universities, industry and partners in government, the ‚Cyberspace and Information' research program ensures that the necessary technology expertise is developed.

Areas of expertise

Cyber defence

Digital interconnectedness leads to information and communication infrastructures being increasingly misused by criminals, terrorists, intelligence services or for the purposes of power politics. New security technologies and cyber defence concepts are being examined to identify threats at an early stage and to increase resilience to them in cyberspace.

Information management

Having the right information of the right quality at the right time is essential for operational command and control. Expertise is developed so as to be able to assess the latest information systems and architectures in view of the increasing volume, speed and heterogeneity of data from cyberspace (the big data problem).

Information fusion and visual representation

Modern analytical processes mean that data from a range of sensors and sources of information have to be combined and presented in a uniform context. Activities focus on new semantic and probabilistic ways of fusing and visualizing information so as to keep track of the situation and issue alerts.

Information acquisition

Acquiring information from publicly accessible sources in cyberspace offers fresh opportunities but also involves significant risks. New procedures for acquiring information will be examined and various approaches evaluated so that the interests and the identity of the people searching for information can be better protected.

Technology demonstrators

Social media intelligence

Analysing information from social media presents novel technical and analytical challenges. A demonstrator is being developed at S+T to investigate and present in a simple way technologies and procedures for acquiring information from, analysing and visualizing data obtained from social media.

Networks

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

- Swiss Armed Forces
- The Federal Intelligence Service
- armasuisse - Procurement
- Cooperative Cyber Defence Center of Excellence, Tallinn (EST)

Universities, universities of applied sciences/industry

- ETHZ, Zurich
- Information Security and Privacy Center, Zurich
- Université de Fribourg
- University of Oxford, GBR
- KU Leuven, BEL
- TU Kaiserslautern, GER
- IMDEA Networks Institute, ESP
- IBM Research, Rüschlikon
- Sero Systems, Kaiserslautern, GER
- Trivo Systems, Bern