RMS +

Revue Militaire Suisse

BRIGADE D'AIDE AU COMMANDEMENT 41

COMMANDEMENT ET BATAILLON CYBER

GUERRE ELECTRONIQUE

QUARTIERS GENERAUX

Numéro Thématique – Br aide cdmt 41

www.revuemilitairesuisse.ch

Un « nœud » d'ondes dirigées permet aux Grandes Unités (brigades, divisions) d'être reliées de manière directe, rapide et sure avec leurs subordonnés directs. Photo © Br aide cdmt 41.

Histoire des troupes de transmission

Un dossier consacré à l'histoire des troupes de transmission et d'aide au commandement au sein de l'armée suisse a été intégré à RMS No. 6/2022. Nous tenons à remercier le col EMG Hanspeter Steiner, président de la CI trm, pour son travail de rédaction. Les textes ont été traduits par la br aide cdmt 41.

Impressum

Rédacteur en chef :
Col EMG Alexandre Vautravers — a.vautravers@yahoo.com

Rédacteurs adjoints :
Lt-col EMG Julien Grand — Of spéc Lena Ebener
Cap Alain Mermoud — Of spéc Olivier Reymond

Membres du comité :

Président	Div Mathias Tüscher	mathias.tuescher@revuemilitairesuisse.ch
Vice-président	Col Christian Rey	info@reygroup.ch
Administrateur	M. Hubert Varrin	administration@revuemilitairesuisse.ch
SMG	Col EMG Denis Mastrogiacomo	d.mastrogiacomo@smg-ge.ch
SSO	Col Gianni Bernasconi	Gianni.bernasconi@bluewin.ch
SVO	Col EMG Christophe Gerber	christophe.gerber@elca.ch
SNO	Maj Sébastien Marti	president@ofne.ch
SOVR	Lt col Roger Haupt	roger.haupt76@bluewin.ch
SFO	Maj EMG Patrick Noger	patrick.noger@sfo-fog.ch
SJO	Lt col EMG Edouard Vifian	edouard.vifian@vtg.admin.ch
SCBO	Col Francesco M. Rappa	francesco@rappa.ch

Administration, abonnements et publicité :
Association de la Revue militaire suisse (ARMS)
Avenue Général-Guisan 117, 1009 Pully
Tél. +41 21 729 46 44
e-mail : info@revuemilitairesuisse.ch
Compte postal: ARMS, 1009 Pully, PostFinance CH84 0900 0000 1000 5209 7

Mise en pages et impression : PCL Presses Centrales SA, chemin du Chêne 14, 1020 Renens

ISSN 0035-368X

Div Mathias Tüscher, Président de l'ARMS

© VBS/DDPS – Sina Guntern

Editorial

L'Armée suisse dans le cyberespace et l'espace électromagnétique – Une longueur d'avance

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

L'Armée suisse s'est toujours trouvée dans un contexte de tensions multidimensionnelles. De tout temps, il a fallu assumer les tâches actuelles tout en anticipant les menaces et défis à venir dans le contexte d'un environnement en constante évolution. Cette réalité est plus que jamais un défi, en particulier lorsqu'il s'agit d'opérer dans le cyberespace et l'espace électromagnétique (CYBEEM). Ces deux domaines, dont la convergence ne cesse d'augmenter, connaissent une accélération sans précédent de leur développement. Dans ce contexte, l'année 2022 prend pour nous un caractère particulier et ceci pour trois raisons.

Premièrement, la guerre en Ukraine nous a révélé que le choix délibéré d'une confrontation armée demeure encore aujourd'hui en Europe, et qu'il s'agit encore d'un moyen pour faire prévaloir ses intérêts et établir de nouvelles frontières. Ce faisant, cette tragique réalité confirme que la mission de défense de notre armée continue d'occuper une place indispensable dans notre édifice sécuritaire. Les premiers constats tirés de cette guerre mettent en évidence le fait, qu'au-delà de la qualité des systèmes d'armes, de la volonté et de l'état de préparation des troupes, c'est bien la mise en réseau par des opérateurs de senseurs par l'intermédiaire des organes de conduite qui fait la différence au combat. Disposer d'un avantage en matière de connaissance de la situation confère, à celui qui l'établit, une supériorité décisionnelle lui permettant de concentrer les forces adéquates et/ou le feu de ses armes à l'endroit et au moment idoine pour remporter la décision. Si l'établissement d'une telle supériorité en matière de connaissance de la situation et de décision influe directement sur la vie ou la mort au combat, elle décide finalement du maintien de l'indépendance ou de la défaite d'une nation. Sa création, son élargissement progressif et son maintien à travers le temps dépendent de l'existence d'une colonne vertébrale numérique s'étendant à travers le CYBEEM.

L'importance de cette épine dorsale à l'échelon de la nation comme première ligne de défense constitue le deuxième élément à prendre en compte. Là aussi, l'exemple de l'Ukraine nous a démontré que, bien avant le début des combats au sol, sur mer et dans les airs, le maintien de l'indépendance d'un pays dépend largement de sa capacité à protéger son infrastructure numérique face à un nombre croissant d'attaques dans le cyberespace et à conserver l'accès aux réseaux internationaux de transferts de données. Les efforts du gouvernement ukrainien en la matière, débutés après l'annexion de la Crimée avec l'appui de puissances occidentales et du secteur privé, lui ont permis, malgré des cyberattaques massives à répétition, de conserver la liberté de manœuvre dans le CYBEEM pour transmettre, tant à sa propre population qu'au reste du monde, un message fort d'unité et de volonté de défense face à l'agresseur. Ce même schéma a été observé cette même année à Taïwan où des acteurs étatiques et non étatiques ont également mené des campagnes de désinformation et de propagande, ont perturbé les organes gouvernementaux civils et ont lancé des attaques au moyen de logiciels malveillants. Contrairement aux actions conventionnelles, les attaques menées dans le CYBEEM sont souvent difficiles à retracer pour pouvoir les attribuer avec certitude à un Etat ou un acteur particulier. Ces incertitudes, combinées avec la facilité d'opérer en faisant fi des distances qui séparent les parties-prenantes et avec une grande fulgurance dans le CYBEEM, brouillent toujours plus la frontière entre la guerre et la paix. Cette évolution marque l'avènement d'un environnement stratégique caractérisé par l'existence d'une rivalité constante, dont le degré d'intensité ne cesse de varier.

En mars 2022, la décision du Parlement suisse de créer un commandement de cyberdéfense et la prise de connaissance par le Conseil fédéral un mois plus tard de la *roadmap* de cyberdéfense constituent le troisième

élément marquant pour l'orientation future de notre armée. Ces décisions créent le fondement nécessaire pour faire du CYBEEM un élément incontournable de notre sécurité. En tant que première ligne de défense constamment à l'engagement, il appartiendra au futur commandement de la Cyberdéfense, non seulement d'assurer la sécurité de notre infrastructure informatique opérationnelle, mais aussi de tirer avantages de la numérisation pour conférer à nos commandants un avantage en matière de compréhension de la situation et de décision, tout en conservant notre liberté d'action dans l'utilisation du CYBEEM. conception générale cyber décrit les développements à effectuer d'ici les années 2030 pour permettre à notre armée d'atteindre cet objectif. Elle traite non seulement des aspects purement militaires, mais elle aborde aussi le thème de la coopération entre des partenaires dans le cadre du réseau national de sécurité et des tiers.

Une telle évolution ne va pas sans transformations de structures actuelles. En effet, la Base d'aide au commandement (BAC) disparaîtra suite à la création du nouveau commandement Cyber. Les compétences et savoir-faire spécifiques en matière d'exploitation et de développement des systèmes militaires opérationnels y seront transférés, respectivement réunis. Celles relatives aux plateformes informatiques de l'administration seront rattachées, dans le cadre du programme de dissociation de l'informatique du groupe défense, au reste de l'administration fédérale.

La réalisation des objectifs donnés au futur commandement Cyber est impensable sans l'existence d'un élément d'engagement intégrant nos formations de milice. Dans ce contexte, le savoir-faire de tous les éléments constituant la brigade d'aide au commandement 41/SIS est essentiel.

Ce numéro de RMS vise à en exposer les aptitudes spécifiques. Celles-ci, au-delà de leurs seules prestations à l'engagement, profitent à notre armée à plus d'un titre. Nos formations de milice lui garantissent d'une part un accès direct aux dernières connaissances techniques en la matière. En effet, elles sont principalement composées de militaires qui disposent d'une expérience professionnelle, souvent à haut niveau, en matière de CYBEEM. Elles assurent par ailleurs un lien irremplaçable entre entre le secteur privé et public tout en offrant une plateforme d'échanges unique à l'intérieur de cette branche et dans les différentes disciplines. Cette configuration gagnant-gagnant est, dans le CYBEEM, plus que jamais essentielle pour armer notre première ligne de défense et garantir ainsi, indépendamment de la situation, notre capacité d'action.

A. V. ; L. C.

© VBS/DDPS – Jonas Kambli

Aide au commandement

Lettre d'introduction du commandant de la br aide cdmt 41/SIS

Brigadier Thomas A. Frey
Cdt br aide cdmt 41/SKS

Chers membres de la br aide cdmt 41/SIS
Chères lectrices et chers lecteurs

Les fêtes de fin d'année ont commencé et l'année actuelle touche progressivement à sa fin – un moment idéal pour passer brièvement en revue les mois intensifs qui viennent de s'écouler. La présente édition annuelle de la célèbre revue spécialisée *Revue militaire suisse*, consacrée à la brigade d'aide au commandement 41/SIS, contient également une rétrospective détaillée de l'année. Je suis extrêmement heureux de pouvoir présenter à un large public la brigade spécialiste des technologies de l'information et de la communication de l'armée suisse. La brigade d'aide au commandement exploite notamment l'infrastructure de communication et de conduite ainsi que la guerre électronique au profit de l'armée. Elle est directement subordonnée à la Base d'aide au commandement (BAC) qui, de son côté, fournit des prestations dans le domaine des technologies de l'information et de la communication (TIC) pour le DDPS. En tant que bras militaire de la Base d'aide au commandement (BAC), la brigade d'aide au commandement est active dans le cadre d'exercices et d'engagements variés, 365 jours par an, dans toute la Suisse. De nombreux événements majeurs de renom ne seraient pas envisageables sans les prestations de notre brigade. Grâce aux connaissances et aux compétences approfondies d'environ 11'400 cadres de milice et soldats astreints au service d'instruction – répartis en 13 corps de troupe et 57 unités et compagnies – la brigade d'aide au commandement suit le rythme effréné du développement technologique et apporte ainsi une contribution essentielle à la sécurité en Suisse – ce qui constitue un énorme avantage pour le système de milice de l'Armée suisse. Un grand merci donc aux membres de milice de la brigade d'aide au commandement 41/SIS, qui agissent toujours fidèlement à leur devoir. En collaboration avec les cadres professionnels, ils ont réussi à fournir des services afin que les bénéficiaires de prestations soient tous extrêmement satisfaits de notre travail – Chapeau !

Le lecteur attentif se pose certainement la question de savoir ce que signifie concrètement le terme « aide au commandement ». En principe, l'aide au commandement comprend toutes les activités et infrastructures qui garantissent la capacité de conduite de l'armée et de la gestion nationale des crises.

En font partie l'exploitation d'installations de conduite, les infrastructures de télécommunication, les datacenters, les applications informatiques civiles et militaires ainsi que la cyberdéfense. D'autres domaines spécialisés sont par exemple la guerre électronique, les services de spécialistes linguistiques et la cryptologie.

La brigade d'aide au commandement 41/SIS dispose des trois domaines de compétences clés suivants :

1. L'utilisation des technologies de l'information et de la communication (TIC) permet le traitement rapide et la distribution sûre d'informations vocales, de données et d'images.
2. La guerre électronique (GE) sert à détecter, à évaluer ainsi qu'à perturber les émissions électromagnétiques étrangères au sein de leur télécommunication sans fil.
3. les quartiers généraux (QG) et les installations de conduite protégées sont exploités de manière à ce que le gouvernement fédéral, le commandement de l'armée et les états-majors des Grandes Unités puissent commander et coordonner les forces et les organisations nécessaires en cas de catastrophe, mais aussi de crise, de conflit ou de sécurisation de grandes manifestations.

En complément des formations de milice, le commandement aide cdmt SIS et ses quelque 38 collaborateurs militaires et civils fournissent un portefeuille de prestations aux multiples facettes. Ils assurent la représentation des troupes dans différents projets d'armement de l'aide au commandement, évaluent les nouveaux systèmes télématiques et informatiques et élaborent les concepts d'instruction. Ils forment le personnel enseignant sur les systèmes à introduire et organisent des cours de service spécialisé. En outre, ils rédigent les règlements techniques spécialisés et mettent à disposition les moyens d'instruction. Le soutien du commandement aide cdmt SIS va de la création de supports de données et de l'exploitation de systèmes de planification à la collaboration avec la compagnie d'intervention aide cdmt 104/204 lors d'engagements subsidiaires. Cette compagnie d'intervention est par exemple intervenue en 2017 lors de l'éboulement de Bondo et a remis en service le système d'alerte au Piz Cengalo, ce qui a ensuite permis d'effectuer les travaux de déblaiement et de sauvetage.

L'objectif premier de la brigade d'aide au commandement 41/SIS est, comme mentionné au début, de mener à bien une multitude d'engagements et d'exercices en formation les plus divers au service de la population et de la sécurité de notre pays, et de les soutenir grâce au savoir-faire approfondi des cadres de milice et professionnels. Si l'on passe en revue l'année écoulée, nous tirons, avec nos bénéficiaires de prestations, un bilan positif. La brigade d'aide au commandement a permis l'organisation de divers événements majeurs, dont le forum économique mondial annuel WEF à Davos, la compétition internationale de ski-alpinisme militaire « Patrouille des Glaciers » en Suisse romande, le sommet de crise entre le président américain Joe Biden et le président russe Vladimir Poutine à Genève, la « Ukraine Recovery Conference » à Lugano ou le congrès sioniste à Bâle. En outre, la brigade d'aide au commandement a été mise à l'épreuve lors de nombreux exercices de formations de Grandes Unités. Ainsi, des prestations ont été fournies en faveur de l'exercice de formation PILUM lors duquel l'armée a pu vérifier avec succès la disponibilité de base de ses troupes au sol à l'échelle 1:1 avec environ 5'000 militaires impliqués. En outre, la brigade d'aide au commandement a rendu possible l'exercice en formation ODESCALCHI, qui a mis l'accent sur la collaboration entre les armées suisse et italienne. Il s'agissait de s'entraîner à l'aide mutuelle en cas de catastrophe naturelle ou d'origine humaine nécessitant une intervention commune. La brigade d'aide au commandement était également présente lors de l'exercice de formation RHODANUS, qui compte parmi les plus grands exercices de la brigade mécanisée 1 avec 2'400 militaires et cinq bataillons impliqués. D'autres bénéficiaires de prestations de la brigade d'aide au commandement 41/SIS ont été, entre autres, le commandement des opérations, le service de renseignement militaire, les Forces terrestres, différentes divisions territoriales, les Forces aériennes suisses, le commandement des forces spéciales, le commandement de l'instruction ainsi que le centre de compétences SWISSINT.

Dans l'optique de vous fournir un bref aperçu de l'année 2023, il convient de mentionner la manifestation publique CONNECTED, qui offre des aperçus passionnants dans les domaines de la cyberdéfense ainsi que de la numérisation de l'armée et de ses partenaires. Du 16 au 20 août 2023, des démonstrations et des présentations seront effectuée sur la place d'armes de Kloten-Bülach et donneront une vue exclusive sur l'éventail des prestations de l'Armée suisse. En outre, il sera par exemple possible de passer la nuit en bivouac, d'admirer des robots et des technologies à venir, de déguster la fameuse croûte au fromage militaire - et bien sûr de vivre de nombreux autres moments forts et passionnants. L'hôte de cet évènement nommé CONNECTED est le divisionnaire Alain Vuitel, qui dirige actuellement le projet « Commandement Cyber » de l'armée en tant que chef de projet. Il est responsable de l'initialisation du projet et de la mise en place progressive du commandement Cyber de l'armée.

Les récents changements de personnel et d'organisation au sein de l'état-major central de la brigade d'aide au commandement 41/SIS comprennent entre autres l'arrivée du lt col Christian Petrocchi (chef du domaine spécialisé de l'aide au commandement), dont le poste était occupé depuis le 1er janvier 2017 par le lt-col EMG Roger Rauper. La raison de ce changement est que le lt-col EMG Roger Rauper a été nommé, comme prévu, chef d'état-major et remplaçant du commandant de la brigade d'aide au commandement 41/SIS. Je remercie chaleureusement le col EMG Thomas Wick, ancien chef d'état-major et remplaçant du commandant, pour son engagement de longue date en faveur de la br aide cdmt 41/SIS et lui souhaite beaucoup de plaisir et de succès dans sa nouvelle fonction de remplaçant du commandant / chef de la gestion des engagements et des carrières au Centre d'instruction de l'armée (CIAL) du commandement de l'instruction.

En ce qui concerne l'articulation de la brigade, il y a également un «nouveau venu» à enregistrer. Ainsi, la prise de commandement du bataillon cyber 42 a eu lieu en mars 2022 dans la cour d'honneur du château de Colombier. Le commandement de ce corps de troupe nouvellement créé, qui regroupe les capacités de l'armée dans le domaine cyber, a été remis au lieutenant-colonel EMG Davide Francesco

Serrago. Les militaires de milice accomplissent leur service dans les trois domaines spécialisés que sont la cyberdéfense, la cyberdéfense militaire et la cryptologie. L'engagement s'effectue tout au long de l'année avec des détachements composés de spécialistes de ces trois domaines. Le cyber bataillon 42 soutient la fourniture de prestations de l'organisation professionnelle de la Base d'aide au commandement BAC dans toutes les situations.

Pour conclure, il convient de mentionner ici que la transformation de la Base d'aide au commandement (BAC) en commandement Cyber au 01.01.2024 bat actuellement son plein. Jusqu'à la fin de cette transformation, la BAC restera un office fédéral autonome et une unité organisationnelle directement subordonnée au chef de l'armée. En mars 2021, le Conseil fédéral a nommé M. Thomas Fankhauser chef de la BAC par intérim pour cette période. La direction du projet de commandement Cyber a été confiée au divisionnaire Alain Vuitel. L'armée suisse doit aujourd'hui et à l'avenir être en mesure de protéger ses systèmes informatiques contre les cyberattaques. L'armée doit également pouvoir déployer des effets dans les sphères d'opération de l'espace électromagnétique et du cyberespace. Des partenariats stratégiques doivent créer la liberté d'action nécessaire pour que le commandement cyber puisse se concentrer sur les missions principales de l'armée.

En fin de compte, il s'agit de faire en sorte que l'armée dispose de l'avance nécessaire en matière de connaissances et de décisions dans le cadre du réseau de capteurs, de renseignements, d'effets et de conduite, quelle que soit la situation.

Compte tenu des turbulences actuelles dans le monde et de l'invasion de l'Ukraine par la Russie depuis le 24 février 2022, il est indéniable que les cyberattaques et les campagnes de désinformation joueront un rôle central à l'avenir également – l'avantage revient à ceux qui s'y préparent et s'y préparent suffisamment tôt.

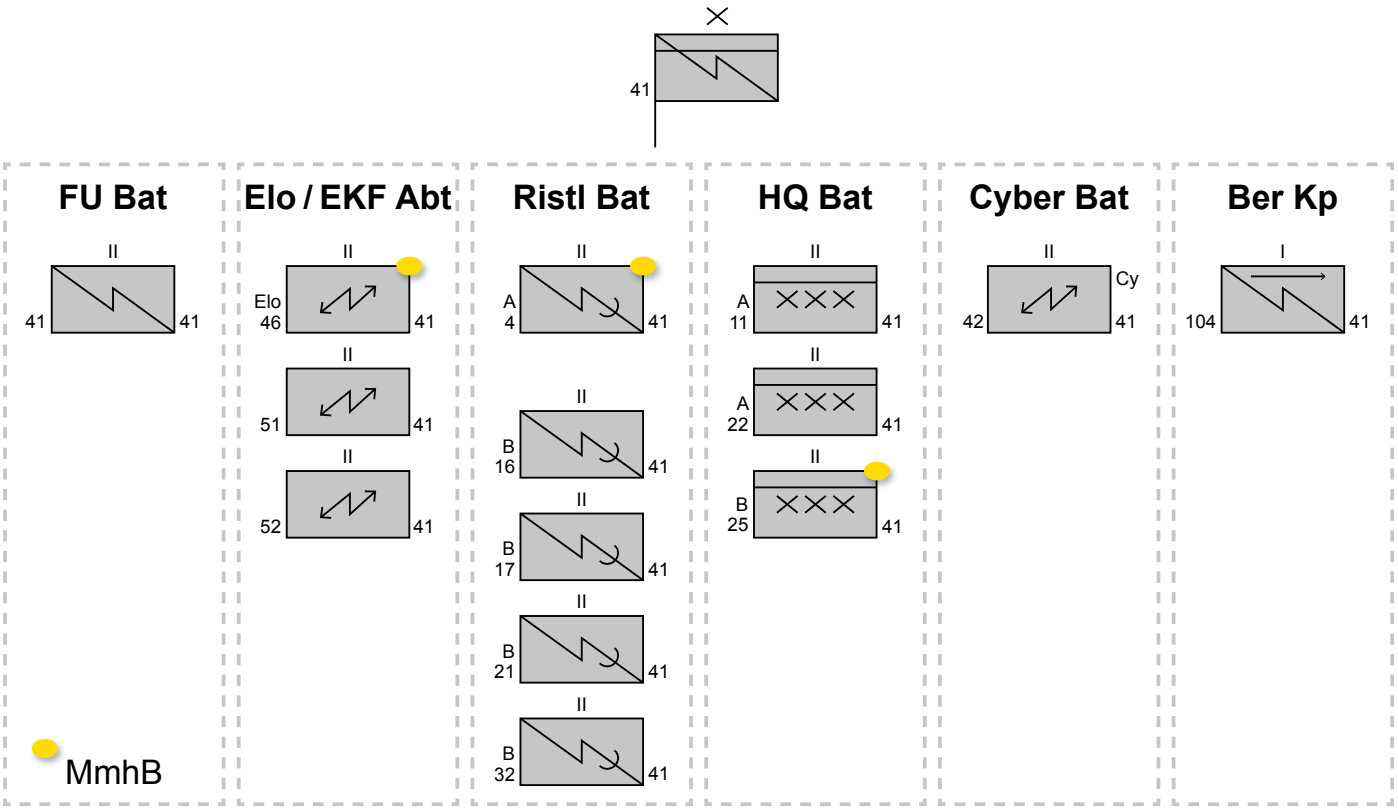
T. F.

CURRICULUM VITAE

Brigadier Thomas A. Frey
Cdt br aide cdmt 41/SIS

Le brigadier Frey dirige la brigade d'aide au commandement 41/SIS depuis le 1er janvier 2020. Il est responsable de la formation et du perfectionnement des états-majors et des troupes et est subordonné au chef de la base d'aide au commandement. Après avoir obtenu sa maturité, il a étudié les sciences du sport et du mouvement à l'EPF de Zurich, où il a obtenu un diplôme de maître de gymnastique et de sport EPF ainsi qu'un diplôme fédéral d'enseignement supérieur. De 1994 à 1996, il a travaillé comme professeur de gymnastique et de sport à l'école cantonale de Zurich-Oerlikon. En 1997, il est entré dans le corps des instructeurs et a été affecté aux écoles d'infanterie de Zurich, puis au commandement de l'instruction en formation à Coire. De 2004 à 2005, il a suivi le cours de carrière de capitaine d'infanterie à l'US Army Infantry School à Fort Benning/Georgia (USA). En 2005, il a été affecté comme officier d'état-major adjoint du commandant du Centre d'instruction de l'infanterie ou du Centre d'instruction des Forces terrestres à Walenstadt, avant d'exercer la fonction de chef des essais des Forces terrestres de 2006 à 2009 au même endroit. Du 1er septembre 2009 au 30 octobre 2012, il a été engagé comme remplaçant du commandant au sein du commandement d'infanterie en service long 14 à Aarau et simultanément comme commandant de la place d'armes de Zurich-Reppischtal, avant de diriger lui-même le commandement et la place d'armes d'Aarau du 1er novembre 2012 au 31 décembre 2015. Du 1er janvier 2016 au 31 décembre 2017, il a été engagé pour la Formation supérieure des cadres de l'armée (FSCA) de l'Académie militaire de l'EPF de Zurich en tant que commandant de la filière bachelor à Birmensdorf. Du 1er janvier 2018 jusqu'à sa promotion au grade de brigadier, il a occupé le poste de chef des directives et du pilotage de l'instruction/chef d'état-major suppléant au commandement de l'instruction à Berne. En tant qu'officier de milice, il a commandé le bataillon d'infanterie de montagne 35 et a été chef d'état-major dans la division territoriale 4.

Le 1er avril 2023, le brigadier Frey prendra le commandement de la Formation d'application de l'aide au commandement.



La saison hivernale et les conditions alpines s'accomodent très bien des installations d'ondes dirigées. Photo © Bat ondi 4.

© VBS/DDPS – Corinne Glanzmann

Cyber

Pour nos camarades sur terre, dans les airs avec le cyberespace

Lt-col EMG Davide Francesco Serrago
Cdt bat cyber 42

Le bataillon cyber 42, lui, a pour but de répondre à trois autres grandes problématique au niveau de l'armée; la cyberdéfense, le suivi de la situation militaire ainsi que la cryptologie. Ces compétences servent à la fois aux autorités civiles et aux milieux entrepreneuriaux. Pourquoi ? Voici la réponse :

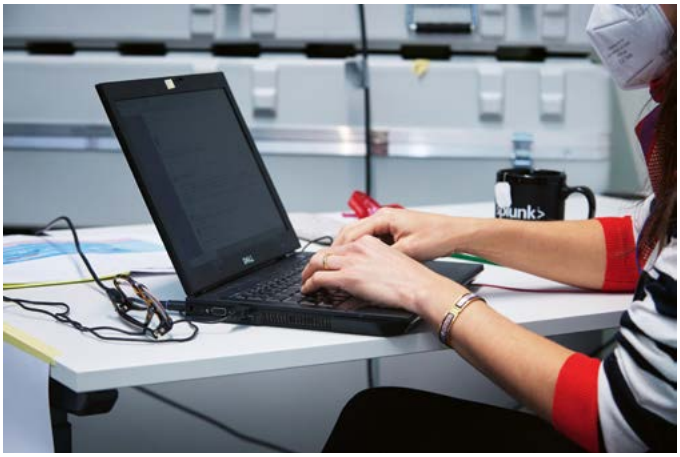
La militarisation de l'espace cybernétique, couplée à l'augmentation drastique de l'importance de ce domaine pour l'économie et pour la société dans son ensemble ont fait de la question de la cybersécurité la première priorité de la défense. Lors des dernières années, il est devenu très facile d'effectuer des attaques peu coûteuses avec des effets disproportionnellement élevés. Cette situation, exacerbée par la facilité avec laquelle il est possible de brouiller les pistes pour empêcher toute éventuelle trace pouvant mener à son ou ses responsables a été une prise de conscience de la nécessité de défendre nos intérêts sur ce plan. C'est pour cela qu'au 1er janvier 2022, un nouveau bataillon a vu le jour au sein de la brigade d'aide au commandement 41/SIS. Il s'agit du bataillon 42, dont la tâche principale est d'assurer la cyberdéfense de l'Armée suisse.

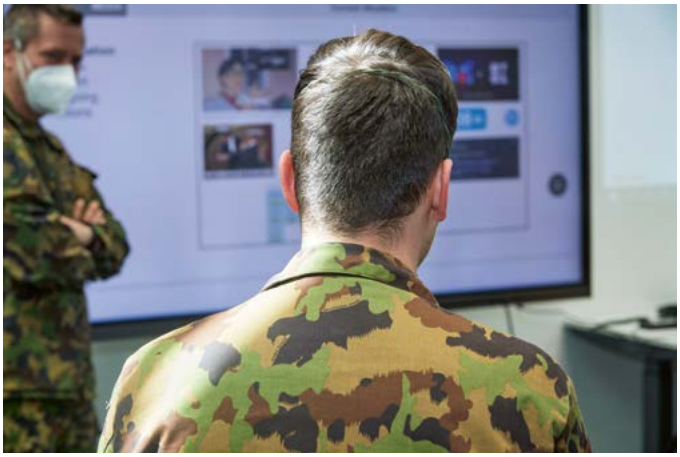
LIFE – UNIVERSE – EVERYTHING

Le numérotage d'unités militaires est souvent lié à une forme ou une autre de tradition. Ceci est également le cas pour le bataillon cyber 42. Le nombre 42 était, jusqu'en 2019, un des rares à ne pas encore avoir été résolu quand considéré en tant que constante dans une somme de trois cubes telle que $42 = x^3 + y^3 + z^3$. La résolution de cette équation (qui a nécessité 1.3 millions d'heures de calculs combinés) en 2019 coïncide avec le début de la planification pour la création du bataillon. Par ailleurs, dans le classique de science-fiction de Douglas Adams, *Le Guide du voyageur galactique*, livre fort apprécié dans le monde de la cybernétique, le chiffre 42 est la réponse à « *la grande question sur la vie, l'univers et le reste* ».

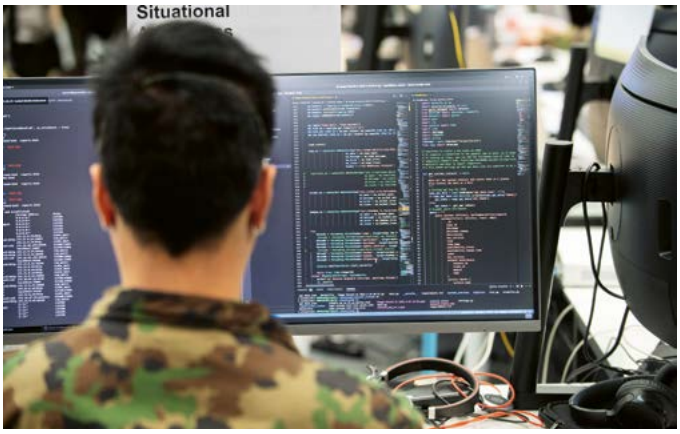
Le bataillon cyber 42 a pour but de répondre à trois grandes attentes au niveau de l'armée : la cyberdéfense, le suivi de la situation militaire ainsi que la cryptologie. Il est divisé en trois compagnies qui reprennent chacune une de ces fins, ainsi que d'une compagnie d'état-major. Les spécialistes qui y sont incorporés effectuent leur

Ci-dessous : Impressions de l'exercice cyber international LOCKED SHIELDS qui s'est déroulé en 2022.





Ci-dessous: Impressions de l'exercice cyber international LOCKED SHIELDS qui s'est déroulé en 2022.



Ci-dessous et page 12: Le commandant de Corps Thomas Süessli à la première prise de l'Etendard du bataillon cyber 42, dans la cour du château de Colombier NE.

service par détachements en se relayant durant toute l'année, fournissant ainsi un service de base constant dans ces trois domaines.

Les militaires du bat 42 se trouvent constamment en situation d'engagement réel et non dans un contexte d'entraînement. Leur engagement s'étend, sur demande, également en faveur d'autorités civiles.

Le bataillon coopère étroitement avec ses partenaires de la base d'aide au commandement (BAC) afin d'assurer la sécurité des systèmes informatiques de l'armée à tout moment. Les militaires en service sont choisis en coordination avec les besoins des différentes branches du centre des opérations électroniques de la base d'aide au commandement dans un souci de conformité, avec pour but un soutien efficace et utile à celles-ci.

Le rôle du bataillon est aussi de fournir un renfort substantiel à la base d'aide au commandement en cas de crise majeure, par exemple dans le cas d'une détérioration de la situation dans le cyberespace qui dépasserait sa propre capacité de réaction. Un engagement de ce type serait comparable au soutien de l'armée apporté aux hôpitaux durant la pandémie de COVID-19.

Les militaires du bataillon cyber 42 se trouvent constamment en situation réelle et non dans un contexte d'entraînement. C'est pourquoi ils agissent avec une diligence toute particulière. Le bataillon peut en outre apporter son soutien aux autorités civiles sur demande en temps de crise, auquel cas la mise à disposition de compétences et de moyens au travers de spécialistes des domaines requis est privilégiée. Dans le cas de tensions particulières ou même de conflit, le bataillon est apte à organiser la détection et la défense contre les cyber-attaques de manière autonome. Cependant, le catalogue complet des capacités du bataillon ainsi que des systèmes protégés par celui-ci n'est pas d'ordre public – ceci afin de garantir l'efficacité du dispositif de protection de l'armée suisse.

Protéger nos camarades sur terre et dans les airs est une question d'intégrité

Le développement des capacités du bataillon a lieu continuellement pour garantir la protection de nos camarades sur terre et dans les airs de toute menace provenant du domaine cybernétique. Le bataillon a pour ambition de s'améliorer et de gagner en flexibilité afin de fournir ses services de manière toujours plus efficace. De plus, son intégration dans le commandement cyber à l'horizon 2024 sera une des clefs de voûte permettant à la Suisse d'avoir une armée adaptée à son époque et garantissant la défense envers toutes les menaces contemporaines.

Le bataillon cyber 42 en est encore à ses débuts. Ses défis principaux à court terme sont étroitement liés à son jeune âge et sont voués à évoluer en fonction de ses expériences dans le contexte de la création du commandement cyber

à l'horizon 2024. Le recrutement est un de ses principaux défis, car le bataillon vise à atteindre le nombre de 600 membres. Il existe de nombreux candidats potentiels ; avec l'intégrité comme facteur de sélection décisif. En fin de compte, le bataillon cyber 42 représente moins d'un pour cent de l'effectif de l'armée. Des défis logistiques sont survenus lors des premières expériences, mais malgré ceux-ci, le bataillon a été en mesure de garantir un service constant et efficace.

Des améliorations sont planifiées au niveau de la disponibilité et de la capacité de fournir des services complémentaires si besoin, et ce de manière ponctuelle. Les ambitions et les épreuves futures liées à la logistique et à la planification ont d'ores et déjà été analysées et les mesures nécessaires à leur résolution ont été prises. Maintenant que le bataillon est en mesure de fournir un service de base constant et efficace, les prochains défis consistent donc à augmenter encore et toujours la quantité et la qualité des services que le bataillon peut rendre, en améliorant d'un côté la palette des moyens du bataillon ainsi que la disponibilité de ces derniers au travers de ses membres.

Le rythme est donné par les changements technologiques

La définition du rôle que le bataillon va jouer à l'échelle du futur commandement cyber ainsi que la manière dont il sera incorporé dans cette structure est aussi un défi auquel fait face le commandement du bataillon. Ces discussions, en partenariat avec la *Task Force* chargée de la mise en place du commandement cyber actuellement en cours auront vraisemblablement une grande influence sur le futur du bataillon.

Parmi les objectifs les plus importants auxquels fait face le bataillon, il y a également l'acquisition de talents et de compétences. Les spécialistes en cyber-sécurité font déjà défaut sur le marché civil, et leur nombre extrêmement limité rend leur recrutement particulièrement épineux. Cette problématique est commune à toutes les armées du monde, mais la Suisse possède l'avantage, et non des moindres, de fonctionner principalement comme armée de milice, créant ainsi des synergies entre la vie civile et militaire et ayant une plus-value personnelle et professionnelle qu'il serait difficile de proposer dans le cadre d'une armée professionnelle.

Un dessein de moindre mesure est la militarisation de la cyberdéfense. Les membres du bataillon ont une connaissance du domaine dont l'application n'a pas encore été théorisée au niveau de l'armée en Suisse. La plupart des connaissances et de la terminologie civile ne sont pas nécessairement facilement compréhensibles pour d'autres formations militaires avec lesquelles travaille et coopère le bataillon. Il est donc nécessaire de réfléchir à la manière dont l'armée va structurer le cadre par défaut des actions militaires dans le domaine cyber de façon à ce qu'elles puissent être comprises et coordonnées avec le reste de l'armée de manière standardisée et efficace.

L'environnement technologique dans lequel évolue cette formation est en constant changement, ce pourquoi les spécialistes qui y effectuent leur service sont triés sur le volet.

Deux voies d'accès au 42

Il existe actuellement deux voix de recrutement afin de devenir un spécialiste cyber et d'être affecté au bataillon cyber 42. La première est d'effectuer un cours prémilitaire dans le domaine cyber, puis d'effectuer la sélection cyber pendant l'école de recrues, auquel cas le militaire est affecté à une section cyber et effectue le cours cyber pendant l'école de recrues. L'autre manière d'être affecté au bataillon concerne les militaires en cours de répétition, et consiste à effectuer une sélection dont la réussite se solde par une mutation dans le bataillon cyber 42.

La première voie de recrutement intéresse beaucoup de jeunes en formation dans l'informatique, notamment des étudiant des EPF ayant un intérêt marqué pour la cybersécurité, et qui doivent effectuer leur école de recrues. Etre étudiant dans ce domaine n'est toutefois pas un critère essentiel, ainsi des membres du bataillon ont déjà été recrutés sur la base de connaissances acquises de manière autodidacte. Les critères de sélection sont bien sûr liés aux compétences et connaissances requises dans le domaine, mais pas uniquement : les compétences sociales ainsi que l'intégrité des candidats sont également des facteurs déterminants. Les militaires recrutés par cette voie effectuent leur Instruction de Base Générale (IBG) dans des écoles de recrues diverses et variées, amenant des connaissances de l'armée provenant de différentes armes. A la fin de l'instruction de base, ils sont mutés à l'école de guerre électronique où ils reçoivent une instruction dans le domaine de la cyberdéfense comprenant des cours donnés par des spécialistes ainsi que des stages sur le terrain parmi les mandants des services du bat ou des entreprises actives dans le domaine. Dès la fin de leur école de recrues, ils sont affectés au bataillon cyber 42 qui profite donc des compétences acquises par ces militaires pour mener à bien sa mission.

La seconde voie concerne les militaires affectés à d'autres Armes mais qui disposent d'une formation civile ou bien d'expérience professionnelle dans le domaine de la cyberdéfense, et qui désirent en faire profiter l'armée suisse. Ceux-ci effectuent une évaluation qui est effectuée par le bataillon cyber 42 ainsi que par ses mandants. A la suite de quoi ils sont réaffectés, si leur profil est jugé adéquat et utile, et ce avec le soutien de tous les commandants concernés ainsi que de l'administration militaire.

Il est vrai que ce type de profil est également très recherché dans le domaine civil, ce qui pourrait porter à croire que l'alimentation du bataillon serait en concurrence avec celui-ci. Cependant, s'agissant de miliciens, la pratique est toute autre : les militaires du bataillon profitent de leurs expériences militaires et améliorent ainsi leur profil au bénéfice de leur employeur. Au niveau de la formation notamment, une collaboration avec ICT Switzerland

permet de faire valoir l'expérience acquise lors du service afin d'obtenir un brevet fédéral de spécialiste en cybersécurité.

Reconnaissant pour le soutien de son canton parrain Neuchâtel

Grâce au soutien de son canton parrain Neuchâtel, le bataillon cyber 42 prévoit un exercice de formation cyber avec l'administration cantonale pour s'améliorer dans le domaine de la cyberdéfense et de profiter de l'échange entre des spécialistes en cybersécurité.

Le bataillon évalue régulièrement les compétences de ses membres pour ne conserver que ceux capables de mettre leurs compétences à jour continuellement. Le recrutement de militaires travaillant en permanence dans le domaine permet au bataillon de profiter de membres toujours à niveau dans un domaine qui change rapidement, créant ainsi des conditions favorables à la réussite de ses missions.

Le bataillon cyber 42 n'en est qu'à ses débuts, mais ses membres ont déjà permis d'améliorer sensiblement les capacités de l'armée suisse dans le domaine cyber. Dans le contexte actuel, il est fort à parier que le bataillon sera fortement mis à contribution dans l'architecture sécuritaire de notre patrie. Le bataillon cyber 42 est prêt à relever les défis qui lui sont présentés pour sauvegarder notre neutralité armée et ainsi contribuer à la paix et à la prospérité qui caractérisent notre si beau pays.

D. F. S.

Guerre électronique

Le groupe de guerre électronique 51 dans l'exercice RHODANUS

Lt-col Gaël Oberson
Cdt gr GE 51

Il y a un peu moins d'un an, la brigade mécanisée 1 a mis sur pied le fameux exercice RHODANUS. Un exercice auquel le groupe de guerre électronique 51 a pris part. Retour sur cet exercice de grande envergure.

Auparavant très secrète et exclusive, la guerre électronique fait couler ces derniers temps de plus en plus d'encre. Notamment dans le cadre du conflit armé entre la Russie et l'Ukraine, les capacités prétendument excellentes de la guerre électronique russe ont tenu de nombreux spécialistes du domaine bouche bée. Pourtant, les performances de ces systèmes n'ont pas apporté l'effet escompté. Si l'on en croit les comptes rendus, outre les problèmes d'approvisionnement et l'équipement insuffisant, la principale lacune dans le domaine de la guerre électronique russe relevait notamment des tactiques, techniques et procédures (TTP) mal maîtrisées.

L'efficacité et la précision de ces TTP étant un défi pour toute force armée, l'Armée Suisse tend à conduire toujours plus d'exercices impliquant différents corps d'armes et ainsi, à entraîner leur synergie. L'exercice RHODANUS en est un parfait exemple.

Habitué jusqu'ici à tester son système dans un cours de répétition individuel, le gr GE 51 a dû relever bien des défis pour répondre aux attentes de ses mandants dans le cadre de RHODANUS. Des défis allant de la logistique à la technique, bien évidemment.

Un engagement concret

Sur le plan technique, la mission est restée la même pour le groupe de guerre électronique 51. La partie senseur a été mise à contribution afin de détecter des émissions dans le spectre électromagnétique dans la région de l'exercice. A la disposition de la direction d'exercice de la brigade, le groupe était en charge, dans un premier temps, de pister et de repérer les bataillons en exercice sur le terrain. Les émissions radio peuvent transmettre un grand nombre d'informations dans la sphère électromagnétique que le groupe est capable d'intercepter, d'analyser afin d'en tirer des conclusions pour le bénéficiaire de prestation, respectivement dans le cas de RHODANUS, la direction d'exercice. Dans un second temps, les effecteurs du groupe se préparaient au brouillage des cibles potentielles avec les chars MZS (chars équipés d'émetteurs à usage multiple).

Voici ce que le groupe guerre électronique est capable de produire en termes de prestations. En parlant de prestations, justement, il s'agit là du premier cours de répétition lors duquel le gr GE 51 a engagé son système IFASS (système intégré d'exploitation et d'émission radio) de manière concrète pour une brigade mécanisée. Comme expliqué plus haut, le gr GE 51 devait travailler dans la sphère électromagnétique afin de repérer son « adversaire » puis, selon les ordres de la direction de l'exercice RHODANUS, brouiller les communications desdits « adversaires ». Dans un cours de répétition classique, le groupe effectue ses tâches avec une certaine liberté afin d'exercer techniquement leurs connaissances. Dans cette situation en revanche, les conditions se rapprochent de la réalité. Bien que l'adversaire était en réalité une autre formation de l'Armée Suisse, la situation dans la sphère électromagnétique tendait vers ce qui se passerait lors d'un conflit armé réel.

Même si les défis techniques sont connus, d'autres se sont ajoutés à la liste. Connaître, du mieux que possible, les caractéristiques de l'autre troupe contre laquelle le groupe était engagé était un réel défi à surmonter durant l'exercice. Mais c'est aussi en cela que servent ces exercices grandeurs nature. S'entraîner, oui, mais en développant aussi l'aspect collaboratif où chaque corps de troupe apprend à connaître les autres, leurs caractéristiques, leurs missions, etc. Chaque militaire s'exerce, comme chaque année, dans son corps de troupe, mais il apprend aussi, par cette collaboration interarmes, ce que font les autres militaires de l'armée.

Un défi logistique et technique de taille pour les sections

Si à l'échelle d'un bataillon les défis sont nombreux, à une échelle plus petite, les changements ont été plus conséquents et souvent plus difficiles à cause du cadre que l'exercice imposait. RHODANUS n'était pas uniquement un exercice mis en place en quelques jours. Ce dernier a nécessité l'organisation de deux dispositifs. Tout d'abord, une phase s'est déroulée dans le Chablais valaisan puis une seconde dans le nord du canton de Vaud. Qui dit deux dispositifs, dit un exercice plus long, deux emplacements à trouver mais aussi un défi important pour déplacer rapidement tous les composants techniques du groupe du premier au second dispositif.

Dans l'absolu, les défis logistiques étaient les mêmes pour les différents corps de troupe. Ils ont dû tout d'abord travailler au sein d'un dispositif A puis se déplacer en direction d'un dispositif B. Trouver un emplacement n'est déjà pas une chose simple, en trouver deux s'avère être une tâche compliquée. D'autant plus quand tant de corps de troupe sont engagés dans la même région et sont donc en concurrence. Les recherches ardues se sont donc mêlées à un brin de chance pour trouver un emplacement convenable tant pour la partie logistique que pour la partie technique.

Trouver la perle rare n'est pas donné à tout le monde. Certaines sections ont vu leur emplacement être séparé en deux avec une partie logistique pour le repos et les repas ainsi qu'un autre emplacement technique où les différentes antennes pouvaient être déployées. Dans ces cas particuliers, les deux emplacements pouvaient se trouver à plusieurs dizaines de minutes l'un de l'autre en voiture. Une difficulté supplémentaire toutefois surmontée, car le groupe, en tant qu'outil de la direction d'exercice, n'était pas soumis à une situation tactique et aux règles qui s'imposeraient dans une telle situation. En somme, le travail quotidien ne différait pas mais la nature de l'exercice a fait que les difficultés habituelles ont été fortement altérées. Un challenge relevé avec brio par le groupe de guerre électronique 51 !

Le gr GE 51 vu de l'extérieur

Pour coordonner un tel exercice, la nécessité d'une liaison entre les deux corps de troupe est absolue. Un rôle tenu, du côté de la brigade mécanisée 1, par le major d'Etat-Major Général Simon Bettschen qui faisait partie du groupe de l'état-major ayant préparé l'exercice RHODANUS. Le major Bettschen nous a accordé un peu de son temps pour discuter de l'exercice passé et de la collaboration entre les deux armes.

Un tel exercice demande une préparation en amont conséquente. *« Nous avons rencontré le lieutenant-colonel EMG Jones, commandant à ce moment-là, au printemps de 2021 pour qu'il nous présente les différentes prestations de la guerre électronique et voir ce qu'il était possible de faire »*. Cette première entrevue posait déjà les bases d'une collaboration importante. Se voir pour

Antenne goniométrique au début de l'exercice.

parler des prestations envisageables était une première raison évidente. Au-delà de simplement discuter des prestations, des attentes et de la manière de travailler, il fallait bien évidemment se voir pour discuter de la guerre électronique en elle-même afin que le mandant puisse avoir les connaissances nécessaires pour préparer son exercice. *« Je connais bien évidemment la guerre électronique pour l'avoir vu lors de l'Ecole EMG, mais je ne connaissais pas tous dans les détails. C'était un défi à relever ».*

Une nouveauté pour tout le monde

En partant de cette idée de base jusqu'à la réflexion, la conception et l'organisation de l'exercice, toutes les étapes relevaient d'une certaine nouveauté pour tous les militaires impliqués. *« Au début, nous avions effectivement beaucoup d'attentes »,* nous explique le major au téléphone, *« nous avons tous fait face à certaines difficultés lors de cet exercice ».*

Une fois le cours de répétition terminé, l'heure est toujours au bilan. D'habitude, ce bilan ne concerne qu'une seule troupe et le travail réalisé. Ici, il a fallu inclure une nouvelle variable, celle de la guerre électronique, une nouveauté certaine pour les deux corps de troupe. *« Le but principal de l'ancien commandant de la brigade était d'exercer sa troupe au brouillage ».* S'exercer au brouillage, mais dans quel but ? *« Souvent, il arrive que nous ayons des soucis de radio et la troupe ne sait pas si la nature de ce problème est le brouillage ou non. Cet exercice a permis de le démontrer en situation d'exercice et de gagner en expérience ».*

Un exercice d'une telle ampleur comporte bien évidemment son lot de complications comme nous l'expliquait le major EMG Bettschen lors de l'entretien *« Cela nous a pris du temps pour trouver des prestations adéquates à nos demandes. Nous avons beaucoup discuté pour savoir ce qui serait utile ou non. Au final, nous pouvons dire que nous sommes arrivés à un produit qui peut nous être très utile ! ».*

De précieux enseignements

Pour le gr GE 51, l'exercice RHODANUS s'est révélé être très constructif et cela malgré les différents défis rencontrés. Il a permis de travailler sur des activités dans le spectre électromagnétique qui n'étaient pas simulées. En effet, les communications captées provenaient d'une véritable formation de combat en pleine action. En plus de rendre la formation des analystes plus réaliste, cela a permis d'accumuler une expérience précieuse concernant les résultats fournis par le système IFASS face à une brigade mécanisée.

En outre, la collaboration avec un autre corps d'arme a également fourni de précieux enseignements. Pour le gr GE 51, il en est notamment ressorti que le rôle de son officier de liaison auprès du mandant est central. Sans pouvoir présenter les produits GE, les détailler et les argumenter auprès du commandant, les capacités du groupe ne peuvent être exploitées pleinement. Ce point, ainsi qu'entrainer la précision et l'efficacité des tactiques, techniques et procédures GE, seront certainement les principaux objectifs lors des prochains cours de répétition. Cela sera aussi le cas lors l'exercice PILUM, prévu en novembre 2022. Le gr GE 51 sera à nouveau de la partie et se réjouit d'ores et déjà des expériences qui pourront y être faites.

G. O.

Antenne à ondes dirigées

Char brouilleur « MZS » lors du paramétrage du système avant l'exercice.

Guerre électronique

La guerre électronique : Renseigner et combattre dans le spectre électromagnétique

Lt-col EMG Micha Grimm
Cdt gr GE 52

Qu'il s'agisse de drones, d'avions de combat ou de systèmes de conduite modernes, tous ne fonctionnent que tant que la communication est assurée, laquelle utilise aujourd'hui encore souvent les systèmes radio comme canal de transmission. La guerre électronique (GE) est un terme générique qui englobe les activités de reconnaissance des signaux (senseur) et de guerre électronique (effecteur) dans le spectre électromagnétique dans lequel ces ondes radio se propagent. La guerre électronique regroupe donc une large gamme de prestations allant de la reconnaissance d'informations importantes pour la conduite jusqu'à la destruction de réseaux radio adverses.

Histoire

La guerre russo-japonaise est considérée comme l'acte ayant donné naissance à la GE. En janvier 1904, le croiseur HMS Diana aurait intercepté un message annonçant la mobilisation de la flotte russe. La capacité des troupes japonaises à écouter les transmissions de la marine russe de haute mer constituait un avantage significatif et a probablement influencé l'issue de la guerre.

C'est seulement plus tard, lors de la bataille d'Angleterre de 1940-1941 que la nécessité militaire de disposer de compétences de renseignement dans le spectre électromagnétique s'est manifestée. Grâce aux systèmes RADAR de la Royal Air Force (RAF), les avions de combat allemands attaquants pouvaient être détectés à temps.

C'est également pendant la Seconde Guerre mondiale que la radiogoniométrie et la radiolocalisation ont été utilisées pour la première fois à des fins militaires afin de localiser les sous-marins allemands. Jusqu'en 1944, les radiogoniomètres ont joué un rôle important pour un tir de sous-marins sur quatre.

Bien qu'encore en phase expérimentale, le Global Positioning System (GPS) a été victime d'attaques de brouillage ciblées dès la guerre du Golfe de 1991. Les systèmes de ciblage des forces armées américaines étaient utilisés pour guider leurs missiles intelligents et pouvaient être influencés, malgré l'équipement irakien plutôt primitif, par leurs adversaires. Aujourd'hui encore, le GPS est vulnérable aux interférences.

Mission de base

Les produits de la GE peuvent être utilisés dans tous les domaines d'action de l'armée.

L'objectif du renseignement électronique (senseur) est d'obtenir des informations importantes pour la politique de sécurité et l'armée en captant et en évaluant les émissions électromagnétiques. Il s'agit essentiellement d'analyser les liaisons radio sans fil afin d'identifier les émetteurs, les réseaux et les regroupements, d'établir des images radio de la situation et, le cas échéant, d'anticiper les intentions des adversaires et parties-prenantes.

La guerre électronique (effecteur) consiste notamment à influencer activement le spectre électromagnétique au détriment de tiers ou au profit des propres troupes. Par exemple, une augmentation drastique de l'intensité du champ électromagnétique utilisé par l'ennemi, c'est-à-dire l'émission sur une même fréquence avec plus d'énergie électromagnétique, doit permettre de perturber durablement ou, idéalement, de rendre impossible la communication radio de l'adversaire.

Senseur

Si quelqu'un veut savoir de quelle direction vient le vent, il peut humidifier son index et le tendre en l'air. C'est ainsi que fonctionne une antenne goniométrique qui permet de détecter les émissions radio dans le spectre électromagnétique.

L'antenne comprend des dipôles en couronne fixés à son extrémité supérieure. La direction peut être déterminée en mesurant l'intervalle de temps entre les signaux radio et les différentes barres. A l'aide de plusieurs antennes, il est possible de calculer la position de l'émetteur à partir de la triangulation des mesures relevées par chaque antenne.

Outre la localisation, l'analyse des moyens radio (fréquence, modulation, comportement) peut également fournir des informations sur les caractéristiques d'un émetteur. En outre, le contenu réel des transmissions radio peut être analysé acoustiquement et, s'il n'est pas crypté, le contexte de la transmission, et donc de la communication, peut être fourni.

Les émetteurs identifiés peuvent être analysés plus en détail. Les émetteurs ayant la même fréquence et des positions géographiques similaires ou des intervalles de temps constants peuvent être regroupés en réseaux. L'analyse de la structure du réseau et fréquences radio permet d'obtenir des informations significatives pour le destinataire de la prestation, par exemple si un réseau de commandement, un relais ou simplement des sites individuels communiquent. Il est très utile de pouvoir découvrir la hiérarchie et la façon de coopérer de plusieurs formations.

Effecteur

Lorsque deux personnes parlent dans une salle et que l'on souhaite empêcher ou mettre fin à cette conversation, il existe plusieurs façons d'y parvenir. Une variante notable consisterait à surpasser le volume de la conversation, avec un ton de voix fort et une volume élevé, la perturbant ainsi. La guerre électronique fonctionne de manière similaire.

A l'aide d'une antenne émettrice, on essaie de couvrir les signaux de l'adversaire sur une ou plusieurs bandes de fréquences. On obtient ainsi une supériorité en termes d'intensité de champ afin d'empêcher toute communication sur ces fréquences dans une zone donnée. Ce brouillage peut avoir différents objectifs, tels que le maintien de ses propres bandes de fréquences ou le brouillage d'importants réseaux pour l'adversaire.

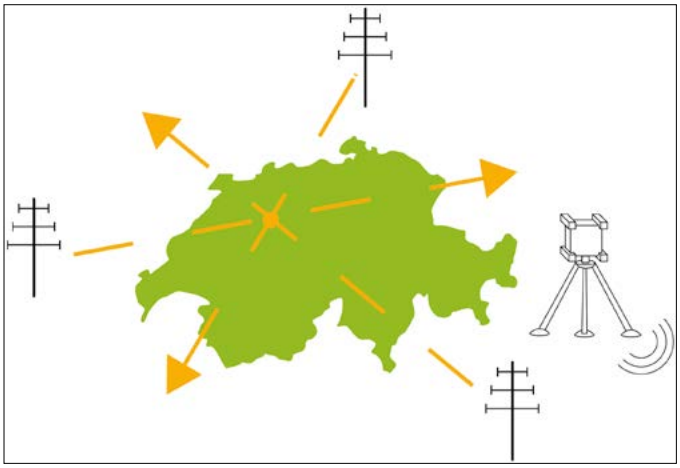
Le signal de brouillage à proprement dit consiste alors généralement en un signal de bruit sourd. Toutefois, il est également possible de diffuser du contenu, par exemple sur une fréquence radio classique pour informer la population ou encore comme forme d'influence psychologique sur des récepteurs potentiels.

Renseignements intégrés

Les senseurs de la GE font toujours partie des Renseignements intégrés (RI) et sont exploités pour le compte d'un destinataire de prestation. Au sein du réseau, les éléments de renseignement de la GE comptent parmi les plus rapides. Une modification du spectre électromagnétique de la situation peut être détectée, classifiée et transmise en quelques secondes. Les informations obtenues doivent alors être vérifiées par d'autres éléments du service de renseignement. En raison des propriétés physiques des ondes radio et de leur possibilité d'évaluation limitée, les conclusions de la GE sont certes rapides mais géographiquement peu précises. Par exemple, des phénomènes radio tels que les reflets à la surface d'un lac ou sur une crête ou leur atténuation par la forêt peuvent fausser le résultat. Les interprètes ont pour mission d'en tenir compte au mieux dans leur évaluation et d'informer les autres destinataires de leurs rapports à ce sujet.

Antenne goniométrique de la GE, composant sensoriel de l'IFASS.

Dispositif d'un secteur d'engagement de la guerre électronique avec la représentation schématique d'une radiogoniométrie par triangulation.



Néanmoins, les signaux générés par le système, la combinaison des données, l'évaluation en termes d'informations et de connaissances offrent une excellente possibilité de compléter l'évaluation de la situation. Avec d'autres sources qui confirment ou infirment les indications, une image de la situation est créée et la conduite peut prendre des décisions en conséquence.

GE en Suisse

La réussite d'une opération dynamique et en réseau nécessite des capacités dans tous les environnements et conditions. C'est pourquoi, dans l'Armée suisse, les groupes GE 51 et 52 sont responsables de l'exploitation des groupes d'action des senseurs et des effecteurs dans l'espace électromagnétique.

Grâce aux conditions du terrain en Suisse, avec ses nombreuses élévations, l'engagement des troupes de guerre électronique contre un adversaire dépendant de la radio est très efficace. Le principal moyen de la Guerre électronique au niveau de l'armée est le Système radio intégré de reconnaissance et d'émission (IFASS: Integriertes Funkaufklärungs- und Sendesystem). Ce système comprend des antennes permanentes qui permettent d'explorer de vastes zones et d'établir une image radio à long terme. Le dispositif est en outre complété par des capteurs mobiles afin de répondre de manière ciblée aux besoins du destinataire de la prestation en matière de renseignement. L'effet effecteur de l'IFASS est assuré par des Emetteurs à usages multiples (MZS: Mehrzwecksender). L'utilisation combinée du système offre la possibilité d'agir en tant qu'effecteur avec le MZS à l'aide d'une puissante énergie électromagnétique sur de grandes distances dans la zone cible et d'utiliser en même temps la technique des senseurs afin d'analyser les effets obtenus et faire de l'exploration radio de manière plus générale.

En comparaison avec d'autres éléments de renseignement, la Guerre électronique convainc par sa capacité à acquérir rapidement des informations sur une grande surface (jusqu'à 100 km²), indépendamment des conditions météorologiques, sans avoir besoin de ses propres troupes dans le secteur d'engagement. La guerre électronique est donc un moyen tactique important pour la conception de ses propres opérations.

M. G.

Emetteur à usage multiple, composant effecteur de l'IFASS.

Aide au commandement

L'importance de la télécommunication

Lt-col Nicolas Flückiger
Cdt bat aide cdmt 41

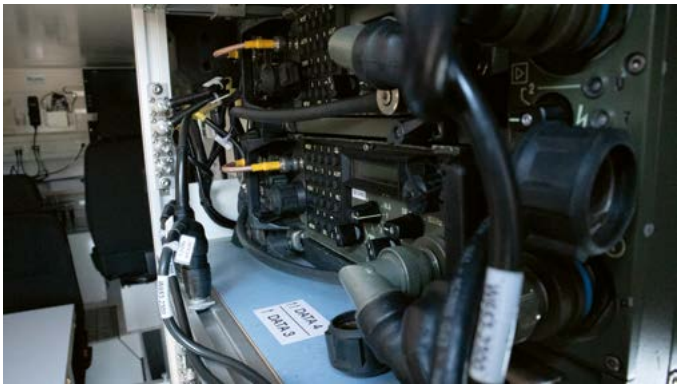
SIC FT ou l'engagement sans téléphone portable

Dans le cadre du conflit en Ukraine, le manque de moyen de communication des troupes russes sur le terrain ainsi que les difficultés de leur état-major de coordonner les actions au sol ont résonné dans les médias. L'armée suisse, à contrario, se prépare grâce à ses troupes spécialisées à ce genre de cas de figures. C'est dans cette optique, respectivement exercer ces moyens de télécommunications autonomes que l'exercice LINK a eu lieu en 2021 afin de tester régulièrement et dans différentes situations les capacités du bat aide cdmt 41. A travers cette publication le bat aide cdmt 41 souhaite donc apporter son point de vue au sujet des systèmes engagés dans leur formation.

Quelles solutions techniques ?

Les forces terrestres suisse dispose depuis de nombreuses années le système de télécommunication SIC FT (Système d'information et de conduite des Forces terrestres). Il soutient les commandants et les états-majors des formations de l'armée de terre, de l'échelon Grande Unité (GU) à l'échelon Unité (U), dans leurs activités de conduite et permet notamment la conduite d'actions en réseau sur la base d'une image commune ou condensée de la situation au sol. Ainsi, les informations sont condensées du bas vers le haut afin d'obtenir une image de la situation la plus pertinente possible pour la phase de prise de décision.

Vue rapprochée d'un module radio dans un container.



Du côté des logiciels, SIC FT se compose des trois applications principales. Tout d'abord, l'application centrale pour la mise en œuvre de la planification des actions et du suivi des situations. Ensuite, un système de gestion des données pour le niveau GU, qui soutient la gestion des processus au bénéfice de l'état-major. Finalement, un système de messagerie qui permet d'envoyer et de recevoir des messages textuels ainsi que des annonces standardisées sur tous les modules SIC FT, tout cela même si le débit de données est faible. Ces trois applications sont intégrées par la société RUAG sur une plateforme qui compose le SIC FT.

Du côté matériel, SIC FT a à sa disposition un grand nombre de véhicules militaires. Cela va du véhicule léger, le Bucher Duro – au véhicule lourd, le char de commandement Léopard II. Cette grande variété de véhicules implique différents formats de serveur et pour cela différentes versions de la plateforme informatique. On retrouvera aussi des composant semi-mobiles et fixes. SIC FT est également déployé dans des containers spéciaux qui peuvent accueillir des serveurs moderne et puissants.

Pour la transmission des données, le SIC FT se base sur les moyens de transmission actuellement disponibles au sein de l'armée suisse, en particulier les radios tactiques à faible débit de données.

Des débuts difficiles

SIC FT s'est tristement fait connaître par le grand publique comme étant un des plus grand flop IT de l'armée suisse. En effet, bien qu'environ 750 millions de francs aient été investis dans l'outil informatique depuis

2006, l'instrument de gestion de l'armée n'a longtemps pu remplir son objectif initial. Grâce à un remaniement drastique du projet, le système est aujourd'hui utilisé et s'est rendu essentiel dans notre engagement de tous les jours. Il est notamment utilisé pour des engagements réguliers et planifiables tel que le WEF (World Economic Forum). En outre, le système est utilisable en tant que système de gestion de crise, lequel sera alors mis en service pour des événements et engagements non planifiés.

Un système en engagement permanent

La conception de base du SIC FT prévoit l'exploitation permanente d'un réseau de sites de conduite sélectionnés – le système de base SIC FT – afin de garantir en permanence une vision de la situation au sol. Ce système est basé sur le réseau de conduite suisse pour la connexion sur les sites de conduite. Avec le principe du serveur, les différents sites / stations – en tant que « client » – sont équipés et reliés entre eux par des réseaux spécifiques. Ce principe permet de limiter l'ensemble du système à des zones restreintes et permet même à certaines stations / lieux de fonctionner de manière autonome lorsque la connexion directe est supprimée.

Un soutien pour la population

Le système SIC FT ne se focalise évidemment pas uniquement sur des engagements militaires. En effet, une des missions de notre armée est la protection de la population et SIC FT peut être engagé à cette fin. Le système a ainsi pu être engagé par le passé au service de la population lors de catastrophes naturelles. Par sa conception permettant une utilisation totalement autonome des réseaux de télécommunications civils ainsi que la possibilité d'utiliser le système sans réseau électrique fixe, SIC FT est le meilleur candidat à disposition pour venir soutenir les autorités civiles, par exemple en cas de glissements de terrain qui isolerait un village ou une région du reste du pays. Grâce à cette autosuffisance, SIC FT permet d'obtenir une vue d'ensemble des données sur la situation locale en temps-record et permet de coordonner les actions nécessaires sur place.

Un partenaire essentiel – Le bat aide cdmt 41

Dans la composition actuelle de notre armée, les troupes terrestres sont soutenues par les troupes d'aides au commandement pour assurer leurs moyens de communication. C'est dans cette optique que le bat aide cdmt 41 est un partenaire essentiel ainsi qu'un fournisseur de service comparable à un opérateur de télécommunication civil. Sans les troupes d'aide au commandement les moyens à disposition des Forces terrestres seraient extrêmement limités. Le bat aide cdmt 41 peut compter sur le soutien de miliciens apportant un bagage de compétences professionnelles.

De la théorie à la pratique – LINK

L'exercice LINK a eu lieu en juin 2021 dans la région de Winterthur et a eu pour but d'exercer nos troupes du bat aide cdmt 41 dans une situation réaliste. Après une donnée d'ordre, un exercice impliquant les moyens de télécommunication commence toujours par un contrôle de la fonctionnalité du matériel ainsi que la mise en place d'un Microdispo. Cette configuration a pour but de tester en miniature la réalité du terrain et de contrôler les paramètres des systèmes afin de s'assurer du bon fonctionnement du matériel. Tout ceci

Mise en place d'un microdispo.

permet de garantir un déploiement à grande échelle. C'est également le moment opportun pour discuter et éclaircir l'aspect tactique qui va jouer un rôle clé dans l'engagement. Cette étape du Microdispo est essentielle afin de connecter les véhicules ensemble. En effet, lors du déplacement sur les emplacements stratégiques, ces derniers sont déjà interconnectés et permettent de communiquer vocalement par radio. Après ce test de fonctionnement, le matériel est ainsi à nouveau empaqueté avec la configuration testée et ainsi l'exercice LINK peut réellement commencer.

L'étape suivante consiste à envoyer des éclaireurs s'assurer de la sécurité des emplacements. Une fois le feu vert donné, les véhicules transportant le matériel se déplacent à leur tour et ainsi les spécialistes peuvent construire les systèmes nécessaires à l'interconnexion de ces points. En effet, ces points étant particulièrement éloignés, l'assemblage d'antennes va permettre d'entrer dans une deuxième phase de la communication puisque celles-ci autorisent une couverture beaucoup plus conséquente en matière de distance. Evidemment, ces emplacements sont protégés d'un point de vue tactique et ne sont visibles que pour un œil avisé.

Durant l'exercice différents cas de figures sont testés. Par exemple, certains emplacements ont été déplacé pour être construits ailleurs et tester le système dans une nouvelle disposition. La déconnexion d'un emplacement puis la reconnexion de ce dernier est également un cas de figure exercé.

L'exercice LINK a mis en évidence pour le bat aide cdmt 41 l'importance d'apporter à chaque participant la vision d'ensemble du réseau. En effet, il en est ressorti que nous avons dans nos rangs d'excellents techniciens et nous devons les pousser à comprendre l'ensemble du réseau pour une exploitation encore plus efficace. Ceci pourra être entraîné lors des prochains cours de répétition.

L'interconnexion internationale

Pour l'armée suisse, en tant qu'acteur actif à l'internationale, les systèmes d'informations doivent évidemment s'aligner et être compatibles avec les standards internationaux. SIC FT garanti l'interopérabilité avec les systèmes de l'OTAN par le respect des standards MIP (Multilateral Interoperability Programme). Dans la même idée, des exercices communs sont conduits régulièrement avec l'Allemagne et l'Autriche avec l'objectif de se focaliser sur l'interopérabilité. FMN (Federated Mission Networking) est quant à elle une contribution essentielle à l'initiative de l'OTAN des forces connectées, qui aide les forces alliées et partenaires à mieux communiquer, s'entraîner et opérer ensemble. La mise en réseau en commun des missions est une aptitude visant à soutenir le commandement, le contrôle et la prise de décision dans les opérations futures grâce à un meilleur partage des informations. Elle offre l'agilité, la souplesse et l'évolutivité nécessaires pour gérer les nouvelles exigences de tout environnement de mission dans les futures opérations de l'OTAN. La mise en réseau en commun des missions repose sur des principes tels que la rentabilité et la réutilisation maximale des normes et capacités existantes.

En outre, la Suisse a été présente ces dernières années à l'exercice 'Coalition Warrior Interoperability Exercise' (CWIX). Le CWIX est l'événement d'interopérabilité le plus important de l'OTAN, axé sur les opérations et le soutien technique, qui répond à un large éventail d'exigences en matière de validation et de vérification de l'interopérabilité. Les capacités de commandement et de contrôle (C2) présentes au CWIX couvrent l'ensemble du spectre des systèmes de communication, d'information et représentent les capacités actuelles, à court terme, futures, et expérimentales de l'OTAN et de ses pays partenaires.

L'avenir c'est la vitesse !

Dans le cadre du développement de l'armée avec la Vision 2030, les moyens de télécommunications actuels vont être remplacés par du matériel plus récent. Le remplacement des systèmes radios actuels ouvrent de nouvelles perspectives tout comme de nouvelles possibilités techniques. En effet, notre système d'information souffre de la bande passante extrêmement limité des systèmes radios et avec la modernisation des logiciels et des besoins grandissant de la digitalisation, ces derniers sont largement dépassés. L'avènement de ces nouvelles radios pourra entre autres permettre la connexion aux réseaux 4G et 5G des fournisseurs de prestations civils mais aussi d'augmenter la bande passante des systèmes purement militaires. Cela pourra offrir des nouvelles possibilités dans les systèmes applicatifs contenus dans SIC FT.

N. F.

Une antenne R-905 utilisée lors du microdispo.

Quartier-général

La richesse discrète des infrastructures protégées helvétique

Lt-col EMG Matteo Pintonello
Cdt bat QG 11

Une des missions permanentes d'un bat QG est l'exploitation et l'entretien des installations de conduite du gouvernement fédéral et de l'armée.

Ce dernier est basé principalement dans le Palais fédéral à Berne. Le bâtiment dispose de salles de travail et de réunions, ainsi que de systèmes informatiques permettant la récolte, le travail, et la diffusion d'informations. Cette infrastructure est nécessaire au bon fonctionnement de l'Etat et à l'accomplissement des nombreuses tâches dont le gouvernement est responsable. Il en va de même pour les hautes autorités militaires, qui doivent pouvoir en tout temps recueillir et analyser l'information, en tirer les conséquences et prendre les décisions nécessaires à la protection de la Nation et de la population. Ces décisions doivent pouvoir être communiquées afin de pouvoir coordonner différentes actions, qu'elles soient politiques, infrastructurelle, ou même militaire.

L'Armée est la réserve opérationnelle du pays en temps de crise. Elle doit pouvoir mettre à disposition des moyens logistiques ainsi que des infrastructures aux organes de commandement civils et militaires en cas de d'événement exceptionnel entravant les activités de ces derniers. C'est aussi le rôle de la brigade d'aide au commandement 41/SIS, via ses trois bataillons Quartier Général (QG).

La fonction et la mission d'un bataillon QG peut paraître mystérieux à première vue, au vu du secret qui entoure ce corps de troupe. Un bataillon QG est un fournisseur de prestation au service du gouvernement fédéral et du commandement de l'Armée. Concrètement, cela signifie l'exploitation d'une installation de commandement, afin d'assurer à une instance politique ou un état-major une infrastructure complète de commandement.

Dans cette optique, certaines formations de l'Armée, généralement des états-majors de planification de la défense, effectuent régulièrement des cours d'Etat-major d'une semaine ou plus dans des installations de commandement de l'armée. Ces exercices se tiennent durant les cours de répétition de bataillons QG. Le but

Soldats du bataillon QG 11 en tenue de protection.

Les activités ne se déroulent pas qu'en intérieur.

de l'opération est d'entraîner aussi bien les compagnies d'exploitation des bataillons, qui profitent de la présence d'organe de commandement dans leurs locaux pour tester leurs prestations, que les Etats-majors eux-mêmes, qui peuvent donc s'exercer en condition réelle, et ce dans les conditions parfois spartiates des installations de conduite.

Mise en évidence des défis que pose l'exploitation d'une installation de conduite au profit des utilisateurs de l'installation.

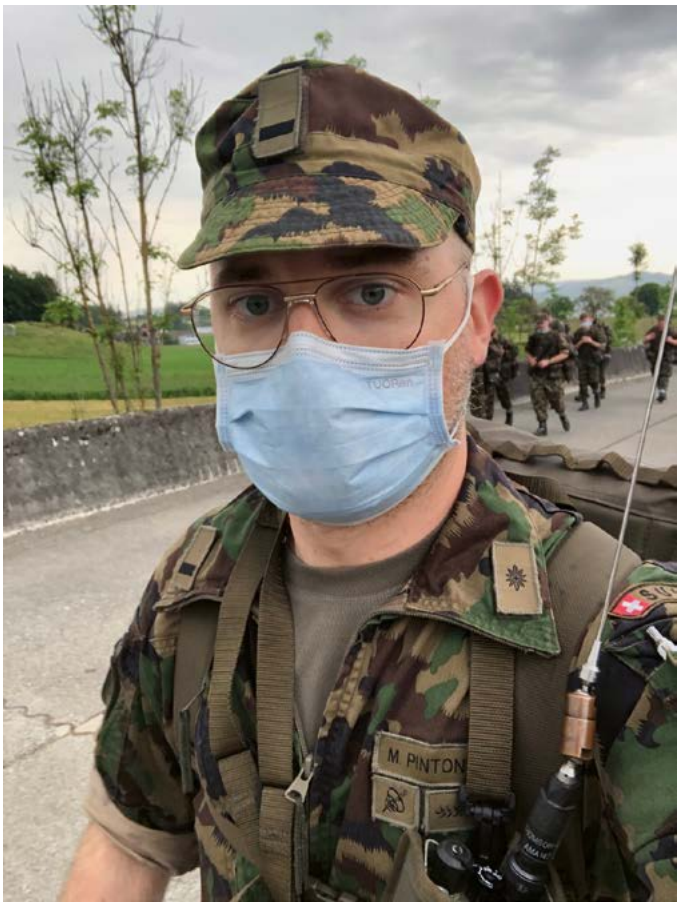
La mise en place ainsi que l'exploitation d'une installation de conduite est une vaste entreprise qui demande de multiples savoirs faire ainsi que beaucoup de flexibilité. L'installation doit pouvoir fonctionner en discrète autonomie tout en permettant la conduite d'une façon aussi flexible que possible. Les installations de conduites étant par nature des lieux militairement sensibles, un périmètre de sécurité l'entoure et doit par conséquent être gardé. Des points de passages surveillés sont établis, ce qui implique la présence de troupes spécialisées dans la surveillance de secteurs ainsi que dans le contrôle de personnes. Plusieurs systèmes de sécurité sont en tout temps actifs au sein et autour des installations. Cela implique que l'entrée, mais aussi la sortie d'une installation n'est pas chose aisée. C'est pourquoi un Bataillon Quartier général doit être en mesure de réagir de l'intérieur en cas d'urgence. Il est ainsi nécessaire d'avoir à disposition, au sein même d'un même ouvrage, des soldats et du matériel spécialisé, par exemple pour combattre le feu, ou des sanitaires et médecins pour la prise en charge médicale. D'autre part, de nombreuses machines hydrauliques, électriques, ou de chauffage sont présentes à l'intérieur d'une installation de conduite. Ces machines nécessitent d'être contrôlées ou, le cas échéant réparées. Cela demande également la présence de soldats ayant une expertise technique ainsi que du matériel spécialisé.

Une fois ces conditions de bases établies, il s'agit de permettre à un organe de conduite de pouvoir effectivement accomplir sa tâche. Un Etat-Major a besoin de surface de travail, de matériel de bureau, de réseau informatique et de sources d'informations. Cela présuppose également de pouvoir communiquer librement avec l'extérieur de l'installation, que ce soit avec des instances politiques, avec les médias, avec la population ou avec des troupes. On retrouve donc également des troupes spécialisées dans la communication et dans les moyens techniques de transmission au sein d'un bataillon QG.

Finalement, afin que chacun puisse accomplir sa tâche avec entrain et dans l'intérêt de la population, il est essentiel de sustenter aussi bien les Etats-majors que la troupe. Nous retrouvons donc nombre de cuisiniers, qui nécessitent eux aussi d'avoir accès à du matériel et à des matières premières de première qualité.

Vous comprenez ainsi la complexité qui se cache derrière l'exploitation d'une installation de commandement, ainsi que les défis logistiques et d'organisation qui en découlent.

M. P.



Le commandant du bat QG 11 en action.

Un tir de combat a été organisé sur la place de tir d'Altmatt-Rothenthurm.

Quartier-général

Il n'y a pas de copeaux sans rabotage

Maj Urs Arnold
Cdt bat QG 22

L'abréviation QG signifie quartier général. Sa mission est d'exploiter les installations de commandement du gouvernement national et de l'armée. En règle générale, un bat QG se compose de compagnies d'exploitation, de transport et de télématique. La compagnie d'exploitation QG est notamment responsable de la subsistance et de l'hébergement des utilisateurs de l'installation, de la protection de l'ouvrage (pompiers, etc.) et des soins médicaux. La compagnie de transport du QG effectue tous les services de transport et la compagnie de télématique du QG assure l'exploitation des installations télématiques ainsi que leur intégration dans les systèmes de transmission de l'armée.

ATTACO – Piste d'entraînement au combat d'Altmatt, à Schwyz

La section du lieutenant (lt) Schintu avec le soutien du lt Weyermann de la compagnie 2 a effectué un tir de combat sur la place de tir d'Altmatt-Rothenthurm. Ouverte en 1978, cette place de tir est la plus importante place de tir d'infanterie de Suisse centrale avec ses installations de tir à 300m ainsi qu'à courte distance, ses installations de combat urbain et ses cibles blindées.

Piste d'entraînement au combat d'Altmatt, canton Schwyz.

Au programme de la journée figuraient le tir dans les cibles à 30m ainsi que la progression avec appui de feu sur la piste d'entraînement au combat dans la partie supérieure du site. En raison du brouillard encore présent, l'instruction n'a pu commencer qu'avec un léger retard et en toute sécurité. Au cours de la matinée, le brouillard a été remplacé par une légère pluie qui n'a pas affecté la troupe. L'équipe PIO (protection des informations et des objets) a pu accompagner le groupe qui avait pris son poste le matin sur la piste d'entraînement au combat.

Visite de la délégation du canton de Berne

L'Office de la protection de la population, du sport et des affaires militaires du canton de Berne a rendu visite au bat QG 22. La visite en présence du directeur de la sécurité du canton de Berne, le conseiller d'Etat Philippe Müller, a été un moment fort. Pour le bat QG 22, la journée se composait de l'organisation du transport aérien au moyen d'Air Request ; et pour la délégation de visiteurs, du vol aller-retour avec un Super Puma des Forces aériennes ainsi que des discussions avec la troupe. Le commandant de brigade d'aide au commandement 41/SIS, le brigadier Thomas Frey et le commandant de la formation d'application d'aide au commandement, le brigadier Marco Schmidlin, étaient également présents. Après le déjeuner, des remerciements ont été prononcés, à la suite de quoi la délégation ainsi que Monsieur le Conseiller d'Etat Philippe Müller sont repartis avec une photo de groupe avant d'entamer le voyage de retour au moyen d'un nouveau vol des Forces aériennes. Le bat QG 22 peut dire avec fierté que cette visite a également été un franc succès.

ATELIER BAT QG 22 – Ce que l'on répare soi-même n'a jamais vraiment été cassé

Le bat QG 22 dispose d'un propre atelier qui s'occupe de son parc de véhicules. Il est la première instance, avant la BLA (Base Logistique de l'Armée), lorsqu'il y a

des véhicules défectueux. Dans la remorque de l'atelier, on trouve tout ce qui est nécessaire pour maintenir les véhicules en bon état, des outils spéciaux spécifiques aux véhicules et aux ampoules de rechange. La troupe du Sgtm (sergent-major) Signorell de l'atelier du bataillon contribue ainsi de manière importante au bon fonctionnement du bat QG. Par exemple, un Duro qui ne pouvait plus reculer se trouvait dans le garage. Les soldats, qui sont des mécaniciens de motos, de voitures et de machines agricoles dans le civil, ont travaillé ensemble pour détecter le problème dans la boîte de changement de vitesse et l'ont rapidement résolu. L'atelier du bataillon a également réparé lui-même les petits dommages à la tôle et à la peinture, car il n'y a pas de copeaux sans rabotage.

Le bat QG 22, l'essentiel pour que tout marche

Peu importe qui en a besoin ou dans quel emplacement se trouve une installation, le bat QG 22 s'occupe des besoins nécessaires au fonctionnement d'un abri de commandement. On peut compter sur les compétences multiples et variées de ce bataillon pour assurer le bon déroulement d'opérations dans une installation. Cela va de la protection d'un ouvrage à l'organisation de la subsistance. La vie dans une infrastructure hors du commun et souvent sous-terre serait difficile sans le soutien du bat QG 22.

U. A.

Délégation de visiteurs du canton de Berne avec le commandant de bataillon, le major Urs Arnold, ainsi que l'adjudant-sous-officier Michael Schumacher.

Les soldats de l'atelier du bat QG 22 travaillent sur les véhicules.

Quartier-général

Bataillons QG – Les perles de l'armée suisse

Lt-col Alain Müller
Cdt bat QG 25

Discrets au niveau de la communication et uniques dans leur performance – c'est ce que sont les bataillons QG ! Mais que se cache derrière ces bataillons uniques en leurs genres et quels sont les défis à relever dans le domaine de la formation technique et de la formation des cadres d'un bataillon QG ? Le bataillon QG (Quartier Général) 25 vous offre un aperçu dans les coulisses de ses activités lors du cours de répétition 2022.

La prestation du bataillon QG 25

Le bataillon QG 25 est l'un des trois bataillons QG de l'armée suisse. Celui-ci a pour mission de gérer les ouvrages de conduite du gouvernement fédéral et de l'armée, d'assurer le fonctionnement des équipements télématiques et des systèmes de transmission qui y sont installés ainsi que d'effectuer des transports en faveur de leurs mandants. Mais qu'est-ce qu'un ouvrage de conduite et qu'est-ce qui en fait sa ses particularités ? Un ouvrage de conduite est une installation au sein de laquelle les états-majors militaires et les organisations du gouvernement fédéral peuvent effectuer leur travail dans des situations particulières. Une installation est comparable à un hôtel de séminaire bien équipé, dans lequel tout est disponible dans le but de pouvoir travailler le jour et de se reposer la nuit. Et comme dans tout hôtel de séminaire d'une certaine importance, d'innombrables tâches doivent être accomplies par les personnes responsables de l'accueil, ceci dans le but d'assurer le bon fonctionnement de l'établissement. Ainsi, il y a un besoin indispensable d'une réception, d'un service d'entretien technique, d'une équipe de cuisine et de cantine, d'un soutien dans le domaine informatique et de la communication ainsi que dans les services sanitaires et de sécurité. Toutes ces fonctions sont assumées par les soldates et soldats du bataillon QG 25 afin que les groupes de travail composés d'états-majors militaires et de représentants du gouvernement fédéral puissent se consacrer à leur travail dans le calme, entourés d'une protection adéquate.

Le défi de la classification

Les ouvrages de conduite sont classifiés. Cela signifie que leur emplacement, leur structure architecturale, leurs degrés de protection et leurs procédures, les processus militaires standardisés ainsi que toutes leurs données quantitatives ne sont accessibles ni à des tiers ni au public. Les militaires sont conscient qu'un bataillon est une organisation comptant plusieurs centaines de soldates et soldats. Vous vous en doutez, l'enjeux dans ce contexte est de garantir la rétention d'information et de communication au sujet de l'ouvrage, et ce à tous les échelons de conduite, que ce soit par la troupe, ou par les cadres et les partenaires externes au bataillon. Ceci a une influence directe sur l'instruction lors des cours de répétition. En effet, la planification de l'instruction et la documentation des supports de formation sont également soumis à cette classification – ceci ne concernant pas uniquement un petit groupe d'état-major, mais des compagnies, des sections et des groupes entiers. Lors des cours de répétition, notre but est, chaque année, de faire un pas de plus en avant en nous appuyant sur les enseignements des années précédentes. L'archivage en conformité avec l'enjeux qu'est la protection de la confidentialité des supports d'instruction et des produits issus des débriefings est une chose. Mais le fait de rendre ces documents à nouveau disponibles au bon moment et au bon endroit lors des préparatifs des cours de répétition, sans pour autant enfreindre les directives relatives à la classification, constitue un défi particulier pour un bataillon QG.

La conduite au sein du bataillon QG

Comme décrit dans le premier paragraphe, un bataillon QG est composé d'un grand nombre de fonctions différentes. Ainsi, nous ne parlons pas ici d'un soldat QG de base avec une fonction supplémentaire spécialisée – comme c'est par exemple le cas pour de nombreuses fonctions dans l'infanterie. Le bataillon QG réunit des

fonctions complètement différentes dans le même secteur d'engagement – comme par exemple un groupe de soldats de sécurité avec un groupe de protection (sorte de sapeurs-pompiers). Cela signifie que chaque soldate et chaque soldat doit maîtriser parfaitement son propre métier et doit aussi très bien comprendre le métier incombant aux autres fonctions – dans le cas contraire, l'interaction dans le secteur d'engagement ne fonctionnerait pas. Ceci nécessite une compréhension mutuelle entre les soldates et les soldats ainsi qu'une maîtrise mutuelle de la fonction de l'autre en ce qui concerne le chef de groupe et le chef de section. Qu'est-ce que cela signifie concrètement pour eux ? La mission de la formation QG consiste à exploiter une installation de manière à ce que les utilisateurs puissent y vivre et y travailler en permanence. En l'essence, cela signifie la gestion de situations particulières. Il peut s'agir d'un incident médical, technique ou même d'un incendie – dans la plupart des cas, il s'agit toujours d'une combinaison de plusieurs situations particulières. Comme c'est le cas dans le reste de l'armée, la règle de base s'applique naturellement aussi au bataillon QG : « Une mission, un emplacement, un chef ». Ainsi, les chefs de groupe et de section doivent non seulement maîtriser leur propre fonction, mais aussi les procédures d'engagement d'autres fonctions, car, si une situation particulière surgit, ils doivent assumer le rôle de chef d'intervention et, en parallèle, prendre la conduite de plusieurs groupes de fonctions. Ceci a pour conséquence de rendre le travail d'un cadre au sein du bataillon QG à la fois varié et exigeant.

Le défi de la formation à la fonction

Alors que dans la plupart des autres troupes la diversité des fonctions est réduite et qu'il existe plusieurs sections d'engagement par fonction, les unités au sein d'un bataillon QG sont structurées de manière plus exclusive. Ainsi, l'étendue des compétences et du savoir de ces formations est essentiel, tout en gardant les groupes de fonctions relativement petits. De ce fait, les commandants d'unité sont grandement sollicités dans la conception des séquences de formation et d'exercices. Lors du cours de répétition 2022, nous avons donc décidé d'organiser une formation technique inter-unités pendant la première semaine. De ce fait, nous avons pu centraliser les différents groupes de fonctions à partir de toutes les unités et les former en profondeur en fonction de leur spécialité respective. C'est ainsi que les groupes de protection ont passé trois jours intensifs à se former sur l'installation de protection incendie de Wangen an der Aare. A cette occasion, toutes les procédures d'extinction et de sauvetage ont pu être entraînées intensivement dans des conditions réelles, c'est-à-dire avec du vrai feu et de la vraie fumée – ce fut un moment fort pour la troupe.

Les groupes de sécurité et les sanitaires ont également été formés de la même manière. Alors que les soldats de sécurité se sont entraînés pendant trois jours dans des conditions météorologiques optimales sur la place de tir d'Altmatt (SZ) à des tirs intensifs de combat en groupe et à toutes les autres procédures d'engagement importantes, les sanitaires ont professionnalisé leurs connaissances techniques à Airolo au sein de l'école sanitaire de l'armée.

Impressions des services d'instruction des formations du bataillon QG 25.

La formation continue est la clé du succès.

Qu'il s'agisse du transport de patients, de la pose de perfusions ou de la prise en charge de blessures graves – le personnel sanitaire du bataillon QG 25 est prêt à aider ses camarades dans toutes les situations. Dans le contexte des ouvrages de conduite, l'autoprotection et la protection des informations revêtent une importance toute particulière. Il s'agit entre autres également des procédures d'intervention de fouille sur des personnes et du matériel. Grâce à une collaboration avec la police de l'aéroport de Zürich, la troupe a pu profiter d'une formation sur le terrain d'une organisation professionnelle – un aperçu exclusif dans l'activité d'un autre partenaire du réseau national de sécurité. Une formation intensive a également été dispensée dans le domaine des transports. La sécurité se trouve toujours au cœur du travail d'un chauffeur – qu'il s'agisse de transport de personnes ou de matériel. Ainsi, durant les périodes sans mission particulière, des manœuvres ont été effectuées, les connaissances sur les véhicules ont été rafraîchies et comme clou du spectacle pour beaucoup : l'occasion a été donnée de manœuvrer des véhicules lourds sur la piste tout-terrain – une aptitude que tout chauffeur militaire doit savoir maîtriser. Il va de soi que la conduite tactique faisait également partie des thèmes centraux de cette formation – c'est-à-dire un déplacement motorisé avec tous les éléments d'engagement. A cet égard, pendant le cours de répétition 2022, nous nous sommes concentrés sur les liaisons et le suivi de la situation au cours d'un déplacement motorisé. Les liaisons – qu'elles soient radio, téléphoniques ou informatiques – sont également le lien central dans la conduite au sein du bataillon QG. Sans liaison, il n'y a pas de conduite. C'est ainsi que tous les pionniers transmissions et informatiques ont effectué leur formation technique au sein du Centre de compétences des systèmes techniques et de conduite (STC). Il s'agissait de retrouver la maîtrise des systèmes radio et informatiques, aussi bien dans le domaine du hardware que dans celui des logiciels.

La centralisation de la formation spécialisée sur l'ensemble du bataillon s'est avérée aussi effective qu'efficace. Les cadres spécialisés ont ainsi pu se préparer de manière ciblée, profiter des connaissances de professionnels externes et proposer à leur propre équipe une formation approfondie tant sur le niveau du contenu que sur le plan méthodologique.

Le défi de la formation des cadres

La diversité des fonctions présente au sein des unités a également une répercussion sur la formation des cadres. Etant donné que ni les chefs de section, ni les commandants d'unité, ni même moi-même, en tant que commandant de bataillon, ne disposons personnellement de l'expertise complète dans l'ensemble des domaines spécialisés, il s'agit alors d'appliquer au mieux la méthodologie d'instruction militaire et de faire confiance aux connaissances spécialisées des chefs de groupe et de section – ce qui est réalisable sans réserve après l'instruction spécialisée intensive qui a eu lieu au cours de la première semaine. Les cadres doivent maintenir et développer en permanence leurs capacités à mettre

en place et à réaliser des exercices. Ainsi, lors du cours de cadres (CC), j'ai accordé une attention particulière à la méthodologie de l'instruction lors de la formation. L'expérience a montré que les thèmes de formation, les scénarios et le déroulement des exercices étaient effectivement définis et développés rapidement. Afin que tant la troupe que les chefs entraînés puissent continuer à apprendre et à se perfectionner, il faut définir des objectifs clairs ainsi que des points d'évaluation et de correctif en découlant. Ce n'est qu'ainsi qu'il est possible de tirer des enseignements et de tirer pleinement avantages des conséquences pour les instructions futures. J'ai ainsi formé les chefs de section et de groupe du bataillon QG 25 en me concentrant sur ces thèmes : formulation des objectifs d'exercice (mesurables) et définition des points d'évaluation et de mesure tout au long d'un scénario. Le résultat a été sans équivoque : les cadres ont réussi à réaliser des exercices courts et intensifs et à identifier ainsi des points d'amélioration très concrets. De ce fait, les groupes et les sections ont ainsi pu se perfectionner rapidement et de manière ciblée.

Instruire durant l'exploitation

Chaque fois qu'un bataillon QG œuvre au sein d'un ouvrage de conduite – également à des fins d'instruction – l'infrastructure est considérée comme étant « en exploitation ». Cela implique des obligations à remplir dans le domaine de la sécurité. Ainsi, l'instruction doit toujours avoir lieu parallèlement à l'accomplissement de la mission proprement dite. En d'autres termes, les cadres sont tenus d'assumer leurs tâches d'exploitation et de piquet tout en assurant l'instruction de leur propre équipe. A cela s'ajoute le fait que le service 24h / 24h doit être assuré en tout temps, ce qui conduit obligatoirement à un travail en relève. Dans ces conditions, entraîner sa propre section sur tous les thèmes de formation reconnus sans « s'user » inutilement, ni user les sous-chefs et la troupe, constitue un défi pour les chefs de section. Cet état de fait exige un effort au niveau de la synchronisation avec les autres éléments d'exploitation, réalité qui n'existe pas dans une telle mesure dans d'autres formations au sein de l'armée.

Bataillons QG – Les perles de l'armée suisse

Les bataillons QG sont caractérisés par une multitude de fonctions, une grande complexité, un niveau de classification élevé et un travail effectué sous l'influence directe de l'échelon supérieur de l'armée et du gouvernement fédéral. Les exigences envers la troupe et les cadres sont par conséquent élevées. Les mandants s'attendent à des performances immédiates. La fidélité à la mission, la précision ainsi que la réflexion sur des solutions optimales sont des exigences que les cadres du bat QG 25 se doivent de remplir. La performance dans le domaine de l'aide au commandement est unique et indispensable dans des situations qui sortent de l'ordinaire.

A. M.

© 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.

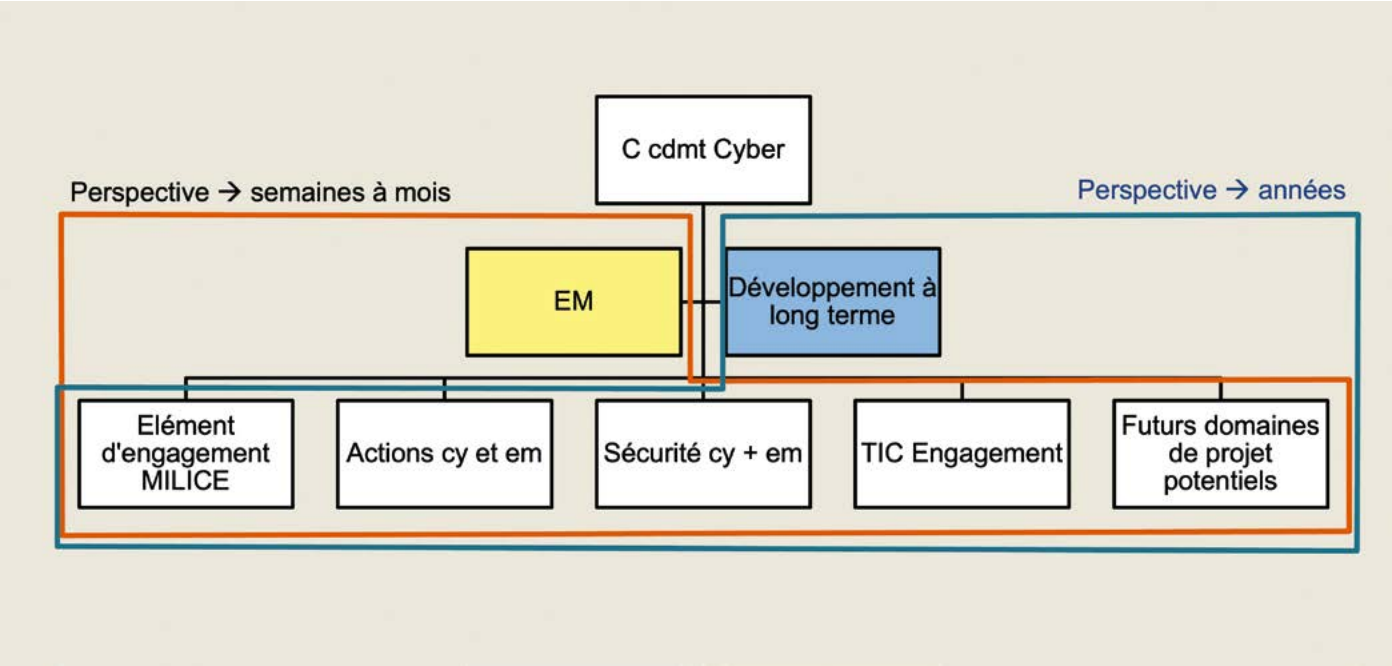
Cet extrait introductif de la Conception Générale Cyber (CG Cyber) décrit de manière exemplaire les défis auxquels l'Armée suisse est confrontée aujourd'hui dans le CYBEEM. En tant qu'un des trois rapports de base que l'armée a publiés ces dernières années, la CG Cyber montre quelle direction les capacités 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

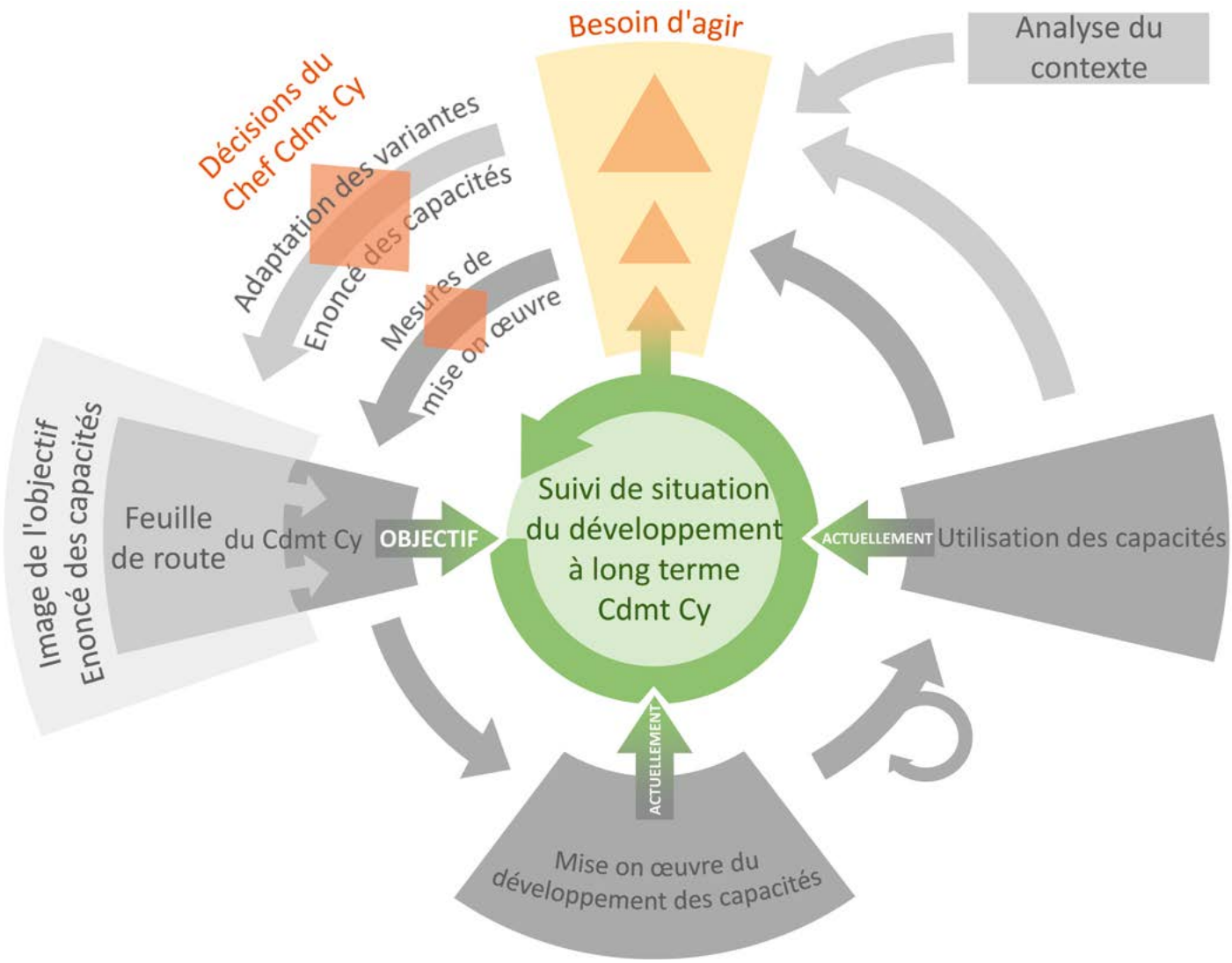
division Développement à long terme identifie un état souhaité à atteindre.

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.

Le char RAP n'est qu'une composante d'un réseau intégré et devant fonctionner en parfaite synchronisation. Photo © Bat ondi 21.

Transmissions

FITANIA – Un réseau de communication résilient de 3'000 km

Col EMG Daniel Ambühl
Cdt aide au commandement SIS

Le renouvellement de l'infrastructure informatique de base de l'armée

Pour pouvoir garantir leur capacité de conduite et d'engagement, les forces armées doivent aujourd'hui disposer d'une infrastructure informatique sûre, permanente et autonome. L'armée suisse renouvelle et étend ses systèmes de technologie de l'information et de la communication en permanence et en fonction des besoins des utilisatrices et utilisateurs.

Ces dernières années, différents projets ont été coordonnés sous le programme FITANIA (infrastructure de conduite, technologie de l'information et raccordement à l'infrastructure de réseau de l'armée). Ces projets ont pour but de renouveler ou d'étendre l'infrastructure de base TIC de l'armée.

Grâce à ces projets, il sera possible de transporter des données et des communications orales depuis les datacenter jusqu'aux terminaux mobiles sur le terrain via un réseau de transmission propre au système. Cela se fera de manière sûre, constante et autonome.

Les TIC (technologie de l'information et de la communication) modernes ont conquis les processus et moyens de l'armée depuis longtemps. Sans moyens informatiques, plus aucun char ne démarre, plus aucun hélicoptère ne décolle. Il n'y a plus non plus de décollage d'avion de combat, ni d'action dans l'espace électromagnétique et encore moins dans le cyberespace. Les TIC sont devenues un élément essentiel des moyens de commandement.

L'Armée suisse dispose d'un grand nombre de systèmes d'information et de communication. Ceux-ci fonctionnent en partie indépendamment les uns des autres et reposent sur des langages de programmation et des technologies différentes. De plus, les données sont stockées dans différents centres de calcul et sur d'autres systèmes isolés. Les capacités et les moyens sont donc fortement segmentés et les données ne sont pas disponibles pour l'ensemble des utilisateurs. Cette situation est due au fait que les moyens informatiques ont été acquis individuellement au fil des ans, en fonction de besoins opérationnels spécifiques. Par conséquent, ils appartiennent techniquement à des générations différentes et un échange de données global n'est pas possible.

Commande et surveillance globales

L'armée a besoin d'une infrastructure TIC qui résiste aux crises. Elle doit être disponible en cas de panne de courant prolongée, d'attaque criminelle paralysant les systèmes informatiques civils, de catastrophe naturelle interrompant les moyens de télécommunication, de systèmes endommagés ou détruits. Mais aussi en cas de frappes militaires ciblées contre la Suisse.

Il s'agit également de simplifier et d'uniformiser le paysage des systèmes. Au lieu de continuer à acquérir chaque système individuellement les uns des autres, les différents éléments seront basés sur une plateforme unique (mais décentralisée) lorsque cela est techniquement et économiquement possible.

La compatibilité et l'uniformisation continue des systèmes, des applications et des langages de programmation, ainsi qu'une organisation et une surveillance globales des réseaux et des installations sont entre-autres des objectifs essentiels. A la clé: une optimisation opérationnelle générale et l'assurance du financement des infrastructures, le tout en garantissant la sécurité de l'exploitation.

Trois projets, un objectif

Sûres, permanentes et autonomes : telles sont les exigences actuelles de l'armée en matière de prestations TIC. Afin de pouvoir garantir ces fonctionnalités à long terme,

les projets concernés portent sur le renouvellement des systèmes informatiques, le regroupement technologique et l'adaptation de l'infrastructure en fonction des besoins. Les projets suivants constituent le noyau de l'infrastructure TIC :

- Trois centres de calcul (deux entièrement protégés par l'armée, un partiellement protégé et à usage civil et militaire), reliés par le Réseau de conduite suisse et réalisés dans le cadre du projet Centres de calcul DDPS/Confédération 2020
- Un réseau de transmission interconnecté ; le Réseau de conduite suisse
- Une extension du Réseau de conduite suisse en faveur du remplacement des moyens radio actuels avec le projet Télécommunication de l'armée.

L'objectif des trois projets est de mettre en place graduellement l'ensemble du réseau et d'intégrer les différents systèmes ou, si cela n'est pas judicieux du point de vue technique ou de la durée de vie, de les remplacer par de nouveaux composants compatibles. Cela permettra non seulement de garantir la capacité opérationnelle de l'armée dans toutes les situations, mais aussi de faire avancer la standardisation des plateformes TIC.

Les systèmes existants seront remplacés par de nouveaux composants de manière coordonnée et harmonisée puis transférés dans la structure interopérable prévue à cet effet. L'exploitation ainsi que la maintenance des systèmes seront également simplifiées.

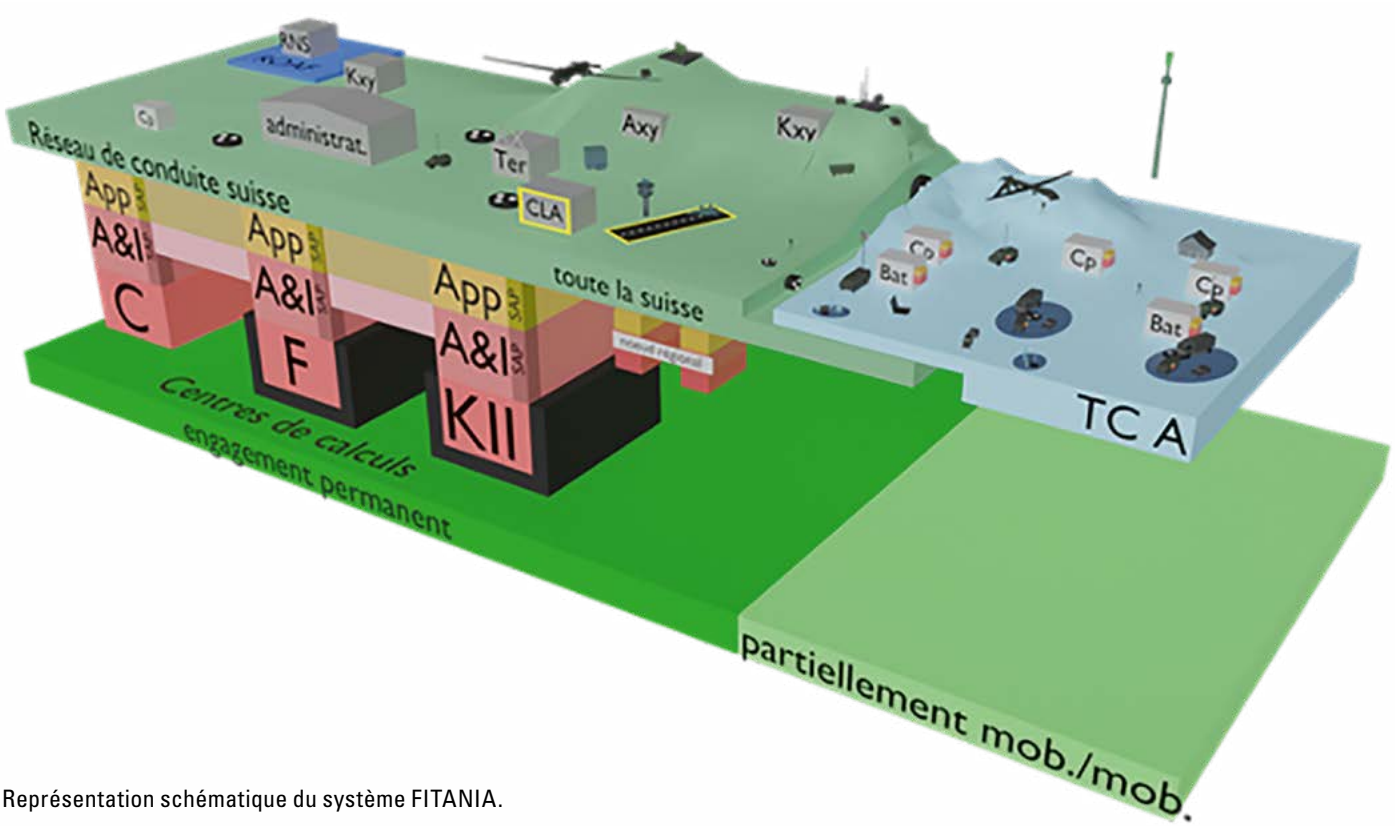
Outre l'infrastructure centralisée, il faudra à l'avenir veiller à ce que les applications de l'armée puissent échanger des données, les traiter, les distribuer et les collecter de manière à ce que l'ensemble des utilisateurs puissent en profiter. Il s'agit ici de modernisation digitale, du capteur à l'effecteur, en passant par les moyens à dispositions pour l'engagement et par le réseau de gestion des données de l'armée. C'est la numérisation à proprement parler de cette dernière, et l'uniformisation de l'infrastructure TIC en constitue techniquement la base.

Trois centres de calcul

Pour pouvoir traiter les flux importants de données, l'armée et les organes de conduite civils, Conseil fédéral compris, doivent disposer de centres de calcul informatique aux capacités suffisamment importantes. Ces centres doivent également répondre à des exigences de protection plus élevées en matière de construction, afin de pouvoir continuer à fonctionner de manière autonome par rapport aux installations civiles en cas de catastrophe (impact physique ou de panne de courant par exemple). En outre, une intégrité totale des données doit pouvoir être assurée. En d'autres termes, si l'un des centres tombe complètement en panne, l'accès aux données reste possible dans les autres installations.

Deux des centres seront dotés d'une protection militaire intégrale. Cela signifie qu'ils seront réalisés sous terre et qu'ils présenteront une résistance accrue aux tentatives d'agression électronique et physique. La capacité des centres de calcul peut être augmentée de manière modulaire, en fonction des besoins des utilisateurs.

Les travaux sur l'un des deux centres de calcul entièrement protégés et sur le centre de calcul exploité conjointement à Frauenfeld sont terminés. La réalisation du troisième



Représentation schématique du système FITANIA.

centre de calcul – le deuxième entièrement protégé – a pris du retard. Ce centre de calcul était initialement prévu à Mitholz. En raison de l'évaluation des risques pour ce site, il a été toutefois renoncé de le réaliser à cet emplaçement et un nouveau site a été recherché. Les activités de planification pour des ouvrages de cette envergure prennent plusieurs années et la réalisation nécessite des moyens financiers considérables. Par conséquent, le troisième site ne devrait pas être achevé avant 2030.

Avec les deux centres de données existants, il est déjà possible de mettre en place un cloud privé et géographiquement décentralisé. Après l'achèvement du troisième centre de calcul, la sécurité apportée par la distance mise entre les datacenter sera atteinte.

L'infrastructure TIC qui sera mise en place dans les nouveaux centres de données est une plateforme largement automatisée, résiliente et décentralisée. Cette « nouvelle plateforme de digitalisation » (NPD) est mise en place dans le cadre du projet commandement Cyber. Dès que les travaux de cette plateforme seront plus avancés, les applications existantes y seront migrées et les anciens centres de calcul seront mis hors service au fur et à mesure.

3'000 kilomètres de réseau de conduite

Le Réseau de conduite suisse est un réseau de transport de données fixe, basé sur des câbles à fibres optiques et des liaisons par faisceaux hertziens. Le réseau de conduite se base sur un réseau central existant (*backbone*) qui dessert déjà une grande partie de la Suisse. Une fois achevé, le réseau s'étendra sur près de 3'000 kilomètres et comprendra environ 300 sites d'utilisateurs. Le réseau étendu permettra de transporter des données cryptées entre chaque site.

Les sites du réseau central ainsi que les sites des utilisateurs seront équipés d'une protection accrue. Cela signifie qu'ils seront renforcés par des architectures capables de contrer les agressions physiques. Une partie considérable de ce renforcement est déjà mise en œuvre.

Le Réseau de conduite suisse est utilisé quotidiennement et a déjà prouvé sa résilience face aux pannes de courant ou aux pannes de réseau des prestataires de services civils dans un passé proche.

Modernisation des moyens de communication militaires

Afin de transporter les données et les informations importantes pour l'engagement vers les éléments mobiles de l'armée et d'assurer la communication vocale, un réseau de télécommunication propre et sécurisé sera mis en place depuis les sites fixes ou le Réseau de conduite suisse. Ce réseau sera également conçu et mis en place sous forme de plate-forme pour remplacer les systèmes isolés et technologiquement dépassés. Les télécommunications de l'armée sont considérées comme un ensemble de systèmes dont la réalisation se fait en plusieurs étapes.

Chaque étape dont la mise en œuvre est autorisée apporte sa pierre à l'édifice. Dans le cadre du projet Télécommunication de l'armée, des appareils à ondes dirigées dotés de fonctionnalités étendues ont déjà été acquis. En outre, un service de données utilisant des antennes de téléphonie mobile civiles comme canal de transmission a été mis en service. Les travaux en cours doivent garantir la compatibilité des différents systèmes. Les étapes réalisées par la suite se basent sur les modules précédents et élargissent ainsi leurs fonctionnalités.

La mise en place progressive de l'ensemble du réseau de systèmes de télécommunication de l'armée s'étendra vraisemblablement jusqu'aux années 2030. Cette longue période de renouvellement des moyens de radio et de communication est notamment due au financement limité. Ainsi, lors de la planification de ces mises à niveau, des étapes échelonnées ont été prévues afin d'acquérir le nombre souhaité d'appareils petit à petit. Bien entendu, les moyens actuels restent en service aux échelons tactiques inférieurs, ce jusqu'à ce que tous les systèmes soient disponibles.

Opérationnel dans toutes les situations

Un datacenter.

Les trois projets sont inter-dépendants en termes de contenu et donc de calendrier. Leur mise en œuvre sera échelonnée dans le temps, en tenant compte de la fin de vie des systèmes existants.

La coordination des différents projets permet de garantir que l'armée dispose d'un réseau TIC consolidé et prêt à affronter l'avenir. Il contribuera à ce que la capacité de conduite et d'engagement de l'armée au profit de la nation et de la population reste garantie dans toutes les situations.

D. A.

Installer un noeud d'ondes dirigées à l'intérieur d'un bâtiment civil améliore sa sécurité ainsi que sa capacité à durer. Photo © Bat ondi 17.

Transmissions

Tour d'horizon des moyens de communication de la troupe

Col EMG Daniel Ambühl
Cdt aide au commandement SIS

Dans cet article, il s'agit pour nous de présenter une sélection de systèmes de communication de l'armée aujourd'hui.

Systèmes radio

L'armée suisse dispose aujourd'hui de différents moyens de communication sans fil. Actuellement, deux systèmes sont principalement utilisés pour la communication. L'émetteur-récepteur SE-X35, qui est utilisé dans toute l'armée dans le domaine VHF pour les courtes et moyennes distances. Et l'émetteur-récepteur SE-240, qui est utilisé à partir de l'échelon du bataillon pour la conduite des Grandes unités dans le domaine HF pour les moyennes et grandes distances. Il convient tout d'abord d'expliquer les deux abréviations utilisées, HF et VHF. Ces deux abréviations expliquent la gamme de fréquences utilisée par chaque système radio. HF signifie « high frequency » et est également connu sous le nom d'ondes courtes. VHF, en revanche, signifie « very high frequency » et est également connu sous le nom d'ondes ultracourtes. Les ondes ultracourtes sont par exemple aussi utilisées par les stations de radio civiles et ont une portée limitée, mais une capacité de données plus élevée. Les fréquences dans la gamme HF sont réfléchies par l'ionosphère, une couche spéciale dans l'atmosphère, et peuvent donc atteindre facilement les stations éloignées.

Le système radio SE-X35 est un système radio VHF pour la transmission numérique de la voix et des données qui fonctionne dans la gamme de fréquences de 30 à 87,975 MHz. Pour assurer la sécurité de la transmission dans le réseau SE-X35, chaque appareil dispose d'un cryptage intégré pour la voix et les données. Pour éviter que les interférences adverses ne perturbent les communications, l'appareil dispose de différents modes de fonctionnement. Par exemple, le mode de saut de fréquence (Frequency Hopping), dans lequel la fréquence change plusieurs centaines de fois par seconde. Cela permet d'éviter que l'adversaire puisse prédire la prochaine fréquence et la perturber. Une autre possibilité est la recherche libre de canaux (Free Channel Search), où l'appareil radio utilise automatiquement une fréquence qui n'est pas perturbée à chaque émission. Bien entendu, l'appareil peut également être utilisé sur une fréquence numérique fixe. Pour se protéger contre l'exploration électronique, tous les signaux émis ont une forme uniforme (signature). Cela signifie qu'en cas d'utilisation d'appareils similaires à tous les échelons de la hiérarchie, seul le type d'appareil connu est identifiable par exploration électronique, mais pas son affectation au réseau ou l'état de la liaison. Tous les paramètres nécessaires à une liaison radio (clés, fréquences, etc.) sont transmis à l'appareil radio par le biais d'un « Fill gun » (FG SE-X35/240). Un appareil peut enregistrer des données pour plusieurs réseaux radio, et le réseau souhaité peut être facilement sélectionné à l'aide d'un commutateur rotatif sur la face avant. Pour éviter une éventuelle tromperie, l'appareil dispose d'un système d'authentification. Il est ainsi possible de vérifier si un membre de l'armée suisse est effectivement assis à la station opposée ou si la station radio est tombée entre des mains étrangères.

L'appareil radio SE-X35 peut être utilisé comme station radio portable (SE-235/t) ou comme station radio intégrée dans un véhicule (SE-235/m1/m2, SE-435). Elles ne se distinguent que par la puissance d'émission disponible et les antennes utilisées. La configuration

prête à l'emploi de la version portable pèse environ huit kg, peut rester en service pendant une vingtaine d'heures et dispose d'une puissance d'émission de cinq watts et d'une portée allant jusqu'à douze kilomètres, si l'antenne correspondante est utilisée. La puissance peut être augmentée jusqu'à 50 watts à l'aide d'un amplificateur, mais cela nécessite l'installation de la station radio dans un véhicule. La puissance amplifiée offre une portée allant jusqu'à 24 km, selon l'antenne utilisée. Grâce à différents accessoires, la SE-235/435 peut être utilisée à distance ou comme station relais automatique. Si la station radio est à portée d'un point d'accès correspondant (Radio Access Point), l'appareil radio peut établir une connexion avec le réseau intégré de télécommunications militaires (RITM) existant. Cela permet à l'utilisateur d'utiliser la fonctionnalité du système de télécommunication militaire directement sur la radio. Par exemple, il est possible de téléphoner à l'ensemble des utilisateurs du réseau de télécommunication et du réseau mobile public, indépendamment de la distance.

Le Réseau intégré de télécommunications militaires (RITM) est le système de communication pour la conduite tactique des Grandes unités et de leurs corps de troupe ainsi que des Forces aériennes. Grâce au maillage et à la commutation automatique, le RITM possède une grande sécurité de transmission. Le RITM se compose de commutateurs, d'équipements d'ondes dirigées, d'appareils de chiffrement ainsi que de terminaux numériques et analogiques pour la voix et les données. Le commutateur est le centre de téléphonie et de données du RITM. Celui-ci peut être configuré en tant que centre de transit au niveau des nœuds et servir principalement d'intermédiaire pour les connexions entre les nœuds. La transmission entre les commutateurs s'effectue en principe sur les ondes dirigées protégées par cryptographie ou sur des liaisons par câble via des fibres optiques. Il existe deux zones de réseau différentes dans le RITM. La Base d'aide au commandement (BAC) exploite et planifie le réseau fixe en tant que réseau interarmées en service permanent sur les différents sites. Le domaine de réseau partiellement mobile est planifié, établi, exploité et entretenu par les bataillons d'ondes dirigées de la brigade d'aide au commandement 41/SIS (br aide cdmt 41/SIS). Le système d'engagement et de planification télématique (TEPLAS) est un module de système militaire spécialisé dans le traitement de l'information qui soutient les commandants ainsi que les chefs de la télématique des Grandes unités ou des formations d'aide au commandement dans les domaines de la planification et de l'engagement de la télématique.

Le commutateur à faible capacité mobile (CF mob) est un véhicule de communication basé sur un Mercedes G qui peut être engagé dans tous les types d'opérations de l'armée. La prestation d'un Commutateur à faible capacité mobile est en règle générale fournie par une demi-section. Grâce à ce dernier, la section peut intégrer au réseau des organisations de commandement de l'échelon du bataillon ou du groupe, des capteurs et des effecteurs (en particulier issu de la défense contre avions) ainsi que d'autres dispositifs de conduite. Le véhicule joue aussi le rôle de raccordement de voix et de données protégées à large bande. Cela permet l'exploitation de différents systèmes d'information de conduite et de systèmes spécialisés. Les militaires de la section sont attribués aux différents mandants, qui peuvent alors disposer des atouts du Commutateur à faible capacité mobile.

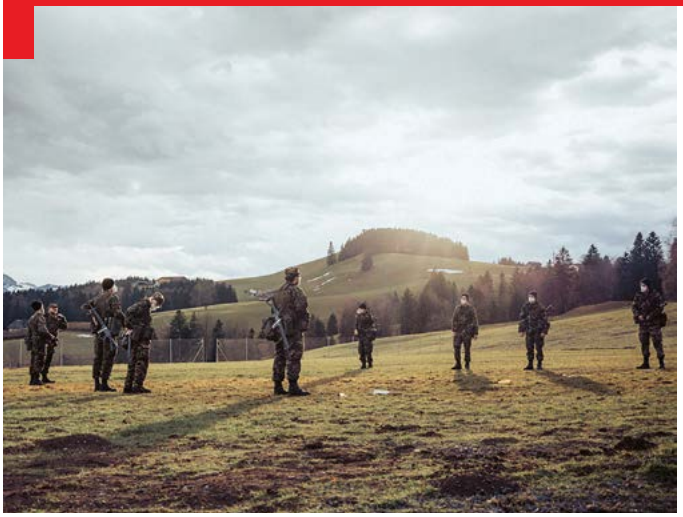
Les Radio Access Points (RAP, points d'accès radio) sont les points d'intégration radio et servent d'éléments de liaison au système radio tactique SE-235/435. Ils sont équipés d'un commutateur RAP/Com Rack et de tout le matériel de chiffrement d'ondes dirigées, de données et de terminaux.

La voiture Radio Access Point (voit RAP) permet d'intégrer dans le RITM des utilisateurs mobiles avec un appareil radio SE-235 et constitue l'interface proprement dite entre le RITM et le réseau radio SE-235. Un RAP permet d'exploiter simultanément cinq liaisons au maximum. L'ensemble du système se compose de la fonctionnalité RAP, des fonctions RITM et du SE-235/435. On parle alors de Combat Network Radio Interface.

Les char Radio Access Point (char RAP) sont attribués par le bat ondi aux Grandes unités et aux divisions territoriales en tant que RAP hautement mobile sur le champ de bataille et protégé contre les attaques. Les caractéristiques RITM et radiotechniques du char RAP sont identiques à celles de la voit RAP. Le char RAP permet d'assurer une capacité d'intégration radio rapide dans le RITM, par exemple en cas d'engagement mobile à proximité du champ de bataille. Le char RAP à l'échelon opératif du bataillon ondes dirigées est dirigé par le service d'engagement télématique du bataillon.

Plateforme de communication avec point d'accès et fonctionnalité de nœud pour chars (char KOMPAK). Le char KOMPAK est un véhicule de communication basé sur un Piranha qui peut être engagé dans tous les types d'opérations de l'armée. Le char KOMPAK est en principe utilisé dans deux types d'engagements différents. Dans le cadre de l'engagement principal, le char KOMPAK est engagé de manière analogue au char RAP, avec en plus la capacité d'assurer la fonctionnalité de nœuds avec quatre stations d'ondes dirigées intégrées dans le mât. Lors d'engagements spéciaux, le char KOMPAK peut être utilisé comme interface entre les différents systèmes de communication militaires et civils du Réseau national de sécurité.

D. A.



Les matériels modernes sont exigeants en matière de formation et d'encadrement. Une pratique et des exercices réguliers sont également nécessaires afin de garantir leur efficacité.
Photo © Bat ondi 17.

Transmissions

Coup d'œil sur la Télécommunication de l'armée

Col EMG Daniel Ambühl
Cdt aide au commandement SIS

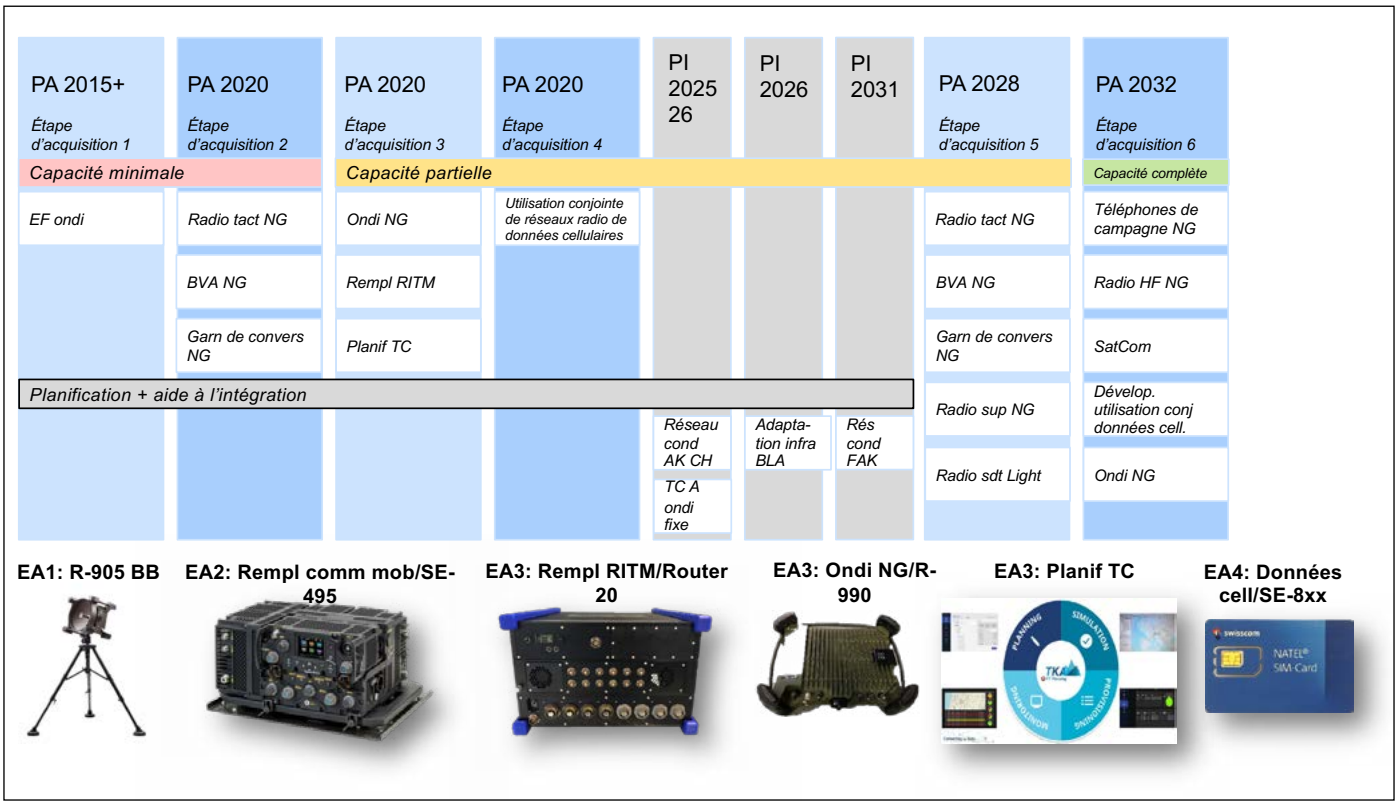
Aperçu des projets d'acquisition actuels avec accent sur le projet Télécommunication de l'armée (TC A).

Le projet Télécommunication de l'armée est le troisième projet du programme FITANIA et permettra de transmettre des services communication vocal et de données à partir du Réseau de conduite suisse depuis les datacenters jusqu'aux unités sur le terrain, en utilisant des composantes mobiles ou partiellement mobiles. L'échange de données se fera de manière cryptée de bout en bout, et ce aussi sur le réseau mobile.

Acquisition par étapes

Le projet TC A est considéré comme un regroupement de systèmes, dans lequel chaque système ou sous-système fournit une prestation particulière. Il s'agit d'un projet très complexe, notamment en ce qui concerne la mise en réseau des différents sous-systèmes mobiles. Pour cette raison et vu les impératifs de sécurité de la transmission de données mobiles, les investissements pour le renouvellement des télécommunications de l'armée sont évalués à environ 1,6 milliard de francs.

Les étapes d'acquisition au travers des différents programmes d'armement.



Chaque sous-système du projet TC A dispose de son propre cycle de vie (initialisation, conception, planification, réalisation, introduction). C'est pourquoi la mise en œuvre du projet TC A se déroule par étapes, chacune correspondant à un niveau de capacité (respectivement : minimale, partielle et totale). Chaque étape représente une nouvelle phase de consolidation du projet TC A :

- **Capacité minimale de 2018 à 2020** : accent mis sur la réalisation des systèmes radio tactiques au niveau de la conduite de la grande unité et du raccordement de nouveaux systèmes modernes de l'armée.
- **Capacité partielle de 2020 à 2032** : réalisation du raccordement partiellement mobile de données (système embarqué, prestation fournie seulement de façon stationnaire) avec le remplacement du réseau intégré de télécommunications militaires (RITM).
- **Capacité totale après 2030** : acquisition d'installations émettrices/réceptrices partiellement mobiles et d'autres systèmes spécialisés, remplacement et acquisition de compléments de systèmes existants.

Projets d'acquisition d'appareils et de systèmes

Performants, les appareils et systèmes en cours d'acquisition permettent de communiquer en toute sécurité et apportent des améliorations du point de vue de la capacité de conduite ainsi que de la cyberdéfense. Il ne s'agit toutefois pas de faire un remplacement purement et simplement, mais d'utiliser ces systèmes de manière coordonnée sur la nouvelle plateforme de digitalisation.

Concernant la communication mobile, il convient de remplacer les appareils radio actuels destinés à l'échelon tactique, qui comprennent aussi les installations de communication de bord ainsi que les accessoires de communication (microphone et dispositif d'écoute intégrés au casque). Ces **appareils radio sans fil** offrent aux utilisateurs et utilisatrices mobiles un moyen sécurisé de transmission vocale et de données. **Les installations de communication de bord** permettent la communication notamment à bord de véhicules blindés et servent d'interface avec tous les moyens de communication externes embarqués, tels que la radio tactique. Les **nouveaux accessoires de communication** visent à remplacer les modèles actuels, qui proviennent de différents fournisseurs et ne sont pas compatibles entre eux.

Sur le plan de la communication semi-mobile, il est nécessaire d'acquérir des **appareils à ondes dirigées** supplémentaires qui permettent l'établissement d'une connexion sécurisée à large bande en direction des infrastructures de l'armée (p. ex. postes de commandement) pour les transmissions vocales et de données via bande passante. Ils peuvent se connecter au Réseau de conduite suisse par le biais du réseau intégré de télécommunications militaires, remplaçant ainsi les appareils à ondes dirigées en service.

Le **réseau intégré de télécommunications militaires** forme avec les nouveaux appareils à ondes dirigées (R-990) la base de la communication militaire. Le système de transfert de données semi-mobile relie les systèmes des échelons opérationnels et tactiques. Il joue un rôle névralgique pour les transmissions vocales et de données, se révélant essentiel pour la diffusion de l'image tactique de la situation. Cette acquisition vise avec un protocole standardisé et de débits de données à remplacer le système existant, notamment en matière de connexion.

Les systèmes en cours d'acquisition.

Si des bandes passantes plus larges que celles dont l'armée dispose par ses propres moyens sont nécessaires et qu'aucun moyen de communication militaire n'est disponible, il lui faut recourir aux réseaux de données radio des fournisseurs civils pour garantir sa communication mobile. Selon les circonstances, ces réseaux assurent le remplacement du système militaire ou servent de moyen de communication principal. Les composants pour la communication, intégrés aux véhicules, prennent en charge une utilisation partagée des réseaux de données radio civils selon le système « best effort » et avec un cryptage *« end to end »*. Pour rendre possible l'utilisation des réseaux de données radio civils , il est prévu d'acquérir entre autres, des cartes SIM, des modems ainsi que des antennes, en les intégrant ensuite aux systèmes militaires correspondants.

Finalement, une interface informatique est nécessaire à la planification des technologies de communication, dans le but de gérer l'emploi des systèmes de communication et de configurer les systèmes. Celle-ci permet l'utilisation en parallèle de fréquences, de numéros de réseau, de clés de chiffrement et d'adresses IP. Elle remplace ainsi les anciens systèmes de planification et simplifie grandement leur fonctionnement.

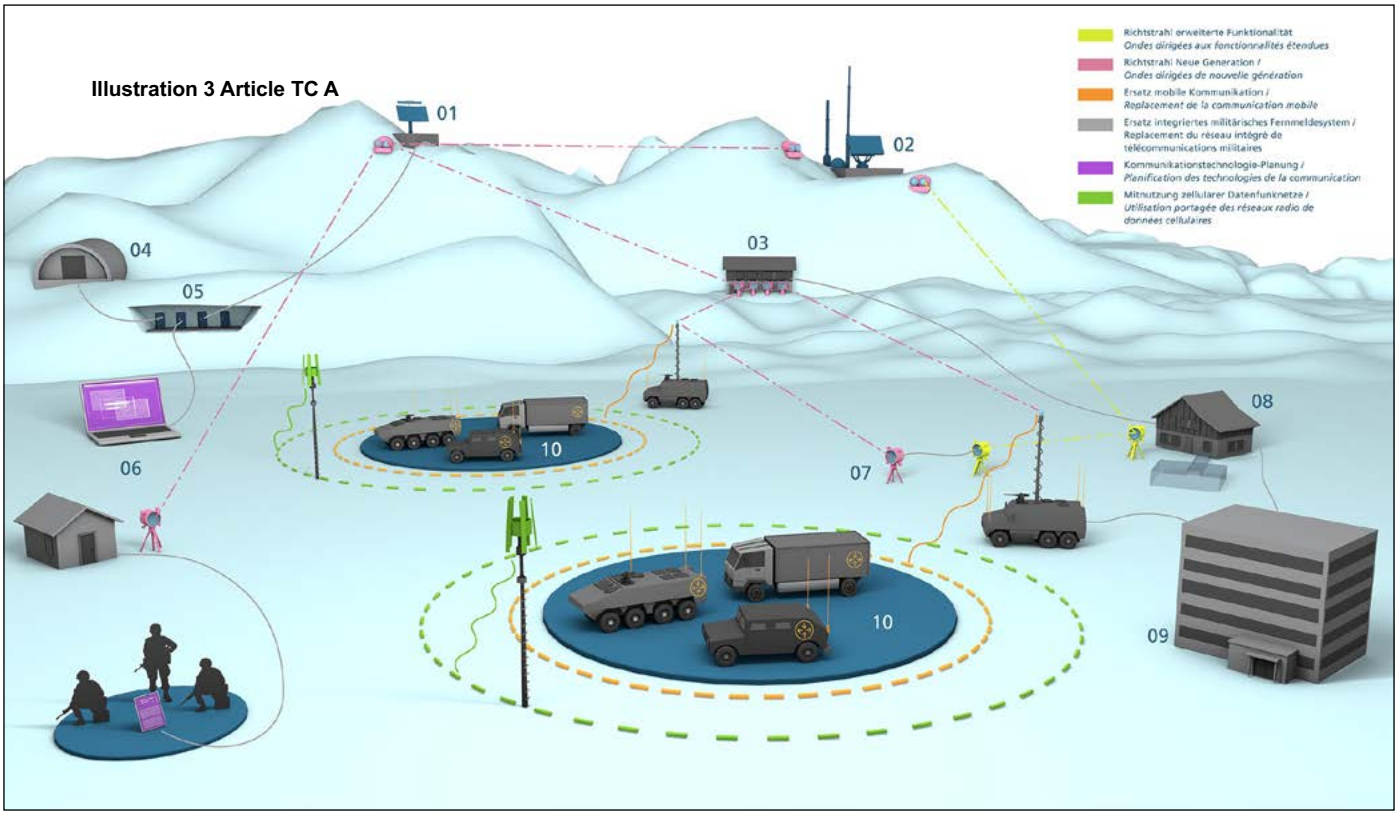
Un projet d'acquisition de grande ampleur

Chaque projet d'acquisition comporte un certain nombre d'incertitudes et d'obstacles tout au long de son existence. Dans le cadre du projet TC A, ces défis sont notamment dû à la complexité générée par l'échelonnement des acquisitions (plus de 20 ans entre le démarrage et la conclusion du déploiement) et par l'impact de celles-ci sur la quasi-totalité de l'armée, et ce tout en synchronisant la nouvelle plateforme de digitalisation avec ce nouvel ensemble. En effet, l'introduction des matériels et systèmes du projet TC A concerne l'ensemble des corps de troupes de milice ou professionnelles au niveau opérationnel et les formations d'applications. De plus, le projet contient une multitude d'interfaces entre les différents commandements de l'armée (cdmt Op, BLA, BAC, cdmt Instr), mais aussi avec l'office fédéral de l'armement (armasuisse) et le secteur privé. Orchestrer un projet d'une telle ampleur nécessite un investissement total et de longue haleine des parties prenantes principales et des fournisseurs de prestations. Finalement, un défi majeur réside aussi dans les évolutions technologiques qui prennent et prendront place dans les prochaines années. Dans ce domaine, les spécialistes d'armasuisse suivent constamment les évolutions technologiques en matière de défense et de communication afin de garantir l'adéquation des acquisitions sur toute la durée du projet. Pour ce faire, des échanges réguliers avec nos partenaires sécuritaires et industriels au niveau national et international ont lieu.

Introduction des nouveaux systèmes et instruction

L'introduction de la TC A est la plus grande introduction dans le domaine de l'aide au commandement que l'armée ait connue jusqu'à présent. Il s'agit en fin de compte du renouvellement de tous les moyens TIC. Cela ne concerne pas seulement les troupes d'aide au commandement, mais toute l'armée. Presque tous les corps de troupe, les systèmes embarqués de véhicules et l'infrastructure elle-même sont concernés par ce renouvellement. La connexion à large bande ouvrira de nouvelles possibilités

Vue d'ensemble / principe d'engagement schématique des composantes TC A.



et les procédures d'engagement des corps de troupe et des Grandes unités seront modifiées.

L'instruction est dirigée et synchronisée par une organisation d'instruction spéciale sous la direction du commandant de la brigade aide commandement 41/SIS. Sur le plan opérationnel, l'introduction de ces système pour le personnel professionnel et les formations en cours de répétition est dirigée par le commandement Introduction / Reconversion TC A (cdmt Intro / reconv CT A), qui est composé d'instructeurs de toute l'armée selon le principe du « Burden Sharing » et qui est dirigé par le commandant du commando aide commandement SIS en double fonction.

Dans une première phase, le personnel professionnel est formé, à partir d'une deuxième phase, la relève est instruite dans les services d'instruction de base (écoles de recrues) et ce n'est qu'à partir d'une troisième phase, tout en maintenant la disponibilité de l'armée, que la reconversion des formations en cours de répétition a lieu sur plusieurs années.

L'instruction emprunte de nouvelles voies et s'adapte à la numérisation. Comme la plupart des systèmes sont constitués en majorité de logiciels et que les appareils sont très chers, l'instruction de base sur ceux-ci est réalisée en partie et surtout au début sur des systèmes d'instruction virtuels, couplés à l'apprentissage en ligne et à des formations basées sur le web.

L'environnement de test et d'intégration TC A

Les systèmes TC A ne sont plus des systèmes distincts, mais des systèmes fonctionnant tous sur la même plateforme de numérisation. Par conséquent, le test et surtout l'intégration prennent une toute nouvelle importance. Pour les systèmes ou les nouvelles versions de logiciels qui ne fonctionnent pas encore parfaitement, le risque serait que la plateforme de numérisation complète ne fonctionne plus sans test d'intégration. Cela mettrait en péril l'engagement et la disponibilité de l'armée.

L'environnement de test et d'intégration TC A garantit que l'infrastructure de test et l'environnement de gestion de ceux-ci nécessaires soient disponibles pendant tout le cycle de vie des systèmes informatiques et radio TC A et que les tests nécessaires soient possibles. Avec une nouvelle construction dans la caserne Auenfeld à Frauenfeld, l'environnement de test et d'intégration TC A disposera dès 2024 d'un nouveau site avec une surface de test d'environ 400m^2. A l'aide des environnements de test du Réseau de conduite suisse et du datacenter, il sera possible à l'avenir de réaliser des tests de bout en bout dans des scénarios proches de l'engagement, de manière manuelle ou (partiellement) automatisée. Dans cette interconnexion, l'environnement de test et d'intégration TC A reproduit l'environnement système des échelons mobile et partiellement mobile.

L'accent est mis sur des tests annuels des nouvelles versions logicielles des systèmes de faisceaux hertziens, de radiocommunication et de réseau TC A. En cas de réception réussie, l'équipe de test autorise leur introduction dans l'exploitation opérationnelle. En outre, les réseaux sont mis à disposition pour les tests des systèmes et applications spécialisés qui utilisent les systèmes de transmission TC A, et leur interconnexion est contrôlée. Cela permet d'éviter les pannes de système ou les éventuels dysfonctionnements causés par l'intégration incorrecte de nouveaux systèmes ou de nouvelles fonctions.

D. A.

Maintien de la Paix

En réseau à travers le monde : moyens informatiques d'information et de communication utilisés dans le cadre du service de promotion de la paix

Centre de compétences SWISSINT

Les militaires de l'armée suisse sont en service aux quatre coins du globe pour la promotion de la paix. En particulier lors de ces missions, l'information doit être transmise vers l'étranger, traitée et gérée de manière d'autant plus sûre et fiable, en raison de la distance et du potentiel de danger. Or, cela représente un véritable défi. Ainsi, pour garantir la communication, reconnue comme un facteur clé dans la gestion opérationnelle, l'aide au commandement joue un rôle déterminant.

Centre de compétences SWISSINT : au service de la promotion de la paix

Situé à Stans-Oberdorf (Nidwald), le Centre de compétences SWISSINT est le poste de commandement national chargé de tous les engagements de promotion de la paix à l'étranger effectués par l'Armée suisse. Il est responsable de la planification et de la conduite, du recrutement, de l'encadrement et de la gestion de tout le personnel, de l'instruction individuelle et de celle des contingents ainsi que de l'équipement des militaires pour l'engagement. Il assure également la logistique à l'étranger, la planification des finances et la gestion des crédits, le travail de relations publiques et l'évaluation des engagements. Quelque 280 officiers, sous-officiers, soldats et membres du personnel civil, femmes et hommes, participent à une douzaine d'opérations en Europe, en Afrique et en Asie, sous l'égide de SWISSINT. Pour l'instruction en vue de l'engagement des soldats, la responsabilité incombe au centre d'instruction (CI) de SWISSINT. Des instructrices et instructeurs expérimentés provenant de l'armée de milice, du corps des militaires de carrière et d'organisations partenaires du CI forment l'ensemble des militaires de l'Armée suisse accomplissant un engagement volontaire à l'étranger dans le cadre de la promotion de la paix. Tous les cours sont conçus de manière à répondre aux exigences et aux doctrines des engagements qui sont confiés à la troupe, et sont adaptés en continu aux besoins opérationnels. Très diversifiée, l'offre de ces cours s'adresse à toutes personnes intéressées, civiles ou militaires, sur les plans national et international.

Lancée en 1999, la mission de la SWISSCOY en faveur de la KFOR au Kosovo est devenue le véritable symbole de tous les engagements à l'étranger. Mais ailleurs, d'autres femmes et hommes (observateurs militaires, officiers d'état-major et de liaison, experts en déminage) sont aussi engagés individuellement ou en petites équipes, que ce soit sur mandat des Nations Unies (ONU), de l'Organisation pour la sécurité et la coopération en Europe (OSCE) ou de la European Union Force (EUFOR).

Le Centre de compétences SWISSINT est directement subordonné au chef du commandant des Opérations et accomplit ses tâches conformément aux directives politiques du Conseil fédéral et du Parlement ainsi qu'aux lignes directrices du chef de l'Armée.

Le domaine de base de conduite I6

La capacité à transmettre, traiter et gérer l'information de manière sûre et, notamment dans le cas de la promotion de la paix, en tout temps et dans n'importe quelle situation à l'étranger représente pour l'Armée suisse un défi important et pour ainsi dire totalement nouveau. La communication est reconnue comme un facteur clé dans la gestion opérationnelle et l'aide au commandement, comme un aspect déterminant pour établir et garantir que les informations soient transmises de manière conforme aux attentes. Pour les missions de promotion de la paix, il faut alors veiller d'autant plus à assurer la communication, en raison de la distance et des dangers potentiels. Les prestations d'aide au commandement (services de la technologie d'information et de la communication TIC) sont nécessaires aussi bien sur le lieu d'engagement qu'en Suisse. Il s'agit donc d'une thématique complexe, dont est chargé le nouveau domaine de base de conduite I6 (DBC I6), au sein du Centre de compétences SWISSINT. Le DBC I6 (domaine de base de conduite) est responsable

de garantir la disponibilité, le fonctionnement et la mise à niveau de tous les moyens d'information et de communication (moyens TIC) utilisés par le personnel en engagement et évoluant au sein de SWISSINT. Il donne des instructions ciblées sur ces technologies, en accord et en collaboration avec les organisations partenaires ainsi que les fournisseurs. Il est aussi l'interlocuteur dédié pour les thèmes cyber et le responsable de la mise en œuvre des mesures préventives nécessaires dans ce domaine. Parmi ces compétences, on compte aussi la surveillance et le développement des systèmes utilisés lors d'engagement et donc la prise en considération des processus de changement en continu des technologies numériques.

L'avantage de disposer d'un propre DBC I6 est notamment de faire concorder l'engagement et l'administration sur le plan de la technique des systèmes, et donc de développer les plus grandes synergies possibles dans le cadre de la transformation numérique, qui suit depuis longtemps son cours. Pour cela, il faut bénéficier d'agilité et d'une excellente compréhension des différentes conditions d'engagement dans le domaine TIC.

Engagements individuels

Environ 50 personnes sont investies individuellement dans différentes missions et zones d'engagement pour la promotion de la paix. Cinq officiers suisses sont aujourd'hui au service de la Commission de supervision des nations neutres (Neutral Nations Supervisory Commission, NNSC) sur la ligne de démarcation entre les deux Corées. Au profit de l'ONU, des observatrices et observateurs militaires ainsi que des officières et officiers d'état-major suisses sont engagés depuis 1990 au Proche-Orient, en République démocratique du Congo (RDC), au Soudan du Sud, au Mali, au Cachemire et au Sahara occidental. L'Armée suisse agit aussi en faveur du déminage humanitaire, en envoyant partout dans le monde des spécialistes auprès de l'United Nations Mine Action Service (UNMAS). D'autres officiers suisses assument le rôle de responsables de cours pour le développement des capacités à divers endroits sur le continent africain. Ils travaillent également dans différents domaines aux Nations Unies à New York et à Genève, ainsi qu'au quartier général de l'Organisation pour la sécurité et la coopération en Europe (OSCE) à Vienne.

Environ 50 personnes sont investies individuellement dans différentes missions et zones d'engagement pour la promotion de la paix.

Les normes attribuées par l'organisation responsable de chaque mission sont très variées. En principe, le personnel est actif en tant que force opérationnelle de contrôle (*operational control*, OPCON). C'est notamment pourquoi la mise à disposition des moyens TIC nécessaires sur le plan opérationnel leur incombe. En raison de la composition multinationale des missions, il s'agit là de la seule approche envisageable. Autrement dit, si les *peacekeepers* venaient avec les systèmes issus de leur propre pays, il serait impossible de garantir une interopérabilité entre les parties prenantes, en l'état actuel des choses, même si la future norme OTAN *Federated Mission Networking* (FMN) devrait prochainement contribuer à améliorer la situation.

La part des moyens fournis par les pays d'origine des intervenants est donc faible. Pour la Suisse, elle se limite aux systèmes permettant d'assurer la connexion vers le Centre de compétences SWISSINT, c'est-à-dire, principalement des ordinateurs portables dotés d'une solution standard telle que BURAUT (Büroautomation) ou d'un système de postes de travail spécial (SPT spéc). En ce qui concerne la téléphonie mobile, on procède jusqu'ici selon le principe *Bring Your Own Device* (BYOD). Toutefois, à l'heure où les cybermenaces se font de plus en plus pesantes, il convient d'aboutir à l'avenir à des solutions adéquates, qui reposent sur des appareils non pas privés, mais fournit spécifiquement pour l'engagement en question. Ainsi, la sécurité de l'information dans le cadre de la mission (INFOSEC), mais avant tout la protection des données du personnel engagé (PERSEC) seront nettement améliorées. La communication entre le personnel stationné et SWISSINT doit, dans la mesure du possible, s'effectuer à travers des connexions sécurisées. C'est pourquoi elle doit se faire en priorité grâce à des applications offrant des services autorisés de messagerie instantanée et d'appels vidéo chiffrés de bout en bout (p. ex. Threema). Pour une communication plus large, on emploie traditionnellement le courriel. Sur les systèmes répondant au standard BURAUT, on utilise Secure Messaging, et ProtonMail sur les autres appareils. De plus, le contenu classifié est crypté via Secure Center.
Mais un obstacle est parfois de mise : l'insuffisance voire l'absence de couverture réseau notamment en déplacement hors des agglomérations ou dans des régions reculées.

Afin d'assurer la communication entre les *peacekeepers* et SWISSINT dans de tels cas, le personnel dispose seulement d'un téléphone satellite, spécialement dédié à pallier cette difficulté. Or, cet appareil de téléphonie classique ne garantit ni le chiffrement des appels ni une liaison optimale (interruptions, transferts refusés). Autrement dit, selon la situation, les conversations ne peuvent pas être tenues convenablement. Pour contrer ce problème, le projet *Travel Safety* a permis de lancer une innovation, qui rend notamment possible l'utilisation de moyens de communication primaires (messagerie instantanée Threema) par transfert de données satellite, indépendamment du lieu.

Bosnie-Herzégovine : EUFOR

En Bosnie-Herzégovine, on compte depuis 2004 jusqu'à 20 militaires suisses en service dans les équipes de liaison et d'observation (*Liaison and Observation Teams*, LOT) en faveur de la mission ALTHEA de l'EUFOR. De plus, jusqu'à six expertes et experts, qui sont affectés à une équipe de formation mobile (*Mobile Training Team*, MTT) d'ALTHEA, instruisent les forces armées de Bosnie-Herzégovine à la gestion des munitions et des armes légères.

Dans cette mission, la situation sur le plan des TIC est semblable à celle décrite pour le personnel engagé individuellement. Les personnes qui y sont envoyées servent en tant qu'éléments OPCON et ont en principe recours aux moyens TIC de la mission. Toutefois, il s'agit d'équipes plus petites, qui ensemble forment, en quelque sorte, un contingent suisse à taille modeste. Ainsi, la part des moyens mis à disposition par la Suisse est proportionnellement plus conséquente ; en effet, les systèmes requis pour l'accomplissement de la mission doivent être en partie acquis et exploités par la Suisse. Il s'agit par exemple d'ordinateurs spécifiques qui correspondent aux critères requis par la mission et à ses normes de sécurité. De plus, les équipes bénéficient de systèmes de postes de travail BURAUT, comprenant au besoin les périphériques ad hoc, ainsi que de certains réseaux locaux et supports de données (NAS). Pour ce qui est des moyens de communication mobiles, SWISSINT met à disposition des téléphones portables munis d'une carte SIM donnant accès aux réseaux des fournisseurs locaux. Il s'agit de smartphones, mais aussi de téléphones satellites à utiliser en cas d'urgence.

En raison du petit nombre de personnes envoyées, l'intégration de spécialistes informatiques n'est pas envisageable. Le support doit donc être fourni par la Suisse. Lorsque cela s'impose, des spécialistes peuvent tout de même être mandatés sur place pour du dépannage. Quoi qu'il en soit, lors des changements de contingent tous les six mois, une équipe de spécialistes est engagée pour le contrôle et la maintenance des systèmes exploités. Pour réduire les charges en matière de support, les *peacekeepers* suivent en amont une instruction en informatique. Ainsi, les équipes sont à même de réaliser de manière indépendante les travaux de maintenance et de sécurisation des données. Etant donné l'absence de spécialistes sur place, il n'est toutefois pas envisageable d'utiliser des systèmes complexes. Cet aspect doit être donc pris en compte au vu de la rapidité de la transformation numérique.

En Bosnie-Herzégovine, on compte depuis 2004 jusqu'à 20 militaires suisses en service dans les équipes de liaison et d'observation.

Kosovo : SWISSCOY

La SWISSCOY est à ce jour l'engagement le plus important de l'Armée suisse pour la promotion de la paix. Depuis 1999, jusqu'à 195 militaires par contingent sont en service auprès de la Kosovo Force (KFOR), assurant le maintien d'un environnement sûr et stable (*safe and secure environment*) et la liberté de mouvement (*freedom of movement*) pour l'ensemble des citoyennes et citoyens du Kosovo.

La plupart des conditions décrites ci-dessus en matière de TIC s'appliquent aussi à l'engagement SWISSCOY. En revanche, un contingent d'une telle taille implique la présence d'un état-major et d'une équipe de support sur place (*National Support Element*, NSE), afin de garantir l'engagement des éléments OPCON. Ainsi, la part des moyens et prestations TIC est beaucoup plus importante que dans les autres circonstances décrites plus haut, et l'envoi d'un large personnel permet l'intégration de spécialistes TIC. Le support n'est donc pas garanti que depuis la Suisse, mais peut être fourni directement sur place et en grande partie grâce à des spécialistes ayant suivi une instruction en amont pour l'engagement (p.ex. S6, resp infm, spéc trm).

Les moyens engagés sont ainsi multiples, allant de la radio tactique (p. ex. SE-x35, TETRAPOL de la KFOR), jusqu'aux moyens informatiques (BURAUT, KFOR Mission Secret, etc.) et aux systèmes multimédias, en passant par la connexion internet (fournisseur local, liaison satellite, et téléphonie telle que UCC, téléphones IP et satellites ou radios mobiles). Tous ces systèmes doivent fonctionner 7 jours sur 7, 24 heures sur 24, 365 jours par an. Au vu de la complexification probable des systèmes à venir, une professionnalisation du domaine de l'aide au commandement (TIC) est incontournable.

Dans la Swisscoy, les savoir-faire requis sont nombreux.

Interconnexions avec les partenaires

Lorsque cela est possible, SWISSINT se fonde également à l'étranger sur des systèmes de troupe déployés, grâce auxquels la maintenance et le support des moyens TIC sont assurés. Les compétences réparties entre SWISSINT, la Base logistique de l'armée (BLA) et la Base d'aide au commandement (BAC) sont à chaque fois définies à l'échelon *système*. Ainsi, SWISSINT est bénéficiaire de prestations, tandis que la BLA et la BAC en sont les fournisseurs, et ce pour le domaine des systèmes de troupe (p. ex. radio SE-x35, SAT Phone, etc.), ainsi que pour les plateformes et systèmes civils (p. ex. BURAUT, SATCOM, Crypto Phone, etc.). Des prestations spécifiques aux systèmes sont également fournies par des tiers mandatés par la BAC. Il s'agit notamment de l'Office fédéral de l'informatique et de la télécommunication (OFIT), de l'Office fédéral des constructions et de la logistique (OFCL), du Département fédéral des affaires étrangères (DFAE) ou de RUAG (entreprise de la défense et des domaines aérospatiaux de la Suisse). Comme évoqué plus haut, on peut constater certaines différences entre les missions. Les directives techniques et tactiques sont imposées par la mission et définies dans des *Standard Operating Procedures* (SOP). Cela concerne entre autres la radio TETRAPOL ou la plateforme informatique Mission Secret.

En conclusion, on notera donc toute l'importance de l'aide au commandement pour les services de promotion de la paix. Pour garantir de tels engagements, il faut pouvoir bénéficier des moyens, des infrastructures et du savoir-faire requis.

Toujours au sein de la Swisscoy, les moyens engagés sont multiples.

Forces aériennes

Le groupe radar mobile FA 2

Lt-col EMG Steven Jauquier
Cdt gr radar mobile FA 2

Le lieutenant-colonel d'Etat-major général Steven Jauquier est le commandant du groupe radar mobile des Forces aériennes 2 depuis 2020. Ce père de deux enfants et commandant des sapeurs-pompiers vit avec sa famille dans le canton de Fribourg. Sur le plan professionnel, le lt-col EMG Jauquier est actif aux Forces aériennes sur la base aérienne de Payerne. Il est chef du Centre de compétence d'exploitation Engineering F/A-18 (CCE) aux Forces aériennes sur la base aérienne de Payerne.

En 2022, vous avez dirigé le groupe radar mobile des Forces aériennes 2 en tant que commandant. Quel lien militaire avez-vous personnellement avec le radar d'aviation tactique (TAFLIR) ?

J'ai été recruté en 2003 comme soldat d'exploitation d'aide au commandement FA et j'ai effectué mon école de recrue à Dübendorf. Après l'instruction générale de base, j'ai rejoint le service technique et c'est là que j'ai vu un TAFLIR pour la première fois de ma carrière. Depuis, il fait partie intégrante de ma vie. Finalement, après ma formation d'officier, j'ai commencé à travailler dans le civil comme mécanicien radar à Payerne en 2006. J'étais responsable de l'exploitation, des travaux de maintenance et des réparations du TAFLIR – j'ai pu appliquer mon savoir-faire militaire.

Vous connaissez donc pratiquement chaque vis du système radar ?

Je dirais plutôt « connaissais ». On oublie vite, et mes derniers travaux sur le TAFLIR lui-même remontent déjà à quelques années. Mais je connais toujours les procédures de prise de position sur le bout des doigts, et je me réjouis à chaque fois que je vois l'antenne tourner sur un emplacement.

Qu'est-ce qui vous fascine tant dans le TAFLIR ? Né en 1985 et introduit en 1987, le TAFLIR ne fait pas vraiment partie des systèmes les plus modernes de l'armée suisse…

Pour comprendre ma fascination en lien avec le TAFLIR, il faut voir la diversité au sein de nos compagnies radar. D'une part, nous avons des personnes qui ont un flair pour la technique et qui s'occupent des différents composants du système et, d'autre part, les soldats de sûreté avec un background d'infanterie assurent l'autoprotection sur une position TAFLIR. Une fonction clé : les chauffeurs poids-lourds, sans lesquels nous ne mettons en mouvement aucun de nos douze véhicules système. Ces différents types de caractères constituent un mélange passionnant.

De plus, notre groupe porte le mot « mobile » dans son nom – nous intervenons donc dans toute la Suisse et sommes confrontés chaque année à une nouvelle situation de départ dans un lieu généralement inconnu, ce qui rend le travail très varié et nous permet de bien connaître la Suisse.

Malgré tout l'amour que je porte au TAFLIR, il n'est plus à la pointe de la technologie, ou alors je me trompe ?

Les données radar que le TAFLIR continue de fournir de manière fiable sont de bonne qualité et complètent l'état de situation aérienne avec des informations supplémentaires importantes. Cette prestation qui nous a été demandée ces dernières années est incontestée au sein de l'armée, ceci a été prouvé à multiples reprises ces dernières années dans le cadre d'engagements. Mais il faut bien sûr constater qu'avec la technique actuelle, les efforts en comparaison à la performance fournie sont disproportionnés. « Mobile » figure certes sur notre badge, mais la compréhension de la mobilité doit être considérée de manière différente dans notre contexte. Nous avons besoin d'une douzaine de camions, d'une compagnie et de longues heures de montage pour mettre le TAFLIR en service. Cela pourrait être nettement plus rapide et efficace avec la technologie actuelle.

Prise de vue lors du CR (2021).

Prise d'emplacement pendant l'exercice COLLOQUID (2021).

Mise en place d'emplacement lors de COLLOQUID (2021).

Engagement de l'URC22 à l'emplacement No. 2 (2022).

Quand le TAFLIR sera-t-il retiré du service ?

La roadmap actuelle prévoit la mise hors service du TAFLIR à la fin de l'année 2025. Cela fait près de 15 ans que j'entends parler de tels horizons en ce qui concerne le TAFLIR, et peu de choses ont changé jusqu'à présent. Mais j'espère bien sûr qu'il sera remplacé le plus rapidement possible. Un avant-projet de remplacement du TAFLIR est actuellement en cours.

Comment devrait-on s'imaginer un TAFLIR de la génération actuelle ?

Un système futur devrait tenir compte de la conception moderne de la « mobilité ». Il devrait être opérationnel en une heure, pouvoir être exploité par une section et ne comprendre qu'un, voire deux véhicules système au maximum. Au lieu de manœuvrer des tonnes de matériel sur une colline éloignée et d'exploiter le TAFLIR de manière plus ou moins stationnaire pendant plusieurs jours, comme c'est le cas actuellement, plusieurs systèmes pourraient être mis en service en parallèle. Pendant qu'un système est opérationnel, un autre se met en place et prend la relève du premier, qui change ensuite d'emplacement. En termes de flexibilité et d'autoprotection, nous serions dans un tout autre monde.

L'engagement en faveur de la « Ukraine Recovery Conference 2022 » à Lugano en juillet 2022 a été le dernier engagement en tant que groupe autonome jusqu'à nouvel ordre (voir article ci-contre), une bonne décision de votre point de vue ?

Pour un engagement des Forces aériennes, toutes les prestations doivent être réunies, il est donc certainement judicieux d'opérer avec des formations d'engagement mixtes. Auparavant, trop de groupes étaient engagés en parallèle et « un secteur, un chef, une mission » ne pouvait pas être mis en œuvre de manière optimale. Mais il est clair que cela me fait mal au cœur que mon groupe soit divisé. Au cours des dernières années, nous avons pu développer un énorme savoir-faire au sein de l'état-major et des compagnies qui est maintenant en partie dispersé. Je reste par contre persuadé que la prestation TAFLIR sera apportée d'une manière compétente, que les données seront de qualité et fournies dans les délais impartis.

« PA CAPONA »

S. J.

© VBS/DDPS – Jonas Kambli

Forces aériennes

L'illustre TAFLIR (1985-202 ?)

Divisionnaire Peter Merz
Commandant des Forces aériennes

Le groupe radar mobile des Forces aériennes 2 exploite le radar d'aviation tactique TAFLIR avec ses deux compagnies. Acquis en 1985, ses performances demeurent incontestées 37 ans plus tard.

Le TAFLIR assure en premier lieu la surveillance de l'espace aérien suisse. Ce n'est certes pas le seul moyen d'établir une image de la situation aérienne, mais au vu de ses engagements annuels, il représente une pièce importante du puzzle qui compose la surveillance de l'espace aérien. Les stations radar militaires (MRS) installées sur divers sommets suisses surveillent l'espace aérien supérieur. Toutefois, malgré leur positionnement en altitude, ces MRS ne peuvent surveiller l'espace aérien inférieur que de manière partielle. La topographie de notre pays les empêche de voir dans les vallées. On parle alors d'« ombres radar » – des zones où la surveillance de l'espace aérien est aveugle.

Le radar d'aviation tactique TAFLIR couvre les ombres radar dans les vallées. Lorsqu'exploité par une compagnie radar mobile des Forces aériennes, sa mobilité permet de le positionner en fonction des besoins et du secteur d'engagement. La portée de son radar comble la zone d'ombre pouvant se créer entre les MRS et les capteurs de la défense antiaérienne, ces derniers ne disposant que d'une portée relativement faible. Les données du TAFLIR sont intégrées en « live » à l'établissement de l'image de la situation aérienne. Le TAFLIR constitue un pilier important de la sécurisation de l'espace aérien suisse, par exemple lors d'engagements en faveur de conférences internationales.

Le TAFLIR à l'engagement

Les compagnies radars mobiles sont engagées chaque année. L'engagement en faveur du World Economic Forum (WEF) de Davos est un point fixe dans l'agenda de chaque soldat TAFLIR. S'y ajoutent de nombreuses autres conférences réunissant dirigeants économiques et premiers ministres de divers pays, et dont la Suisse doit assurer la sécurité au nom du droit international. Aucune lacune ne peut dès lors être tolérée dans la surveillance de l'espace aérien. La Suisse démontre ainsi ses capacités à organiser de tels événements d'ampleur internationale et à assurer ses bons offices. Le groupe radar mobile des Forces aériennes 2 a ainsi été engagé dernièrement en faveur du sommet qui a réuni Vladimir Poutine et Joe Biden à Genève en été 2021 ainsi qu'au profit de la « Ukraine Recovery Conference 2022 » qui s'est tenue au Tessin en juillet dernier.

Bien que le TAFLIR soit en service depuis 35 ans, sa contribution assurée par les compagnies radars mobiles des Forces aériennes est indispensable. L'Armée suisse ne dispose actuellement d'aucun système suffisamment mobile et performant pour combler durablement les lacunes en termes d'imagerie aérienne conformément au cahier des charges requis par les missions qui lui sont confiées. Il serait par exemple disproportionné de surveiller l'espace aérien d'un site de conférence pendant plusieurs jours uniquement avec des avions. Les charges en pilotes, en personnel au sol, en avions et en entretien seraient énormes. Certes, le TAFLIR, du haut de ses 35 ans, n'est plus *state of the art*, mais l'Armée suisse ne dispose actuellement d'aucune alternative équivalente.

Les dépendances augmentent

En raison de l'utilisation intensive de ce système lors d'engagements et par les écoles de recrues à des fins de formation, les coûts d'exploitation augmentent. Entretemps, l'appui de fournisseurs de prestations civils tels que RUAG est devenu indispensable pour assurer le bon fonctionnement du système. Après 35 ans d'utilisation, la technique est de plus en plus sujette à des pannes et le support de certains composants du système est de plus en plus difficile à assurer.

Exercice de l'escadrille 11 sur la base de Meiringen.
Photos © Markus Müller.

Entre-temps, le nombre d'instructeurs capables de former les conducteurs pour le véhicule le plus important du système, le véhicule-antenne Saurer 10DM, se réduit naturellement. L'alimentation en chauffeurs de ce type de camion devient, au fil des années, un défi.

Mise hors service en 2026 et perte de savoir-faire ?

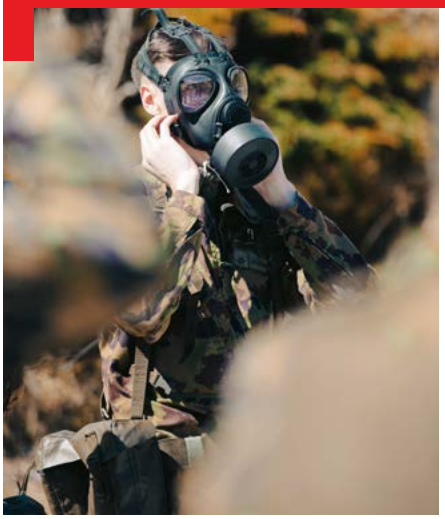
Il est prévu de mettre le TAFLIR hors service à la fin de l'année 2025. On ne sait toutefois pas si cela se fera effectivement (voir à ce sujet l'interview du commandant du groupe radar mobile des Forces aériennes 2). Chaque année, l'Armée suisse a besoin du TAFLIR dans le cadre de ses engagements, mais ne lui connaît encore aucun successeur. Un avant-projet est en cours pour formuler le catalogue des capacités de son futur remplaçant.

En revanche, les premières mutations organisationnelles sont d'ores et déjà mises en œuvre au sein de la brigade d'instruction et d'entraînement des Forces aériennes. Ces mesures organisationnelles ne sont certes pas directement liées à l'arrivée d'un successeur au TAFLIR, mais elles sont prises pour tenir compte de la demande en continuelle croissance pour des données radar supplémentaires. Aussi, en 2023, les membres du groupe radar mobile des Forces aériennes 2 seront répartis entre les groupes de renseignements des Forces aériennes 1 et 2. Ainsi, l'engagement de différents capteurs sera conduit par une seule et même structure, ce qui est à saluer au regard du principe « un secteur, un chef, une mission ». De plus, la brigade gagnera en liberté d'action lorsqu'il s'agira de mener d'autres missions que celle du WEF.

Cette redistribution des militaires rend d'autant plus urgente une relève rapide. Bientôt, les connaissances du système et surtout l'expérience acquise par les officiers et sous-officiers dans l'état-major lors des engagements ne seront plus que difficilement disponibles pour les compagnies. Sans ce maintien du savoir-faire, essentiel pour l'engagement du TAFLIR, celui-ci ne serait que partiellement opérationnel et il faudrait s'accommoder d'une lacune dans la protection de l'espace aérien en temps de paix ; ce qui n'est pas envisageable pour une armée digne de ce nom. Et il n'est pas certain que les capteurs de la défense aérienne basée au sol puissent combler cette lacune à eux seuls.

Comme nous l'avons mentionné en début d'article, c'est précisément en cas de défense que l'engagement tactique et la décentralisation revêtent une importance décisive. C'est d'ailleurs ce que démontrent les récents événements en Ukraine : faute de pouvoir être déployés de façon mobile, ces systèmes clés sont mis hors-jeu en peu de temps. Sans une protection efficace contre les attaques aériennes, la défense du pays dans un environnement opérationnel moderne est au mieux fortement compliquée, au pire impossible.

P. M.



Transmissions

Nous rendons le *leadership* possible – Connexion à tout prix

Lt-col Gian-Reto Schmidlin
Cdt bat ondi 4

Nous, le bataillon d'ondes dirigées 4 (bat ondi 4) de la brigade d'aide au commandement 41/SIS, disposons d'un large éventail de moyen. La devise de notre bataillon est « Nous relions et rendons possible la conduite – dans toutes les situations ». C'est avec ce credo que plus de 1'500 militaires (mil) accomplissent chaque année leur service au sein du bat ondi 4.

Marche d'entrée le premier jour du cours de répétition (CR). La compagnie s'est rendue dans la belle ville d'Andermatt dans des conditions météorologiques parfaites.

Le bat ondi 4 fournit plusieurs prestations de service. Nos troupes raccordent au réseau de conduite suisse principalement des unités et des installations de conduite. En outre, le bataillon est en mesure d'assurer la protection terrestre de ses propres installations, ainsi que l'exploitation et la sécurisation des stations radar. Pour ce faire, le bat ondi 4 peut relier plusieurs centaines de kilomètres carrés de cellules radio ou d'installations de conduite au réseau de commandement suisse.

Le bataillon est en mesure de sauver ses propres troupes (p. ex. des blessés) dans des installations, d'éteindre des incendies et d'évacuer une installation en cas d'urgence. En outre, leur domaine d'intervention s'étend à des spécialités telles que la recherche en cas d'incident en lien avec des avalanches, d'escalade ou de randonnées.

Une autre particularité du bat ondi 4 sont les soldats de système de transmission à larges bandes (BBUS) qui entretiennent le réseau de conduite suisse et relient les différents nœuds par ondes dirigées. Ces spécialistes travaillent en étroite collaboration avec les pionniers d'ondes dirigées, qui s'occupent de l'aspect technique des deux côtés de la liaison.

Les troupes de sûreté, qui peuvent sécuriser les installations en altitude, constituent un autre élément important. Elles assurent la protection terrestre et font monter en puissance le dispositif de sécurité des installations.

Il ne faut pas oublier les autres fonctions qui contribuent considérablement aux capacités de notre bataillon telles que les logisticiens, les équipes de cuisine, les soldats de service et les ordonnances de bureau.

Comme on peut aisément le constater, notre contribution est décisive pour le succès de chaque engagement. Sans communication, aucun avion ne vole, aucun char ne roule et aucun commandant ne conduit. C'est pourquoi les

Notre PC a été monté le plus rapidement possible à l'aide d'ordonnances de bureau.

Transport aérien du matériel du bat ondi 4 vers les emplacements éloignés de la Patrouille des glaciers.

Nos spécialistes d'exploitation des installations en altitude ont été formés à l'utilisation des téléphériques.

prestations de notre bataillon sont disponibles en l'espace de quelques jours après une mobilisation. En tant que formation de milice à disponibilité élevée, nos militaires sont en mesure d'entrer rapidement en service et de remplir leur mission en cas de mobilisation.

Avec plus de 80 fonctions différentes, le bat ondi 4 est multitalent et, grâce à son important effectif, l'un des plus grands bataillons de l'armée suisse.

Engagement PdG 2022

La Patrouille des Glaciers (PdG) est l'une des plus grandes compétitions de ski de randonnée en patrouille d'Europe. C'est à trois que les sportifs ambitieux s'attaquent au parcours de 57,5 km et franchissent 4'386 mètres de dénivelé. La compétition est organisée par l'armée et attire de nombreux sportifs nationaux et internationaux. Des passionnés de ski de randonnée viennent de 35 pays pour s'affronter de Zermatt à Verbier en passant par Arolla. Entre-temps, la PdG s'est forgée une bonne réputation et la population civile suit également les courses avec beaucoup d'intérêt.

Pour qu'un tel événement sportif puisse se dérouler avec le dispositif de sécurité nécessaire, de nombreuses précautions doivent être prises. Cette année, le bat ondi 4 a également pu contribuer à la réussite de la PdG.

Grâce à nos liaisons, nous avons permis une couverture réseau complète sur le parcours de la randonnée. En collaboration avec Swisscom, des antennes 4G ont été installées en haute montagne pour permettre l'envoi d'appels d'urgence par téléphone portable et pour le chronométrage. En plus de la couverture réseau normale, toutes les patrouilles étaient équipées d'un tracker GPS qui indiquait en permanence leur position via le réseau 4G. Ainsi, les proches et le grand public ont pu suivre les sportifs en temps réel sur le site web de la PdG ou sur l'application dédiée.

Les membres du bat ondi 4 se sont installés à différents endroits sur les sommets le long du parcours de la course. A chaque emplacement, la situation de départ était différente : Cela allait des routes enneigées aux remontées mécaniques, en passant par des endroits tout simplement inaccessibles autrement que par hélicoptère. Heureusement, le credo bien connu des pionniers des faisceaux hertziens nous a aidés : « Connexion à tout prix ».

Nous avons fait tout ce qui était en notre pouvoir pour rendre la communication possible. En effet, nos connexions et la couverture réseau qui en découlait étaient décisives pour l'événement. Sans nos performances, les courses ne pouvaient pas démarrer. Nos soldats étaient donc toujours conscients de la responsabilité qu'ils devaient assumer – et l'ont assumée avec brio.

En outre de la collaboration avec Swisscom, nous avons également travaillé de manière intensive avec le commandement de la PdG. Des officiers expérimentés

issus de divers horizons ont coordonné l'engagement de l'armée lors de la Patrouille des Glaciers. Grâce à notre officier de liaison, nous avons pu intégrer directement nos connaissances techniques à la planification, simplifiant ainsi considérablement la communication entre l'état-major d'engagement PdG et l'état-major du bat ondi 4.

La PdG a été un franc succès et les sportifs ont réalisé des performances impressionnantes. Nous espérons avoir prochainement l'occasion d'effectuer un engagement aussi passionnant !

Engagement ARAMIDE AIUTO TUTTO 22

En plus de ces deux engagements, le bat ondi 4 a fourni cette année d'autres prestations au profit de tiers. La division territoriale 2 (div ter 2) s'est exercée avec son bataillon d'état-major, ainsi que l'ensemble de l'état-major d'urgence. Ils ont dû donc déplacer l'ensemble de leur quartier général. Cela peut paraître banal – mais c'est un véritable défi lorsqu'il s'agit de conserver à tout moment la souveraineté en matière de commandement et de décision.

L'état-major de la division territoriale 2 est le lien entre l'armée et les autorités civiles. Il intervient par exemple en cas de black-out, d'inondations et d'autres catastrophes naturelles, lorsque la demande leur en est faite par les communes ou les cantons. La div ter 2 effectue des engagements dans son secteur du type AIDER – PROTEGER – LUTTER.

Le bat ondi 4 a été engagé pour assurer la capacité de conduite de l'état-major de la div ter 2. Nous avons établi et sécurisé d'importantes liaisons de communication. L'exercice a donc été un exemple parfait de ce que peut être notre mission en tant que bataillon. Un fait en passant : nous pouvons même établir nos liaisons au-delà des obstacles en utilisant des relais à ondes dirigées lorsque nous ne pouvons pas communiquer directement avec le réseau de commandement suisse. C'est par exemple ce qui s'est passé lors de cet exercice (voir photos).

L'exercice s'est très bien déroulé et nous avons pu soutenir l'état-major de manière optimale.

Engagement ALPA ECO 22 SOMMER AE22-S

Le bat ondi 4 participe régulièrement à l'engagement susmentionné. Nous fournissons des prestations en faveur des formations qui assurent la sécurité du World Economic Forum (WEF) à Davos.

Le WEF est un événement qui attire à Davos des représentants d'entreprises privées et semi-privées du monde entier. Des thèmes d'avenir y sont discutés, des entrevues au plus haut niveau y sont tenues et des informations sont échangées. La rencontre attire des représentants de la politique et de l'économie du monde entier. La Suisse est tenue par le droit international de protéger ces personnes et de préserver sa souveraineté aérienne.

Normalement, le WEF a lieu en janvier. Cependant, en raison de la pandémie Covid-19, l'événement a dû être reporté ou annulé à plusieurs reprises. En 2022, le forum a de nouveau été organisé au printemps à Davos.

L'environnement printanier de la rencontre a toutefois entraîné de tout nouveaux défis pour les troupes impliquées. Par exemple, les cols normalement recouverts de plusieurs mètres de neige étaient praticables sans problème ou les zones marécageuses – qui servaient d'aires d'atterrissage pour les hélicoptères en hiver – étaient dégelées. Cette mission a donc exigé de toutes les troupes une nouvelle planification, de la flexibilité et de l'inventivité. Mais avec le recul, on peut dire que ces bons préparatifs en valaient la peine.

Dans cet engagement exemplaire, le bat ondi 4 avait une fonction similaire à celle d'un opérateur télécom. Nous avons relié toutes les formations participant à cet engagement et avons permis aux organes de conduite de transmettre sans problème les données, ainsi que les communications orales, ce de manière cryptée et à large bande.

Les formations les plus diverses ont été engagées lors du World Economic Forum. Cela allait des forces aériennes avec leurs éléments de transport aérien et de défense antiaérienne jusqu'aux capteurs. En outre, des unités d'infanterie et des formations logistiques ont été rattachées.

L'engagement de l'armée a également été démontré dans le passé du WEF ! Il est arrivé à plusieurs reprises que des personnes non autorisées tentent de se procurer un accès au site ou que des avions non déclarés pénètrent dans l'espace aérien du WEF. De tels incidents renforcent l'importance de notre engagement.

Lors de cet engagement, l'Armée suisse a mobilisé plus de 5'000 militaires qui ont veillé 24 heures sur 24 au bon déroulement de l'événement. Pour notre part, nous avons pu remplir notre mission et remercions tous les membres du bat ondi 4 pour leur contribution à la bonne marche de l'événement.

G.-R. S

Un R-905 sur un site relais quelque part en Suisse.

Notre adjudant d'état-major lors des festivités à Zermatt pour la PdG. Une photo devant le Cervin était bien entendu indispensable.

Le directeur de l'exercice de formation avait toujours le contrôle des actions par radio et guidait sa troupe à travers les différentes phases.

Ce R-905 permettait de relier la vallée à l'antenne du réseau 4G sur la PdG.

Les spécialistes des installations d'altitude sont également formés et entraînés à la lutte contre les incendies.

Un site mobile quelque part en Suisse.

Deux soldats doivent porter le matériel pour une liaison hertzienne sur quelques mètres.

Une compagnie a entraîné l'interaction entre les éléments de sûreté et de sauvetage lors d'un entraînement en formation.

Une autre liaison a été mise en place dans le cadre de l'exercice AAT22.

Transmissions

S'exercer en engagement

Lt-col Roger Haupt
Cdt bat ondi 16

Auteur : Romain Wanner

Un bataillon d'ondes dirigées tel que le bat ondi 16 effectue très régulièrement des prestations pour le compte de tiers, que ce soient les autorités civiles d'un canton, des événements locaux (WEF ou PdG) ou simplement d'autres unités de l'Armée Suisse. Un bon exemple ? La participation du bat ondi 16 à l'exercice RHODANUS !

Rares sont les cours de répétition axés à 100% sur la formation pour un bataillon d'ondes dirigées comme le bat ondi 16. En effet, les compétences des troupes télématiques, véritables opérateurs en télécommunication de l'Armée, sont toujours plus demandées, tant par les autorités civiles, qui apprécient de mettre à l'épreuve la connectivité des différents systèmes, que par d'autres unités de l'Armée Suisse. Tous peuvent ainsi tester un mécano en conditions réelles, avec des télécommunications (téléphone, fax et données) 100% militaires.

Ainsi, lorsque le bat ondi 16 part en exercice, c'est souvent en tant que prestataire de service et non pas en tant que troupe en formation. Dès lors, l'échec n'est pas envisageable, sans quoi c'est la faisabilité même de l'exercice qui tomberait à l'eau. Le bataillon s'est notamment illustré lors de l'exercice RHODANUS qui, lors de l'automne 2021, a rassemblé pas moins de cinq bataillons de la brigade mécanisée 1.

Un challenge télématique

« C'était un challenge », commente le lt-col Roger Haupt, commandant du bat ondi 16. *« La zone d'engagement était particulièrement grande : ça nécessitait beaucoup de liaisons et un réseau assez complexe ! Nous avons toutefois pu engager notre système avec succès, tant le RITM (réseau intégré de télécommunications militaires) que les interfaces RAP (radio access point) au profit de la brigade mécanisée 1. »*

« La durée de l'exercice, qui s'est étiré sur plus d'une semaine, était aussi un défi pour notre bataillon. Nous en avons tiré quelques leçons, notamment dans la façon de gérer les différentes phases d'un exercice d'une telle envergure et sur la façon d'adapter nos liaisons aux changements d'emplacements et au temps imparti pour obtenir des liaisons lors d'un déplacement. »

Un autre challenge que le bataillon a rencontré n'était autre que celui d'avoir suffisamment de spécialistes aux points clés de son réseau : *« Pendant RHODANUS seul 54% de l'effectif complet du bataillon était en service. Cela a complexifié passablement l'engagement, à tous les niveaux. De nos jours, la gestion des effectifs est chaque année un plus gros défi ! Et ce n'est pas une fois en service que l'on peut trouver une solution à ce problème… »* Mais c'est peut-être du côté des cantons, qui sont responsables des demandes de déplacement de service, qu'il y aurait quelque chose à faire.

Un exercice, plusieurs systèmes

L'élément clé pour une mission au sein d'un bataillon d'ondes dirigées, est de monter un réseau. Par contre, savoir ce qui va transiter par le réseau et comment le connecter, ce n'est pas forcément toujours évident.

Dans le cas de RHODANUS, c'est principalement le système SIC (système de conduite et d'information), plus connu sous son appellation alémanique FIS HE, le système de conduite des Forces terrestres, qui aura passé au travers des liaisons du bat ondi 16. Ce système d'aide à la conduite, qu'on pourrait comparer à un intranet de conduite relié à tous les postes de commandement, a permis à la brigade mécanisée 1 d'échanger des informations, de l'échelon brigade à celui des troupes sur le terrain, que ce soit sous la forme d'ordres, d'images ou au moyen de la carte de suivi de situation.

C'est au moyen d'antennes à ondes dirigées R-905 que le bat ondi 16 connecte les différents emplacements à son réseau.

Mais là où RHODANUS a poussé encore plus loin la connectivité, c'est qu'il aura fallu interconnecter le réseau télématique, le système SIC FT et le village de containers. Cette combinaison des trois réseaux était, pour le bat ondi 16, une grande première. Résoudre tous les problèmes posés par ces difficultés techniques n'aura pas été simple, mais très formateur.

Etre engagés pour apprendre

Contrairement à bon nombre de troupes, les ondes dirigées vont presque apprendre davantage sur un engagement que sur un exercice organisé à l'interne du bataillon. La raison est simple : c'est dans la complexité d'un réseau et dans les besoins particuliers des divers « clients » du bataillon, tant civils que militaires, que viendra la difficulté pour un bataillon d'ondes dirigées et avec ça un apprentissage riche et varié, que ce soit au niveau de la troupe ou des membres de l'état-major.

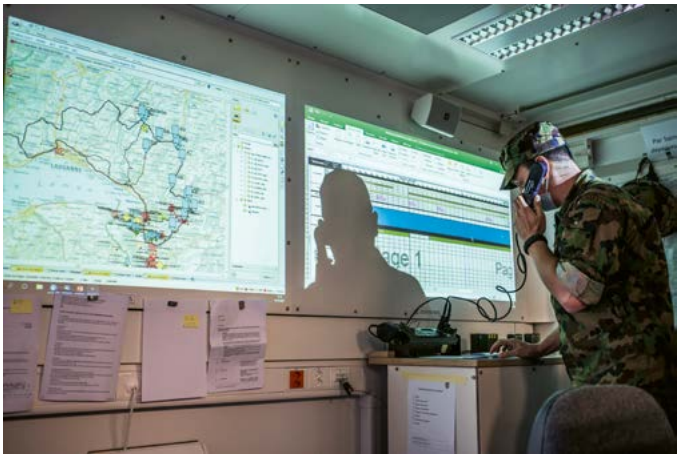
Cela demande systématiquement de résoudre des problèmes de connectivité ou de processus parfois inconnus au niveau des parties prenantes. Les conclusions tirées de tel problème sont essentielles pour qu'à l'avenir, ceux-ci ne se reproduisent plus.

Dès lors, tous les engagements sont bons à prendre. Et, pour l'instant, le bat ondi 16 n'a jamais failli une mission. « Sans nous, rien ne va » fut un temps sa devise, remplacée désormais par un motto plus vif : « Connectés dans l'action ».

R. H.

Sûreté rapprochée d'un char RAP du bat ondi 16 intégré à l'infrastructure de conduite mise en place par le bataillon d'état-major de la brigade mécanisée 1.

Un des défis de RHODANUS aura été de connecter les divers emplacements de l'exercice au village de container dans lequel se trouvait le PC de la direction d'exercice (DIR EX).




Y. WISMER

Politique de sécurité

Salutations et remerciements du canton de Zurich

Conseiller d'Etat Mario Fehr PS / ZH
Directeur militaire du canton de Zurich

Ces dernières années en particulier, l'armée et ses membres ont prouvé à maintes reprises leur mission de protection et de soutien de la population : Un grand merci pour tous vos services, votre flexibilité et votre grand travail !

Le canton de Zurich ainsi que moi-même, en tant que directeur militaire, sou-tenons l'armée. Au contact de la population, je constate régulièrement la grande sympathie et le soutien dont bénéficie l'armée. Des événements tels que les cérémonies de promotion, les prises d'étendard et de drapeau ainsi que la visite de différents corps de troupe constituent une part importante de mon agenda.

Le canton de Zurich est le « canton parrain » de 11 bataillons et groupes. Il s'agit de bataillons d'infanterie, de logistique et mécanisé, ainsi que du bataillon QG 11, l'un des bataillons de la br aide cdmt 41/SIS. J'aurai l'occasion de rendre visite aux membres du bat QG 11 cette année encore et je m'en réjouis d'ores et déjà.

Ces visites à la troupe sont très importantes pour moi et les impressions que j'en retire me laissent toujours un bon souvenir. Cette année, j'ai notamment pu rendre visite à des parties du bat PM 4 lors du World Economic Forum (WEF) à Davos. La compagnie de police militaire engagée a assuré la sécuri-té des participants au WEF. La collaboration exemplaire entre l'armée et les autorités civiles fait ses preuves depuis de nombreuses années et elle est in-dispensable à la sécurité de tous les participants.

En novembre dernier, j'ai été invité à la cérémonie de promotion de l'EO aide cdmt 30 et j'ai pu saluer les nouveaux officiers de toute la Suisse.

La décision d'aller plus loin sur la voie militaire que la personne moyenne m'impressionne. En devenant officiers, les jeunes militaires assument des responsabilités supplémentaires – pour eux-mêmes et pour les autres. En plus de leur profession et de leur formation. L'engagement pour l'armée mérite bien entendu une grande reconnaissance, quel que soit le grade ou la mission.

L'armée fait partie de notre pays, des cantons, des communes et des villes. En même temps, le soutien de la population est la base d'une armée performante et forte. Et c'est en grande partie grâce à vous, les militaires.

L'armée fait actuellement l'objet d'une attention différente qu'elle ne l'était il y a peu de temps: de nombreux réfugiés d'Ukraine cherchent également refuge en Suisse. L'Ukraine est en Europe, tout comme nous. Tout ce conflit montre sans relâche ce qui est nécessaire : Pour notre armée. Pour notre sécurité. C'est pourquoi je continuerai à m'y engager au quotidien en tant que directeur militaire !

M. F.

REY GROUP

HÔTEL & IMMOBILIER
GENÈVE

LOCATION D'APPARTEMENTS - HÔTELS ET RÉSIDENCES - PROMOTION IMMOBILIÈRE

REY GROUP CRÉATEUR DE LIEUX DE VIES

DEPUIS PLUS DE 50 ANS

REY GROUP participe à des opérations immobilières d'envergure et s'est aussi spécialisé dans la location d'appartements meublés. En parallèle, il propose des hôtels résidences via sa filiale Rey Hôtels & Résidences : Drake Longchamp*** sur la rive droite et Sagitta*** sur la rive gauche***

info@reygroup.ch
+41 (0)22 731 53 40