



Programme de recherche 3 - Espace cybernétique et information

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



Les capacités opérationnelles de l'armée dans l'espace cybernétique prennent une importance toujours plus grande. Le programme de recherche «espace cybernétique et information» met en place l'expertise nécessaire pour développer les capacités militaires traditionnelles dans les domaines du service de renseignement et du commandement dans la sphère d'opération de l'espace cybernétique. Les travaux se déroulent sous la forme de projets de recherche et de l'utilisation de démonstrateurs pour des essais en laboratoire et dans l'environnement réel.

La croissance constante et la pénétration des technologies de l'information (IT) dans la société font de l'espace cybernétique un théâtre d'opérations central des conflits et des guerres modernes. Aujourd'hui, les attaques en provenance de l'espace cybernétique sont très probables en Suisse et leur potentiel de dommages est très difficile à évaluer. Simultanément, toutefois, l'espace cybernétique comme sphère d'action militaire offre de nouvelles possibilités d'obtenir les informations disponibles avec une meilleure actualité, intégralité et qualité.

L'objectif du programme est l'acquisition de compétences portant sur de nouvelles technologies de l'information en vue de l'acquisition, de la gestion et de l'analyse d'informations provenant de l'espace cybernétique, ainsi que l'identification et l'appréciation des risques connexes. Les cycles technologiques étant très courts et la situation de la menace changeant rapidement, les priorités de la recherche sont gérées avec une grande souplesse en fonction des tendances et des besoins actuels de l'armée. Actuellement, les activités de recherche se concentrent sur quatre champs de compétences. Ce sont: défense cybernétique, acquisition d'informations, gestion de l'information, et fusion et visualisation.

Pour protéger les propres réseaux, des compétences soutenant le MilCert dans la défense contre des attaques sont mises en place. Il s'agit, par exemple, de l'élaboration de

concepts en vue de la détection d'anomalies dans le trafic des données sur les propres réseaux et de la lutte active contre des attaques.

Avec les moyens de communication modernes, l'espace cybernétique est devenu un milieu contenant des quantités d'informations pouvant être utilisées aussi pour des opérations militaires. Les médias sociaux et l'Internet des objets, par exemple, sont des sources d'informations globales de grande actualité.

La gestion de grandes quantités de données non structurées (Big Data) et l'analyse de ces dernières permet d'obtenir des informations sélectives en fonction des besoins de décideurs et de les visualiser. Pour ce faire, il faut regrouper les connaissances spécifiques militaires et les bases technico-scientifiques. Le programme de recherche «espace cybernétique et information» fournit les compétences technologiques nécessaires à l'aide d'un vaste réseau d'experts international, composé de hautes écoles, de l'industrie et de partenaires étatiques.



Champs de compétences



Défense cybernétique

En raison de l'interconnexion numérique, les infrastructures d'information et de communication sont utilisées toujours plus fréquemment abusivement à des fins criminelles, pour l'obtention de renseignements, pour l'exercice du pouvoir ou par des terroristes. De nouvelles technologies de sécurité et des concepts de défense cybernétique sont analysés pour pouvoir détecter suffisamment tôt les menaces et améliorer la résistance dans l'espace cybernétique.



Gestion de l'information

Disposer des informations adéquates dans la qualité requise et au bon moment est essentiel pour la conduite opérationnelle. Des compétences sont mises en place pour pouvoir faire l'appréciation de systèmes d'informations et d'architectures modernes en relation avec les quantités croissantes, la vitesse et l'hétérogénéité des données en provenance de l'espace cybernétique (problématique Big Data).



Fusion d'informations et visualisation

Les méthodes d'analyse modernes requièrent de regrouper des données provenant de différents capteurs et sources d'informations pour les placer dans un contexte commun. L'accent est mis sur de nouvelles méthodes sémantiques et relevant de la théorie des probabilités pour fusionner et visualiser des informations servant au suivi de la situation et au déclenchement de l'alarme.



Acquisition d'informations

L'acquisition d'informations provenant de sources publiques dans l'espace cybernétique offre de nouvelles chances mais comporte aussi des risques importants. De nouvelles procédures d'acquisition d'informations sont analysées, et des approches sont évaluées pour mieux protéger les intérêts et l'identité des auteurs des recherches.

Démonstrateurs technologiques



Social Media Intelligence

L'analyse d'informations en provenance des médias sociaux comporte de nouveaux défis techniques et analytiques. W+T met en œuvre un démonstrateur permettant d'examiner de nouvelles technologies et procédures d'acquisition, d'analyse et de visualisation de données en provenance des médias sociaux et de présenter les résultats sous une forme simple.

Réseaux

Création et maintien d'un réseau actif d'experts et de partenaires nationaux et internationaux auprès de l'industrie, des écoles supérieures, des universités ainsi que des divers organismes et laboratoires de recherche. Afin de garantir une orientation adéquate des activités et un transfert optimal des connaissances, un contact étroit est établi avec le DDPS dans les domaines de la planification, des essais et des achats.

Partenaires étatiques / Confédération

- Armée suisse
- Service de renseignement de la Confédération
- armasuisse – Acquisitions
- Cooperative Cyber Defence Center of Excellence, Tallinn (EST)

Universités, Hautes écoles / industrie

- ETHZ, Zürich
- Information Security and Privacy Center, Zürich
- 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