Zeitschrift: Revue Militaire Suisse
Band: - (2022)
Heft: [2]: Numéro Thématique 2

Artikel: Le projet de commandement Cyber : du mandat de projet au commandement opérationnel
Autor: Vuitel, Alain / Castelberg, Lorena
DOI: https://doi.org/10.5169/seals-1035406

© VBS/DDPS – Sina Guntern

Cyber

Le projet de commandement Cyber – Du mandat de projet au commandement opérationnel

Divisionnaire Alain Vuitel; Lorena Castelberg
Chef de projet et cheffe communication du projet commandement Cyber

«L'armée se trouve dans un champ de tensions multidimensionnel. Elle doit en effet non seulement remplir ses missions actuelles, mais aussi, pour rester dans la course, anticiper à temps les menaces et les défis futurs ainsi que les évolutions toujours plus rapides dans le cyberespace et l'espace électromagnétique (CYBEEM). Cela implique des processus d'adaptation rapide.» Conception Générale Cyber, p.9.

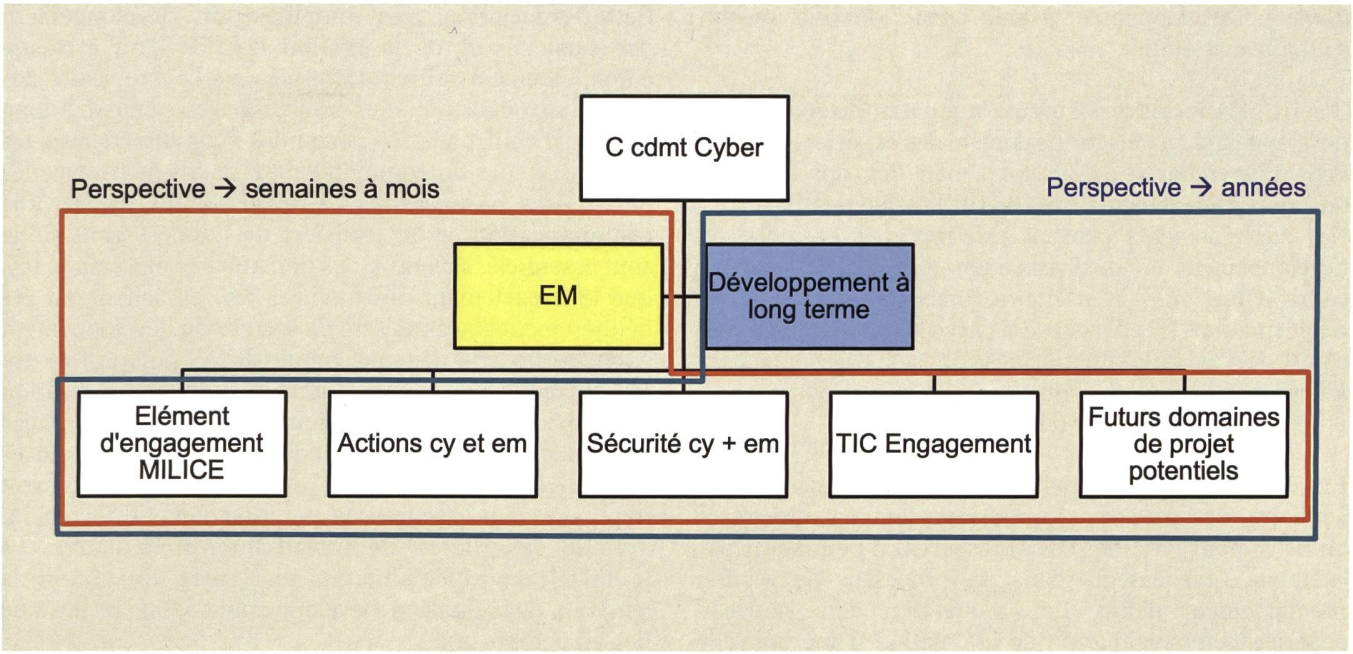
Cet extrait introductif de la Conception Générale Cyber (CG Cyber) décrit de manière exemplaire les défis auxquels l'Armée suisse est confrontée aujourd'hui dans le CYBEEM. En tant qu'un des trois rapports de base que l'armée a publiés ces dernières années, la CG Cyber montre quelle direction les capacités militaires doivent suivre dans les années 2020 et dans les années 2030 ainsi que quels investissements sont nécessaires à cet effet. En même temps, la CG Cyber, dont le Conseil fédéral a pris connaissance au printemps de cette année, est le premier produit publiquement visible issu du projet commandement Cyber actuellement en cours. Le présent article a pour but de présenter plus en détail ce projet, ses objectifs et ses défis. Sous la forme d'un rapport d'atelier, le contexte et les intentions qui ont conduit à l'initialisation du projet sont d'abord mis en lumière, avant que les différentes parties du projet ne soient brièvement présentées. Des perspectives clôtureront le rapport.

Les débuts sont toujours difficiles – «Cyber» au début du millénaire

Un bref regard en arrière sur la genèse du projet montre que le chemin menant à la création d'un commandement militaire autonome au sein de l'Armée suisse s'est déroulé en plusieurs étapes, suivant un processus de maturation. Etant donné que la sécurité ne jouait pas un rôle primordial lors de la création d'Internet, les menaces et les dangers potentiels dans et depuis le cyberespace ont augmenté de manière significative à partir des années 90, parallèlement à la digitalisation croissante de tous les aspects sociétaux et à la commercialisation d'Internet qui en a découlé. En raison de l'augmentation continue de la dépendance, ces risques n'ont plus seulement concerné des acteurs économiques ou des personnes privées, mais ont eu de plus en plus le potentiel de mettre en danger la sécurité et la prospérité de tout un pays. Au début des années 2000, le discours sur les cyberrisques potentiels a donc pris une dimension supplémentaire, celle de la politique de sécurité. Ainsi, le rapport sur la politique de sécurité 2000 (RAPOLSEC 2000) contenait déjà les premières indications sur les menaces potentielles dans les domaines du cyberespace. Ces indications n'ont par la suite pas débouché sur des mesures effectives de protection contre ces menaces. Tout comme l'est le développement des ordinateurs quantiques aujourd'hui, le thème du cyber était à l'époque encore trop peu tangible pour une grande partie de la population et de la politique.

Le cyber fait partie de l'agenda politique

Avec l'augmentation constante des cyberattaques, tant sur les appareils privés que sur les entreprises et les institutions publiques, la conscience de l'importance de la sécurité dans le cyberespace n'a cessé de croître. En 2010, le thème a donc été à nouveau abordé de manière éminente dans le cadre du rapport du Conseil fédéral lors de l'Assemblée fédérale sur la politique de sécurité de la Suisse. Les «attaques contre l'infrastructure informatique» ont été considérées comme importantes pour la politique de sécurité. Le thème du cyber a définitivement fait son entrée dans l'agenda politique. Cela s'est notamment traduit par l'élaboration de divers concepts et stratégies au niveau politique, comme la *stratégie nationale de protection contre les cyberrisques* ou le *Plan d'action Cyberdéfense du DDPS*. La création de cybercommandements autonomes en Allemagne ou en France, par exemple, a rapidement fait naître en Suisse la revendication d'un cybercommandement propre au sein de l'Armée suisse (motion 17.3507, Un commandement de cyberdéfense avec des troupes cyber pour l'armée suisse).



La structure schématisée du commandement Cyber au 01.01.2024.

Cette demande a finalement trouvé une expression concrète en 2022 dans le cadre de la révision de la loi sur l'armée et de la révision de l'organisation de l'armée en 2023. Afin de pouvoir mieux répondre aux défis actuels, des mesures préparatoires déjà entamées au cours des années précédentes ont ainsi enfin reçu une direction juridique définie. Ceci ayant pour objectif de remplacer la Base d'aide au commandement (BAC) de l'armée par un commandement opérationnel Cyber d'ici 2024.

Le projet se présente

Depuis lors, le projet de commandement Cyber s'est beaucoup développé. Outre la CG Cyber mentionnée précédemment dans l'article, le projet s'est surtout concentré au début, dérivé des besoins évalués en termes de compétences, sur le développement d'une structure adaptée aux défis futurs pour le commandement. L'illustration 1 présente le résultat de ces réflexions. Dans les paragraphes suivants, les différents sous-projets de cette nouvelle structure schématisée se présentent plus en détail et montrent la multitude de défis auxquels le projet est actuellement confronté, mais aussi ce qui a déjà pu être réalisé.

Les subordonnés directs du chef du commandement Cyber

Le domaine du développement à long terme

Afin de permettre au commandement Cyber de gérer ses ressources à la fois sur une perspective à court terme (état-major) mais aussi à long terme (développement à long terme), il dispose de deux éléments d'état-major différents. La division développement à long terme se concentre sur l'orientation à moyen et long terme du commandement. Il s'agit notamment d'observer les tendances à long terme ainsi que l'avancement technologique, la conduite du développement des capacités, la gestion des ressources, y compris la gestion de la fréquence, et d'autres domaines transversaux regroupés.

La vision du développement à long terme: «Nous façonnons l'avenir du commandement Cyber» décrit l'ambition de ce service d'état-major. Pour mettre en œuvre cette vision avec succès, les horizons de réflexion à court et à long terme doivent être harmonisés. Cette coordination se fait en plusieurs étapes. Tout d'abord, il s'agit d'identifier les tendances à un stade précoce en suivant en permanence le discours scientifique et social ainsi que les progrès technologiques. Ensuite, ces connaissances sont évaluées quant à leur aptitude à être utilisées par l'Armée suisse et testées dans la pratique à l'aide d'applications servant d'exemple. Si l'examen est concluant, les tendances peuvent finalement être intégrées dans la planification et la gestion des capacités.

Cette planification des capacités et la conduite constituent donc l'élément central du domaine du développement à long terme. Elle doit être assurée dans l'ensemble du commandement Cyber par un cycle de commandement militaire clairement défini. Le centre de suivi de la situation du domaine du développement à long terme est au centre de ce cycle. Ce centre a pour mission de comparer en permanence les capacités actuelles du commandement Cyber avec les capacités visées à l'avenir et d'identifier les éventuelles mesures à prendre.

Pour mener à bien cette tâche complexe, il a besoin de la contribution de tous les secteurs du commandement.

D'une part, sur la base d'une représentation de l'objectif prédéfinie, un horaire approximatif est établi pour déterminer comment et quand le commandement Cyber doit acquérir certaines capacités (Roadmap). A partir de ces informations, le centre de suivi de la situation de la

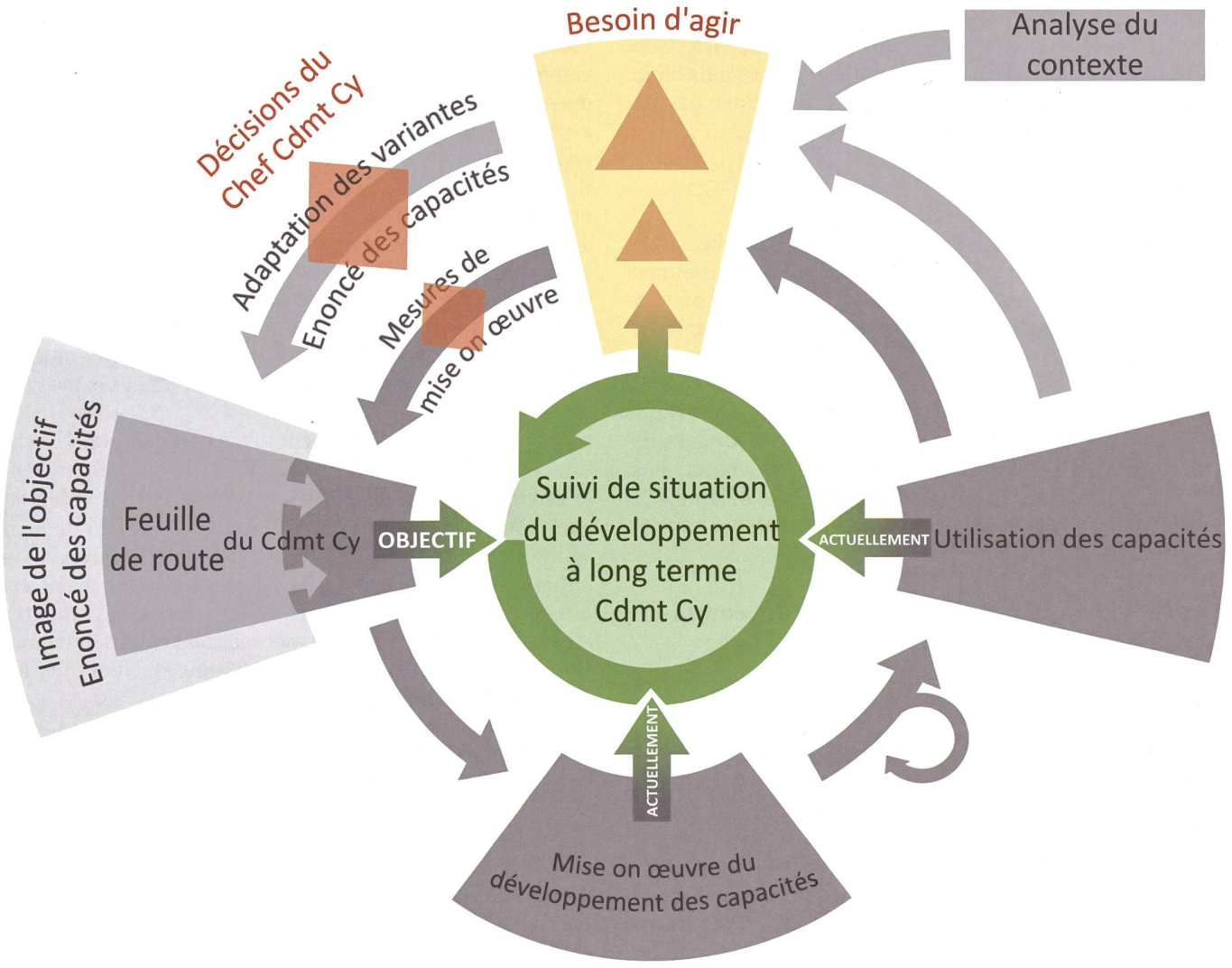
division Développement à long terme identifie un état souhaité à atteindre.

D'autre part, le centre de suivi de la situation du domaine du développement à long terme dépend des expériences tirées de la mise en œuvre du développement des capacités ainsi que des enseignements tirés de l'utilisation des capacités. Ces enseignements peuvent provenir, par exemple, du développement ou de l'utilisation d'un logiciel dans le cadre d'une mission militaire, mais aussi d'un retour d'informations (Feedback) de la part d'utilisateurs civils. Le centre de suivi de la situation de la division Développement à long terme rassemble ensuite ces informations pour en faire une vue d'ensemble de l'état actuel.

En cas d'écarts potentiels entre l'état actuel et l'état souhaité, des mesures appropriées sont ensuite mises en place pour éliminer ces différences. Il peut s'agir par exemple d'ajustements dans un processus de gestion préalablement défini, de l'acquisition d'un nouveau support technologique ou de la création d'une nouvelle capacité.

Cette description très simplifiée du développement des capacités et de la gestion à l'aide d'un cycle de commandement militaire illustre déjà la complexité des tâches auxquelles le sous-projet Développement à long terme est confronté. En raison des liens directs avec les autres secteurs du commandement, mais aussi avec les partenaires à l'intérieur et à l'extérieur de l'armée, une communication et un transfert de données sans faille sont essentiels. En outre, des domaines transversaux tels que le département des finances ou des achats ont été délibérément placés au sein du secteur du développement à long terme afin de tenir compte de la « perspective des ressources » dans tous les domaines de la planification des capacités et de la gestion. Le développement des compétences ne se fait pas indépendamment des autres domaines. Au contraire, ces derniers sont directement impliqués dans le processus et mis en œuvre directement à l'aide de groupes de travail interdisciplinaires. Le premier rapport de situation du Centre de suivi de la situation de la division Développement à long terme a eu lieu en octobre 2022.

Le suivi de la situation Développement à long terme schématisé.



L'état-major

Les collaborateurs du sous-projet Etat-major s'occupent actuellement du développement de produits pour la conduite du commandement Cyber, de la définition des processus correspondants et l'évaluation des structures en vue de la formation d'un état-major organisé de manière militaire. Il s'agit notamment de développer les capacités de suivi permanent et global de la situation ainsi que la conduite intégrale de l'engagement. De plus, l'état-major est responsable des affaires en cours d'année dans l'instruction et dans des domaines transversaux définis. Le mandat de projet prévoit que l'état-major ait la capacité d'autonomie, de durabilité et d'action au 01.01.2024, ainsi qu'il soit intégré dans les structures et les processus de l'armée, tout en étant opérationnel.

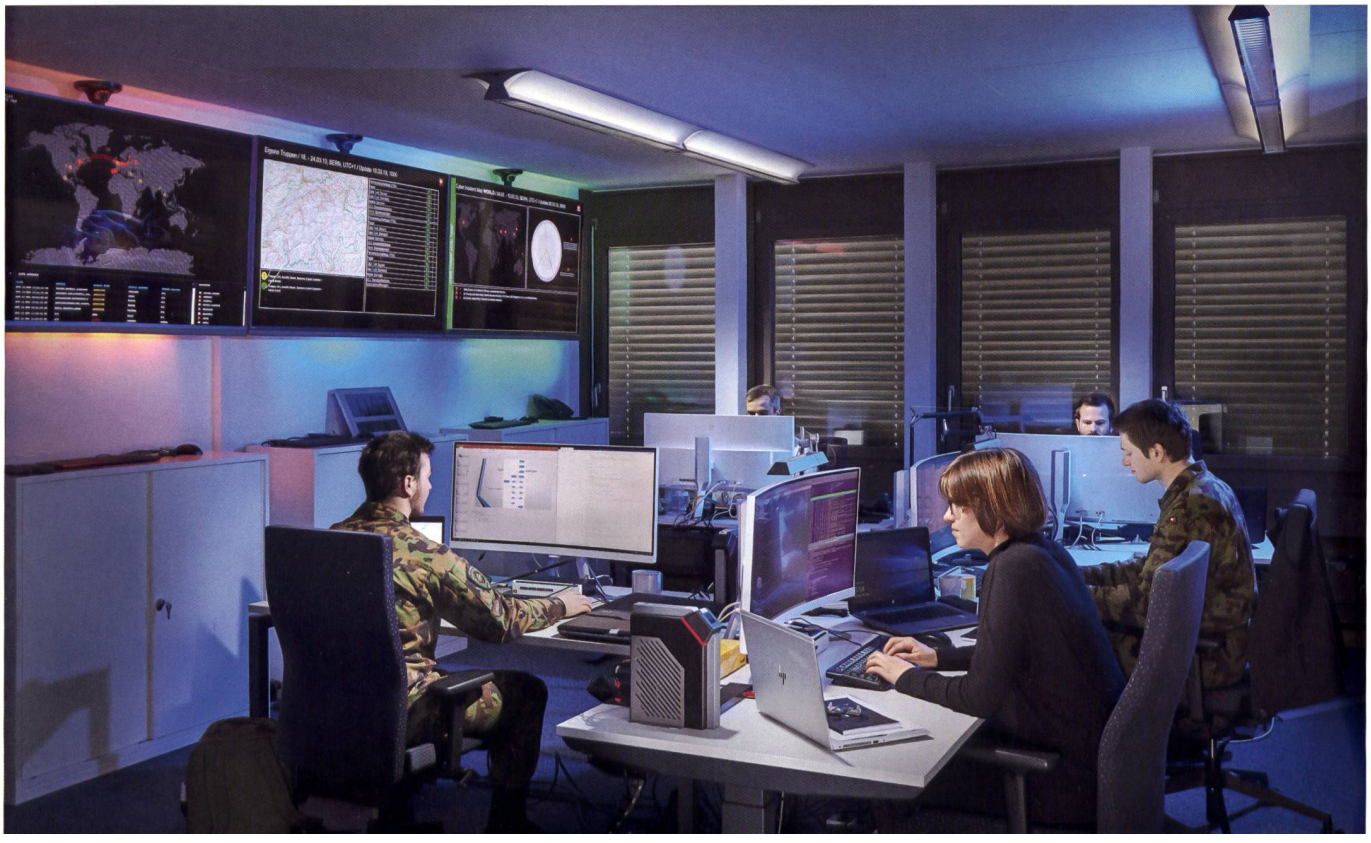
Afin de tenir compte en particulier des processus de conduite de l'armée et des structures, l'état-major du commandement Cyber est structuré selon les domaines de base de conduite conformément au règlement Conduite et organisation des états-majors de l'armée 17 (COEM 17). L'organisation se concentre sur les domaines de renseignement militaire, des opérations/planifications, de la logistique/appui au commandement et de l'instruction. Le futur centre de suivi de la situation du commandement Cyber sera rattaché au domaine des opérations/planifications. Les nouvelles structures doivent permettre de planifier et de conduire simultanément trois actions et d'établir ainsi l'image intégrale de la situation dans le cyberespace et l'espace électromagnétique ainsi que dans le domaine des technologies de l'information et de la télécommunication, 24 heures sur 24 et 365 jours par an. La collaboration coordonnée et bien rodée avec les départements du commandement Cyber est ici une clé essentielle du succès. En particulier pour l'établissement de l'image consolidée de la situation CYBEEM/TIC, l'état-major du commandement Cyber dépend de la collaboration fluide avec les autres domaines du projet. Un flux de données et d'informations largement automatisé est donc indispensable. L'état-major a également pour mission d'établir les points de contact nécessaires avec le commandement des opérations ainsi qu'avec d'autres partenaires et bénéficiaires de prestations, afin d'ancrer le commandement Cyber dans le cadre général de l'armée.

Outre l'organisation professionnelle, l'état-major de milice de la Base d'aide au commandement (BAC) sera réorganisé et deviendra l'état-major de milice du commandement Cyber. Jusqu'à présent, l'état-major de milice de la BAC se concentrait principalement sur le travail de projet comme sur le travail conceptuel. A l'avenir, les capacités de l'état-major de milice seront axées sur la planification et la conduite d'actions en collaboration avec la composante professionnelle de l'état-major de commandement Cyber, afin de renforcer ce dernier et d'assurer sa capacité à endurer. Il s'agit également de développer les compétences en matière de planification et de réalisation d'exercices d'état-major et de formation transversaux.

L'élément d'engagement de milice

Dans le mandat de projet pour le commandement Cyber, l'élément d'engagement de milice est décrit comme suit: *« L'élément d'engagement milice est centralisé et comprend toutes les formations de milice du commandement Cyber. Ce domaine assure la conduite militaire des formations de milice. La conduite technique de l'engagement des formations de milice incombe aux domaines spécialisés ».*

Aperçu du Security Operations Center.
Source: VBS/DDPS – Jonas Kambli



Lors du lancement du commandement Cyber, l'élément d'engagement comprendra, en plus des formations de milice, l'état-major central de la br aide cdmt 41/SIS ainsi que le Commandement Aide Cdmt SIS. Dans le cadre des adaptations aux formes modernes de collaboration dans le domaine des TIC, il a été décidé de transférer des parties du Analog zu oben SIS dans le domaine de l'engagement TIC (ce domaine est décrit plus loin). Il s'agit ainsi de garantir que l'utilisateur de systèmes puisse interagir directement avec les développeurs dès les premières phases du projet.

Lors de l'introduction du projet, les formations de milice de l'élément d'engagement de milice comprendront toutes les formations de milice de la br aide cdmt 41/SIS. Le passage au commandement Cyber doit permettre d'améliorer encore la coordination entre la conduite militaire et la conduite technique grâce à une étroite collaboration avec les différents domaines spécialisés. Ainsi, les avantages de la conduite militaire peuvent être utilisés en combinaison avec le savoir-faire des divisions spécialisées, ce qui augmente leur efficacité.

En collaboration avec le domaine Développement à long terme, on évalue actuellement les capacités et les prestations qu'une milice CYBEEM devra avoir. Par exemple, la création d'une formation de milice axée sur l'analyse des données permettrait de rendre accessible à l'armée le précieux savoir des spécialistes de ce domaine dans l'économie privée et la science. Sur la base de ces réflexions, les étapes de développement de ces prestations doivent être présentées dans un concept en comparaison avec les révisions périodiques de l'organisation de l'armée (Rév OA). Pour cela, ce concept indiquera également quelles étapes sont nécessaires à la réussite de son implémentation dans l'armée.

Aujourd'hui déjà, les formations de milice fournissent un travail précieux dans l'environnement technologiquement complexe du CYBEEM. Toutefois, à l'avenir, ces atouts seront exploités encore plus efficacement. Mais, les premiers changements découlant de ce concept concerneront la milice au plus tôt lors de la Rév OA 2026.

Dans cette étape, on examinera quelles formations doivent fournir au mieux leurs prestations dans le cadre du commandement Cyber et, le cas échéant, quelles formations peuvent éventuellement être engagées dans une autre unité organisationnelle au profit de l'ensemble du système de l'armée, afin de fournir leurs prestations de manière encore plus optimale.

Dans cette étape, l'état-major de milice de la br aide cdmt 41/SIS sera harmonisé et développé avec les structures de l'état-major de milice du commandement Cyber. En outre, de nouvelles capacités seront éventuellement intégrées dans le domaine de la milice et les formations correspondantes seront mises sur pied ou adaptées. Des prestations de la milice en faveur des centres de calcul de l'armée ou le développement des capacités d'analyse des données déjà mentionnées, sont par exemple possibles. Pour ce faire, le savoir-faire déjà existant de la milice doit être regroupé dans une structure correspondante.

Le domaine du cyber et de la sécurité électromagnétique

Le 1er avril 2022, la division Cybersécurité de la Base d'aide au commandement (BAC) a été transférée au projet de commandement Cyber, posant ainsi la première pierre de la mise en place de l'autoprotection CYBEEM au sein du commandement Cyber et pour l'Armée suisse. La sécurité TIC et Cyber de tous les systèmes de l'armée sont au cœur des travaux actuels et futurs. Une nouvelle tâche consistera à définir et à mettre en place des prestations concrètes dans le domaine de la sécurité électromagnétique.

Avant le transfert, la division était déjà responsable de la sécurité de l'infrastructure TIC existante ainsi que de la sécurité de la Nouvelle Plateforme de Digitalisation NPD en cours de développement (voir le domaine de l'engagement des TIC). La stratégie de sécurité ainsi que la gouvernance de la sécurité, qui relie le niveau de maturité visé aux priorités commerciales et aux aspects de la mise en œuvre concrète, ont été finalisées en octobre 2022.

La cybersécurité et la sécurité électromagnétique se composent aujourd'hui de deux sections, la Cyberprotection et le Centre de Fusion Cyber.

Le rôle central de la section Cyberprotection est de gérer et de vérifier la sécurité de l'information, des TIC et de la cybersécurité. Pour atteindre une sécurité intégrale, le respect des directives des sous-secteurs est toujours vérifié. Ces secteurs sont la sécurité des personnes, la protection des biens et la sécurité des locaux/de l'environnement/des collaborateurs. Une attention particulière est accordée aux activités des cyberarchitectes. Ceux-ci ont pour mission importante de conseiller et d'accompagner les projets en vue de la concrétisation des prescriptions de sécurité et de leur mise en œuvre. Ils coordonnent également l'intégration des nouveaux processus de sécurité en étroite collaboration avec le service Engagement TIC.

La section Cyber Fusion Center est responsable de l'établissement de l'image de la situation cyber et de la surveillance de la sécurité des systèmes de l'armée sur l'ensemble du territoire. Elle se compose de différentes équipes spécialisées. L'équipe Cyber Operations Center a notamment pour mission d'analyser les cybermenaces et les conséquences des points faibles sur nos infrastructures TIC. Différentes représentations de la situation sont déduites et sont rassemblées au sein de l'état-major du commandement Cyber pour former une image intégrale de la situation. Le Security Operations Center SOC est responsable de la détection précoce et de la défense contre les cyberattaques. Les analyses approfondies en cas de cyberincident ainsi que la conservation des traces sont assurées par l'équipe « milCERT ». Enfin, l'équipe Infrastructure et Développement s'occupe de manière ciblée du développement de nos capteurs et d'une plateforme d'analyse/d'évaluation.

Le changement d'organisation depuis avril 2022 exige, dans l'approche duale (BAC et commandement Cyber), beaucoup de flexibilité et d'engagement de la part des

collaborateurs, mais offre également de nouvelles opportunités à la division. Dans le processus de transformation, davantage de responsabilités seront à l'avenir déléguées aux différents collaborateurs, une forte réflexion orientée vers la résolution de problèmes sera établie et la méthode de travail sera axée sur des équipes interdisciplinaires. Afin de créer une culture commune, nos valeurs ont été définies dans le cadre de différents ateliers et un cockpit culturel a été créé.

Le domaine Cyber et actions électromagnétiques

Le sous-projet Cyber et actions électromagnétiques se focalise sur le développement du Centre des opérations électroniques (COE) jusqu'à la fin des années 2020. A partir de ces travaux, il s'agit également de coordonner et d'harmoniser de manière optimale la future fourniture de prestations dans l'espace cyber et électromagnétique de l'armée avec tous les partenaires, par exemple avec les Forces aériennes.

Les tâches principales du COE comprennent en principe :
- Acquisition d'informations au moyen de l'exploration radio et par câble ainsi que des cyber-actions pour le Service de renseignement de la Confédération.
- Acquisition d'informations au moyen de l'exploration radio pour le service de renseignement militaire.
- Assurer le service spécialisé de cryptologie de la Confédération.
- Assurer des actions dans le cyberespace et l'espace électromagnétique au profit des opérations de l'armée.
- Acquisition d'informations provenant de sources accessibles au public au profit des deux services de renseignement et d'autres services autorisés.

Les tâches mentionnées sont aujourd'hui et seront à l'avenir accomplies sur la base de la loi sur le renseignement et de la loi sur l'armée.

Les travaux actuels se concentrent sur la question de savoir comment ces tâches pourront être accomplies à l'avenir. En résumé, les moteurs du renouvellement sont les suivants : l'évolution de l'environnement militaire et des services de renseignement, le développement technologique, la forte augmentation du volume de données à traiter et les attentes des spécialistes actuels et futurs envers un employeur moderne.

Le COE et l'organisation qui lui succède acquièrent des informations du monde entier. Pour conserver cette capacité, les développements technologiques doivent pouvoir être suivis rapidement. Si ce n'est pas le cas, les sources d'information s'épuisent ou les systèmes de brouillage radio deviennent inefficaces. Ces renouvellements nécessaires doivent pour se faire être effectués en permanence et dans des « conditions d'exploitation ». Il s'agit donc aussi, dans ce sous-projet, d'étudier de manière approfondie les développements technologiques. Ces travaux sont également réalisés avec le soutien d'armasuisse, Science et Technologies en étroite collaboration avec le secteur Développement à long terme.

Sans la capacité d'obtenir des informations à partir de la très grande quantité de données, il n'est déjà plus possible aujourd'hui d'obtenir des résultats utiles en matière de reconnaissance. C'est pourquoi ce sous-projet cherche actuellement la manière de mettre en œuvre le changement vers une organisation centrée sur les données. Des questions telles que « Qu'est-ce qu'une organisation centrée sur les données concrètement ? » ou « Comment mettre en place une telle organisation ? » font actuellement l'objet de discussions intensives presque quotidiennes au sein du sous-projet.

Enfin, les aspects culturels d'une telle réorganisation en profondeur sont également d'une grande importance. Il s'avère que le chemin vers une organisation centrée sur les données sera avant tout un chemin de changement culturel. La question de la culture d'entreprise est également liée à la question de savoir quelle culture et quelles formes de travail un employeur moderne doit vivre, respectivement permettre. Travailler de manière flexible avec un degré élevé de digitalisation, permettre des modes de travail agiles, y compris à distance (Home Office), ainsi que la diversité au sein du personnel ne sont que quelques-uns des thèmes qui doivent être abordés. Des exigences de confidentialité élevées pour les tâches décrites précédemment augmentent encore les défis pour le sous-projet.

Le domaine de l'engagement des TIC

Le sous-projet Engagement TIC est responsable de la « Nouvelle Plateforme de Digitalisation (NPD) » de l'armée. Par NPD, on entend la plateforme TIC distribuée, robuste, hautement sécurisée et résiliente, sur laquelle l'armée met à disposition des applications critiques pour l'engagement. Outre les composants types de la plateforme (puissance de calcul, mémoire, etc.), elle comprend d'autres éléments tels que les terminaux, les éléments de sécurité, les services de collaboration, les services d'intégration pour l'échange intégral de données, mais aussi la mise en place de l'organisation d'exploitation, y compris les structures et processus nécessaires. A l'avenir, la plateforme devra par exemple héberger des services de transmission de données et d'informations tels que le projet « Télécommunications de l'armée » ou le réseau de commandement. Après la mise en place initiale de la NPD, celle-ci sera développée en permanence avec une forte implication des utilisateurs.

Ce n'est pas la seule raison pour laquelle l'unité TIC travaille selon des principes agiles. Avec une organisation basée sur « SAFe » *(Scaled Agile Framework)*, les utilisateurs, les collaborateurs et la création de valeur générée en cycles courts sont au centre des préoccupations. La transparence, la capacité d'apprentissage et l'attractivité du poste de travail s'en trouvent considérablement améliorées. Selon la devise *« you built it, you run it »*, la qualité des prestations TIC est maintenue à un niveau élevé dans le cadre d'une culture DevSecOps *(Development, Security, Operations)*.

La NPD permettra à l'avenir l'exploitation largement standardisée et automatisée de prestations clés TIC

telles que la puissance de calcul, le stockage de données, l'authentification, mais aussi l'exploitation de services transversaux tels que les géodonnées militaires. Ces services peuvent ensuite être utilisés par les applications utilisatrices qui s'y appuient. Jusqu'à présent, différentes plateformes ont été acquises pour différents cas d'utilisation. Cela a conduit à la création de « solution-silo » de plus en plus séparées les unes des autres. Avec la réalisation de la NPD, l'acquisition et l'exploitation de plates-formes TIC propres à chaque système doivent appartenir au passé. Il s'agit donc d'une capacité centrale du fournisseur de prestations TIC militaires: La NPD permet de réaliser un réseau technique efficace qui fournit à l'utilisateur les applications et les données qui soutiennent ses tâches critiques pour l'engagement et qui garantissent finalement l'avance de l'armée en matière de connaissances et de décisions.

Défis pour le commandement Cyber

Le projet commandement Cyber met les bouchées doubles pour faire avancer les travaux présentés ci-dessus. Le passage du statut de projet à celui de commandement opérationnel pose plusieurs défis.

Le passage d'un projet à une organisation opérationnelle constitue l'un des plus grands défis. Les structures prévues doivent faire leurs preuves dans la réalité, les procédures doivent se consolider et les différents collaborateurs doivent apprendre à connaître les interlocuteurs et procédures dans leur travail quotidien. Cela ne peut pas fonctionner sans l'établissement d'une compréhension commune de la performance et d'une culture commune. Dans le cadre du projet commandement Cyber, ce processus est donc étroitement accompagné par des ateliers culturels dans les différents départements.

Le positionnement du commandement Cyber au sein du système global de l'armée constitue un autre défi. En tant que nouveau commandement avec de nouvelles capacités et de nouveaux processus, il peut y avoir des chevauchements de compétences ou des changements dans les responsabilités et les dépendances pendant la mise en place ou la phase d'introduction. C'est pourquoi, pendant la mise en place du commandement Cyber, les différents subordonnés directs du chef de l'armée ont toujours été étroitement impliqués dans le processus.

Le dernier défi à relever est l'environnement dans lequel le commandement Cyber opère. En tant que commandement devant être performant dans un environnement très technologique, il est essentiel de suivre le rythme du progrès continu. Pour ce faire, il a besoin d'un personnel hautement qualifié. Malheureusement, le projet n'échappe pas à la pénurie de personnel qualifié qui touche l'ensemble du secteur. C'est pourquoi, en collaboration avec différents établissements d'enseignement et partenaires du secteur privé, elle a déjà commencé, au cours des dernières années, à créer des possibilités de formation pour les jeunes intéressés par le cyber. Grâce à des initiatives telles que le stage cyber ou la formation cyber avant le service, des spécialistes importants devraient être recrutés pour l'engagement dans l'armée.

Les défis décrits ne sont bien sûr que quelques-uns des nombreux autres. Mais la réussite de tous ces défis passe par une sensibilisation permanente à la cybersécurité dans l'utilisation quotidienne des appareils informatiques et des systèmes d'armes en réseau. Chacun d'entre nous peut ainsi contribuer au succès du commandement Cyber et à la sécurité de la Suisse. En effet, une armée qui ne dispose pas d'un réseau sécurisé et d'une protection résiliente de ses propres systèmes ne sera plus suffisamment performante à l'avenir pour faire face à des situations de crise potentielles. La mise en place réussie du commandement Cyber est donc d'une importance capitale pour l'armée et pour la Suisse.

A. V.; L. C.

Les cyberrisques sont un sujet de préoccupation pour chaque soldat – même sur le terrain.
Source: VBS/DDPS – Clemens Laub.