

Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: Fighting hackers : début de l'instruction en cybernétique de l'Armée suisse
Autor: Vernez, Gérald
DOI: <https://doi.org/10.5169/seals-823448>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 23.02.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>



Les candidats lors de l'évaluation à Jassbach.
Photo © Auteur.

Cyber

Fighting hackers : Début de l'instruction en cybersécurité de l'Armée suisse

Gérald Vernez

Délégué à la cyberdéfense, DDPS

Le stage de formation en cybersécurité débutera le 6 août 2018 : environ 20 recrues et cadres triés sur le volet entameront une phase d'instruction exigeante et intensive avec des objectifs très élevés. Ce stage de formation permet à l'Armée suisse d'étendre ses capacités cybersécuritaires et de renforcer la capacité à durer de son personnel.

Est-il possible d'organiser une instruction en cybersécurité dans le cadre des stages de formation de base de l'Armée suisse avec au moins 20 participants ? Ces derniers peuvent-ils satisfaire aux exigences élevées des engagements cybersécuritaires après le stage de formation ? Pour apporter des réponses à ces questions, la Base d'aide au commandement (BAC) et le commandement de l'Instruction (cdmt Instr) ont mis sur pied fin 2017 une équipe de projet composée de militaires de carrière et de cybersécuristes de l'organisation professionnelle de la BAC. Des représentants du Secrétariat général du DDPS et du Secrétariat d'Etat à la formation, à la recherche et à l'innovation, des officiers de milice de l'état-major de la BAC et l'association professionnelle ICTSwitzerland ont également été associés aux travaux afin de leur fournir une assise solide. Au cours des six derniers mois, l'équipe de projet a élaboré un concept de stage de formation qui doit maintenant être mis en œuvre et contrôlé dans le cadre d'un stage pilote.

Genèse et conception

Le développement de l'armée prévoit de renforcer le domaine cybersécuritaire avec une compagnie disposant d'une centaine de cybersécuristes. Pour couvrir les besoins qui en découlent au niveau de la relève, l'instruction en cybersécurité qui existe depuis 2010 au sein de l'école de guerre électronique 64 (E GE 64) doit être adaptée. Jusqu'à présent, l'organisation professionnelle formait directement entre deux et quatre recrues par école de recrues (ER) sur les systèmes d'engagement de la BAC. Puisque le nombre

de participants sera bien plus élevé à l'avenir, cette solution ne pourra plus être appliquée. L'instruction a été repensée sous la forme de sous-domaines. C'est ainsi qu'est née l'instruction en cybersécurité, organisée pour la première fois à l'E GE 64 en tant que stage de formation pilote avec le début de l'ER 2/2018.

Sélection et formation

La durée d'une simple ER est insuffisante pour assimiler toute la matière. C'est pourquoi l'instruction dure 40 semaines – comme pour les éclaireurs parachutistes –, et toutes les recrues accomplissent le perfectionnement menant au grade de sergent. Avant que le recrutement ne se déroule selon le processus normal (probablement dès l'ER 1/20), les candidats intéressés et compétents de toute la Suisse seront sélectionnés dans les ER. L'armée souhaite en particulier motiver des femmes à suivre l'instruction en cybersécurité.

Une grande importance est attachée au processus de sélection : celui-ci comprend tant des tests écrits et en ligne que des entretiens personnels. En effet, la matière enseignée est vaste et exigeante et requiert une motivation et une persévérance supérieures à la moyenne. De plus, il est indispensable de mieux connaître les recrues lors des entretiens personnels, car il ne faut surtout pas qu'un usage abusif soit fait des connaissances acquises lors de l'instruction. Les recrues sélectionnées accompliront le stage de formation en cybersécurité après l'instruction militaire de base.

Les disciplines enseignées lors des quelque 800 heures d'instruction vont de l'éthique au droit en passant par les technologies de l'information et de la communication et une formation classifiée dans le domaine technique proprement dit. Cette dernière dépend de la fonction dans laquelle l'incorporation a lieu (voir encadré). L'instruction axée sur l'engagement est quant à elle effectuée sur les systèmes d'engagement

de l'organisation professionnelle de la BAC dans le cadre de petits détachements.

Étant donné que les menaces, les procédures et les moyens se développent particulièrement vite dans le cyberspace, la BAC conserve la responsabilité technique du stage de formation afin de garantir que l'expérience acquise en engagement se retrouve dans l'instruction. De son côté, le cdmt Instr répond de l'organisation du stage de formation. Les participants dont les performances sont insuffisantes ou dont le comportement est problématique reçoivent un statut provisoire. S'il n'y a pas d'amélioration, ils sont incorporés dans une autre fonction au sein de la conduite de la guerre électronique.

Collaboration avec l'économie privée

Une attention particulière a été portée au corps enseignant afin d'assurer un lien avec le monde professionnel et les études. Le concept du stage de formation en cybersécurité a été présenté à l'association ICT-Formation professionnelle Suisse, qui a montré son enthousiasme à collaborer dès le départ. Après un examen poussé, les militaires ayant réussi le stage de formation pourront demander le titre de spécialiste en cybersécurité avec brevet fédéral à partir de l'automne 2019. Outre le brevet fédéral qu'il propose, le stage de formation offre aux participants de grands avantages pour leur carrière professionnelle grâce à une collaboration étroite avec l'économie privée et les établissements de formation. En effet, la matière est enseignée par des spécialistes chevronnés. L'armée a pu engager des formateurs expérimentés pour renforcer l'instruction en cybersécurité. La possibilité de faire reconnaître le stage de formation dans le cadre des études au moyen de crédits ECTS fait actuellement l'objet de clarifications.

Avantages de la milice

Grâce à notre système de milice, l'armée peut compter sur des recrues bien formées. Contrairement à ce qui a cours au sein des armées professionnelles étrangères, le stage de formation en cybersécurité ne commence pas par le b.a.-ba de l'informatique. Grâce au savoir acquis par les participants lors de leur apprentissage, de leurs études gymnasiales ou universitaires, ou en autodidacte, il est possible de partir d'une bonne base et, dans le cadre de 40 semaines intensives, de développer, d'approfondir et d'appliquer leurs connaissances avant de les adapter aux besoins militaires. Comme le relève le chef de la BAC, le divisionnaire Thomas Süssli, « *En Suisse, nous avons la chance extraordinaire de pouvoir commencer le stage de formation avec des jeunes gens déjà très bien formés* ».

Outre le stage de formation, l'armée dispose d'une autre solution pour alimenter aussi rapidement que possible la cybercompagnie. Les cyberspecialistes astreints au service militaire qui ont achevé leur formation professionnelle peuvent aussi se faire réaffecter à la cybercompagnie après l'instruction militaire de base

Les militaires sont incorporés dans trois fonctions différentes selon leurs points forts et leurs connaissances.

Spécialiste CNO

Spécialiste des computer network operations (CNO) avec des tâches relevant notamment du développement d'outils logiciels, ainsi que de l'analyse d'événements cyber, des vulnérabilités et des cyberattaques.

Spécialiste milCERT

Spécialiste du military computer emergency response team (milCERT) avec des tâches relevant notamment de l'analyse au sein d'un security operation center (SOC), comme par exemple l'analyse des menaces cybersécurité au niveau des systèmes informatiques et de communication de l'armée, de la gestion des incidents cyber, des investigations techniques et de l'informatique légale (analyse forensique).

Spécialiste CYD

Spécialiste de la cyberdéfense (CYD) avec des tâches de renseignement relevant notamment de l'analyse et de la présentation de la situation afin de se défendre contre des cyberattaques et d'apporter un support (technique et forensique), de conseiller et de former les troupes actives dans le terrain.

ou un perfectionnement. Une fois le stage de formation achevé, il est également possible d'embrasser une carrière militaire en bifurquant sur la voie d'officier de carrière : toutes les portes sont ouvertes aux participants. Les besoins en matière de relève exigent qu'au moins un sergent par stage de formation réussisse la sélection (additionnelle) et qu'il reçoive la proposition d'avancement pour l'école d'officiers de la Formation d'application de l'aide au commandement.

Pour une Suisse sûre

La milice soutient les organisations professionnelles dans le domaine de l'autoprotection des systèmes d'information et des réseaux informatiques militaires, assure la capacité à durer de son personnel et complète les capacités techniques. Avec la nouvelle instruction en cybersécurité et ses spécialistes très bien formés, l'Armée suisse renforce le domaine de la cybersécurité pour que la Suisse reste sûre en toute situation et dans tous les secteurs d'opération. Son mot d'ordre, « Combattre, protéger, aider » s'applique en effet aussi au cyberspace.