Inauguration de Cyber-Defence Campus à lÊPFL

Autor(en): **Mermoud, Alain / Lenders, Vincent**

Objekttyp: **Article**

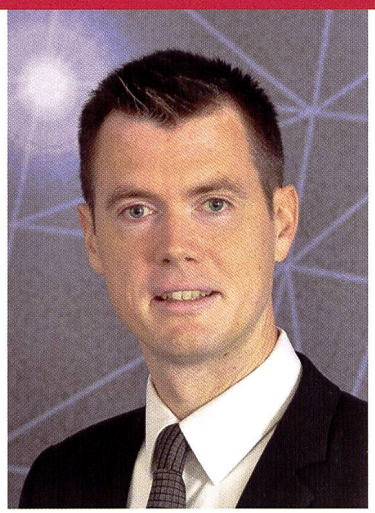
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2019)**

Heft 6

PDF erstellt am: **27.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-977460



L'inauguration du Cyber-Defence (CYD) Campus et une conférence de deux jours à Lausanne le 5 septembre dernier ont marqué le début d'un partenariat renforcé entre le DDPS et l'EPFL.

armasuisse Sciences+Technologies

Inauguration du Cyber-Defence Campus à l'EPFL

Dr. Alain Mermoud*, Dr. Vincent Lenders**

* Chef veille technologique CYD Campus, armasuisse S+T, ** Directeur CYD Campus, armasuisse S+T

La cyberdéfense exige des approches coordonnées en vue de s'adapter rapidement aux nouvelles menaces et de développer les compétences et capacités requises. Après Thoune et Zurich, armasuisse Science et Technologie (S+T) a ainsi implanté un nouveau site de son CYD Campus[1] à l'Innovation Park de l'EPFL, marquant le début d'un partenariat avec le « Center for Digital Trust » (C4DT).[2] Ce partenariat est placé sous le signe d'une collaboration plus étroite en matière de recherche et de développement avec l'écosystème de l'innovation de l'EPFL. Il vise à offrir de nouvelles perspectives de collaboration ouverte entre les chercheurs de l'EPFL, l'industrie et armasuisse. Ce partenariat met l'accent sur la promotion des transferts de technologies et d'innovations, en accordant la priorité à la cybersécurité, à la confiance numérique (*Digital Trust*), à la science des données et à l'intelligence artificielle (IA).

Les trois piliers du plan d'action DDPS pour la cyberdéfense sont les suivants :

1) La Base d'aide au commandement (BAC) pour l'utilisation sûre des systèmes et infrastructures d'information et de communication (TIC) ;
2) Le renseignement et la défense pour la protection et l'action dans le cyberespace ;
3) Le Campus cyberdéfense comme unité de soutien et centre de compétences placé sous la responsabilité d'armasuisse.

Ce nouveau partenariat matérialise une partie de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)[3] ainsi que le Plan d'action cyberdéfense du DDPS (PACD).[4] Plateforme d'anticipation en matière de cyberdéveloppements, le CYD Campus sert donc de lien entre le DDPS, le monde académique et l'industrie, créant ainsi un écosystème visant à produire une capacité de cyberdéfense efficace. Les tâches du Campus cyberdéfense incluent entre-autres :

La veille technologique

Plateforme d'anticipation : une partie de cette prestation consiste à élaborer et à actualiser en continu une cartographie des cybertechnologies et cyberacteurs en Suisse sur la base d'outils de surveillance des technologies et des marchés, en utilisant et en développant le réseau de compétences existant. La préparation, la diffusion et la publication des découvertes et tendances en fonction des groupes cibles constituent une plus-value importante en la matière.

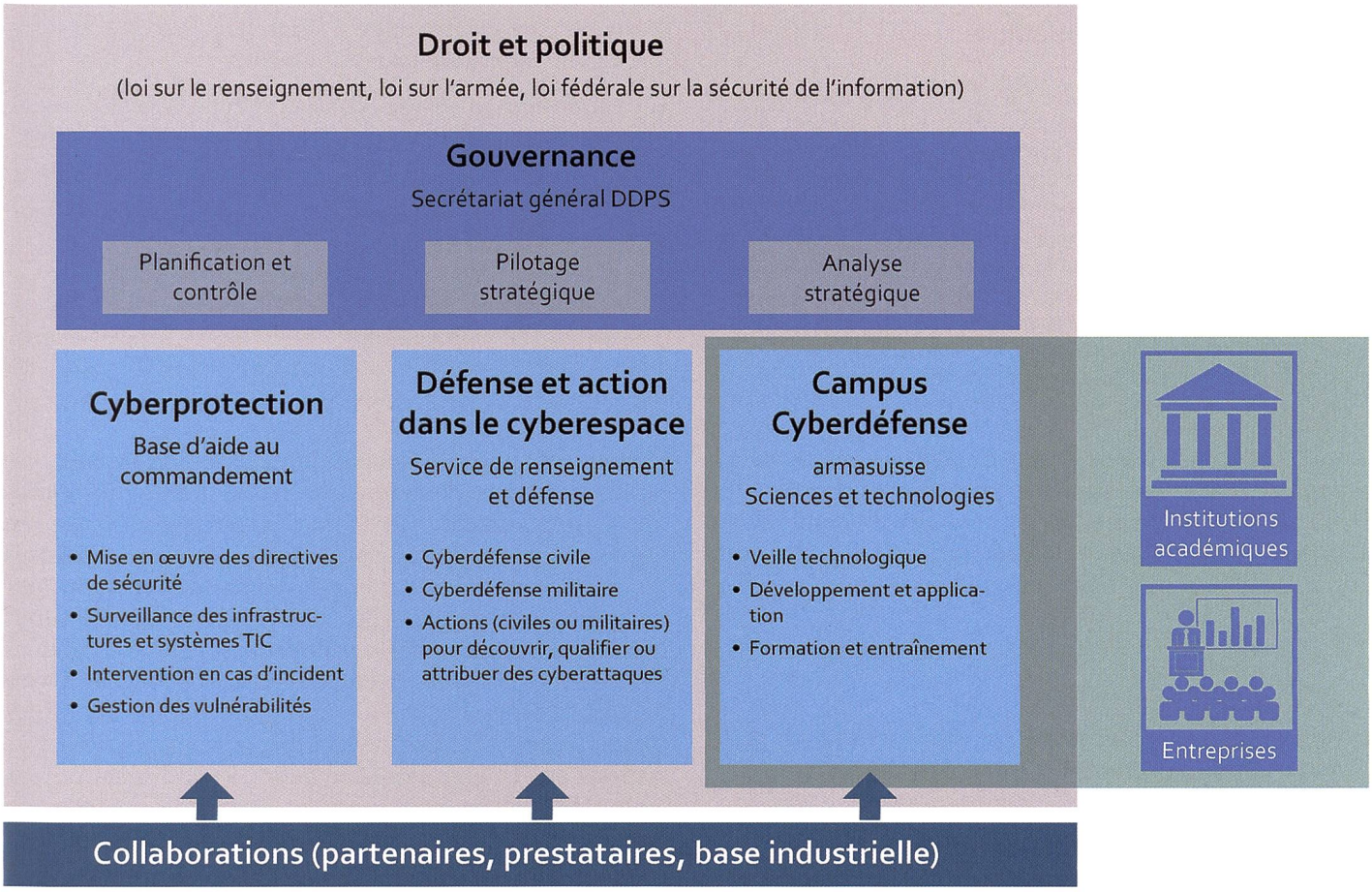
Réseau de compétences et savoir-faire :
les compétences nécessaires sont assurées au moyen des propres laboratoires de cyberdéfense ainsi que de partenariats stratégiques au niveau de la recherche sectorielle comme de la base technologique et industrielle suisse (STIB) du domaine de la sécurité.[7] Un réseau international axé sur les besoins est mis sur pied et développé en collaboration avec des nations amies et des organisations multilatérales dans le cadre du CYD Campus.

1 Plus d'informations sur le CYD Campus : https://www.ar.admin.ch/fr/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html (consulté le 09.09.19)

2 Plus d'informations sur le C4DT : https://www.c4dt.org/ (consulté le 09.09.19)

3 Plus d'informations sur la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) : https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html (consulté le 09.09.19)

4 Plus d'informations sur le Plan d'Action Cyberdéfense du DDPS (PACD) : https://www.vbs.admin.ch/fr/defense/protection-cyberattaques.detail.document.html/vbs-internet/fr/documents/defense/cyberattaques/Aktionsplan-Cyberdefense-f.pdf.html (consulté le 09.09.19)



Le plan d'action pour la cyberdéfense du DDPS (déjà évoqué dans la RMS) se décline en trois pans : le fonctionnement sûr des systèmes et infrastructures des technologies de l'information et de la communication (TIC), la défense et l'action dans le cyberespace, et enfin le Campus cyberdéfense (CYD Campus).

Développement et application

Il s'agit notamment de définir et de certifier des partenaires stratégiques, de développer des propres composants de niche ainsi que des composants logiciels et matériels, d'assurer la souveraineté technologique dans des domaines clés et d'analyser les risques comme les faiblesses (« second opinion ») pour garantir la sécurité et l'interopérabilité des acquisitions et de l'exploitation.

Formation et entraînement

Promouvoir et attirer les talents : les résultats de recherche forment la base de la formation et de l'entraînement au sein du CYD Campus. En accompagnant des travaux de bachelor, de master et de doctorat, nous formons les jeunes talents et recrutons des « hauts potentiels » le plus tôt possible dans leur carrière. Il s'agit là d'une contribution majeure à la préparation du personnel du DDPS à l'avenir numérique.

Une conférence de deux jours en présence du futur chef de l'armée

La conférence de deux jours consacrée à l'IA a fait intervenir des experts internationaux de premier plan issus du monde de la recherche, de l'industrie et des autorités à l'occasion de deux *keynotes* et de dix présentations. Ces deux journées ont principalement porté sur le rôle que joueront les futures cybermenaces et les développements dans le domaine de l'IA pertinents pour le secteur de la défense et de la sécurité.

Conséquences de l'IA sur la défense et les forces armées

En résumé, la conférence a démontré que l'utilisation de l'IA transforme tous les domaines de la défense et de la sécurité. Historiquement, l'élément clé des programmes modernes d'IA est leur capacité à prendre des décisions autonomes. Selon le Chef de la BAC, l'IA joue en réalité déjà un rôle important dans l'entier de la boucle[5] OODA.

Dans le monde entier, d'énormes investissements sont consacrés à de tels programmes, et l'IA est de plus en plus utilisée comme une ressource stratégique pour le positionnement et l'influence politique. Simultanément, le caractère autonome de la prise de décision marque la phase initiale d'une course aux armements en IA. Que ce soit dans la défense contre les cyberattaques ou dans la création de

5 La boucle OODA (*OODA loop*) est un concept inventé par le pilote de chasse John Boyd de l'United States Air Force en 1960 pour conceptualiser sa facilité à battre tous ses élèves lors de simulations de combats aériens, en itérant rapidement quatre processus : « Observe, Orient, Decide and Act » (« observer, s'orienter, décider et agir »). À l'usage, ce concept s'est révélé applicable dans bien d'autres situations, notamment dans le domaine de l'IA.

L'apprentissage automatique

L'apprentissage automatique (*machine learning*) est une discipline de l'intelligence artificielle. Elle permet aux systèmes informatiques de reconnaître des modèles et des lois basés sur des données et des algorithmes et de développer des modèles. Ces modèles peuvent ensuite être utilisés pour résoudre des problèmes tels que la classification d'objets ou la détection d'anomalies. L'apprentissage automatique devient de plus en plus important pour l'armée. C'est le cas partout où les données sont disponibles sous forme numérique et peuvent donc être analysées plus rapidement et plus efficacement par un ordinateur que par un être humain.

Prochaine conférence à Zurich : La cybersécurité dans l'aviation

La prochaine conférence CYD Campus aura lieu au Hilton de l'aéroport de Kloten les 19 et 20 novembre 2019. Inscription et programme sur l'application pour les événements :

Pour télécharger l'application, recherchez « Events ar W+T » dans l'App store ou cliquez sur l'un des liens ci-dessous :

Lien App Google : http://bit.ly/2YfMdMP
Lien App Apple : https://apple.co/2YK5aGH

complexes connaissance de la situation ou même mises en œuvre dans des systèmes d'armes autonomes, les applications d'IA permettent de résoudre de nombreuses tâches avec des performances impressionnantes qui surchargent la pensée humaine en temps normal

Le divisionnaire Thomas Süssli, actuellement chef de la Base d'aide au commandement (BAC), est entré dans le corps des officiers de carrière en 2015, après une longue et brillante carrière civile dans la banque. Sa nomination à la tête de l'armée symbolise la montée en puissance de la cyberdéfense, un domaine où le transfert de connaissance entre civils et militaires est particulièrement important.

Cependant, la haute qualité des solutions d'IA n'est pas gratuite. La grande complexité des nouvelles approches d'IA, par exemple les systèmes d'apprentissage en profondeur, précèdent l'explicabilité de tout processus de prise de décision. L'inexplicabilité devient à son tour un problème majeur si les conséquences des décisions prises par les machines ont des conséquences juridiques ou éthiques inappropriées. La grande complexité ouvre la porte à différents types d'abus et de manipulations des programmes d'IA. Des débats précoces sur les multiples aspects de l'IA entre les chercheurs, les utilisateurs et les autorités réglementaires offrent l'occasion de façonner le développement et l'utilisation de technologies d'IA bénéfiques. Cette conférence a fourni une première plate-forme dans ce sens.

Exemple d'un projet récent développé par le CYD Campus

Détecter les cyber-attaques en temps réel

Les cyberattaques réussies passent souvent inaperçues pendant plusieurs mois. En collaboration avec des experts d'armasuisse S+T et de l'EPF de Zurich, le CYD Campus a développé une méthode qui permet à l'armée d'identifier en temps réel les cyberattaques sur les réseaux informatiques militaires. Cette méthode pour une défense plus efficace dans le cyberespace est basée sur l'apprentissage automatique (*machine learning*). L'objectif est qu'à l'avenir, l'armée soit en mesure de détecter les activités des attaquants de manière fiable et en temps réel. Cette méthode a été utilisée pour la première fois dans le cadre de l'exercice «*Locked Shields*», le plus grand exercice international de cyberdéfense au monde, organisé par l'OTAN.

Déroulement de l'exercice

L'exercice international de cyberdéfense «*Locked Shields*» est organisé chaque année par le Centre d'excellence de cyberdéfense coopérative de l'OTAN à Tallinn (Estonie). En avril dernier, plus de 1'000 cyber-experts y ont participé. Une équipe d'attaquants expérimentés, la *Red Team*, a mis à l'épreuve les défenses de différentes nations cette année encore en avril pendant plusieurs jours. Des équipes nationales de spécialistes IT, agissant comme des équipes bleues, aident chacune un pays fictif à s'armer contre les cyberattaques à grande échelle de l'équipe

rouge. L'équipe bleue suisse, qui est dirigée chaque année par la Base d'aide au commandement (BAC) est également impliquée. Le réseau à protéger se compose d'ordinateurs et de serveurs traditionnels, mais aussi d'appareils dotés d'applications logicielles pour les infrastructures critiques ainsi que de routeurs et d'appareils pour la communication mobile sans fil.

Pendant tout l'exercice, l'équipe rouge attaque les systèmes de l'équipe bleue. Les activités sont enregistrées dans le réseau protégé par les équipes bleues. Après l'exercice, les équipes bleues sont évaluées et l'équipe rouge soumet un rapport sur les attaques et les tactiques utilisées afin que les équipes bleues puissent améliorer leurs stratégies de défense.

Le CYD campus s'attaque aux cyberattaques

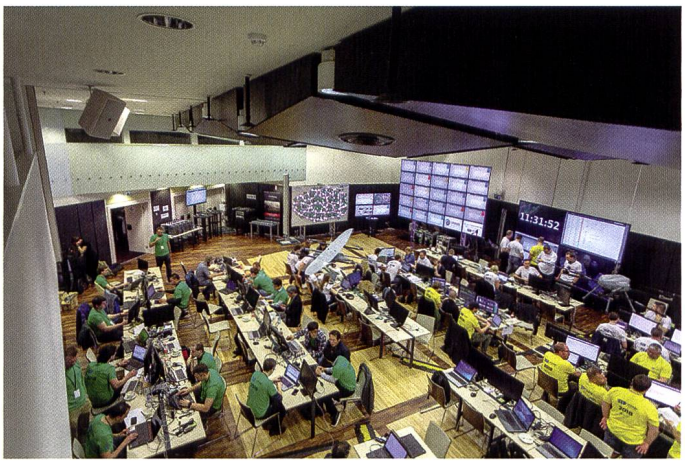
Le CYD Campus, en l'occurrence une équipe de cyber-experts d'armasuisse S+T et d'étudiants du groupe de l'ETH Zurich dirigé par le Prof. Laurent Vanbever, a évalué les possibilités d'identifier des canaux de communication entre les logiciels malveillants et les serveurs *Command and Control* (C2) au moyen de l'apprentissage automatique.

Les cyberattaques, c'est-à-dire le trafic de données des attaquants, doivent pouvoir être identifiées en temps réel afin de limiter au maximum le nombre de ces incidents. Dans la pratique, les ressources humaines disponibles ne sont pas suffisantes pour analyser manuellement l'énorme quantité de flux de données. Par conséquent, la caractérisation du trafic de données est réalisée avec une nouvelle approche de l'apprentissage automatique.

Le projet a d'abord défini et évalué environ 80 caractéristiques de flux de données pour différencier les flux de trafic réseau légitimes et malveillants. Grâce aux enregistrements de plus de 300 Go d'exercices « *Locked Shields* » des années précédentes, le CYD Campus a pu analyser le comportement et les moyens utilisés par les attaquants par apprentissage machine et développer ses propres techniques de détection et d'intervention. Après plusieurs unités de test, la nouvelle méthode a obtenu de meilleurs résultats que les méthodes connues auparavant, qui fonctionnent sans apprentissage machine: le CYD Campus a atteint une précision d'identification de 99% et un taux de rappel de plus de 90%. Afin d'accroître l'efficacité de la caractérisation des données pour distinguer le trafic de données légitime du trafic malveillant, les 20 caractéristiques les plus influentes des 80 caractéristiques de flux de données définies ont été sélectionnées.

Application réussie de la méthode dans l'armée

Afin de permettre à l'armée d'utiliser cette nouvelle méthode, le CYD Campus a travaillé en étroite collaboration avec la BAC ces derniers mois. Les nouvelles procédures ont été intégrées par des « Cyber-Sergents » dans les systèmes existants de la BAC et étendues de telle sorte que la détection des attaques avec les systèmes d'enregistrement réseau existants de la BAC fonctionne en temps réel



En avril 2019, la procédure a été utilisée pour la première fois lors de l'exercice LOCKED SHIELDS par la Swiss Blue Team. Cet exercice confirme que la méthodologie est très efficace pour détecter les attaques de l'équipe rouge en temps réel.

La manière dont un tel projet a pu être réalisé en moins d'un an, de l'idée à la mise en œuvre réussie, est presque aussi importante que le résultat. Grâce au lien étroit entre la recherche fondamentale de l'ETH Zurich et les unités opérationnelles de cyber-organisation des forces armées, le CYD Campus a pu transférer et mettre en œuvre très rapidement et de manière agile les résultats et les nouvelles connaissances acquises dans les forces armées. En retour, de nouvelles expériences pratiques et questions ont été acquises dans les forces armées, qui à leur tour seront incluses en tant que nouveaux projets sur le CYD Campus et se sont poursuivies cette année avec les universités.

Comment d'autres organisations peuvent-elles tirer profit des résultats?

Les résultats du projet ont été publiés et présentés à l'*Annual International Conference on Cyber Conflict* (CyCon 2019)[6] en mai 2019 à Tallinn. Cette publication devrait permettre aux autres nations, mais aussi aux organisations civiles, de bénéficier des connaissances acquises pour leur propre défense.

A. M., V. L.

CYD | CYBER DEFENCE CAMPUS

6 https://cycon.org/ (consulté le 10.09.19)

7 https://www.ar.admin.ch/fr/beschaffung/sicherheitsrelevante-technologie-und-industriebasis-stib.html (consulté le 03.11.19)