L'Armée suisse dans le cyberespace et l'espace électromagnétique : une longueur d'avance

Autor(en): **Vuitel, Alain / Castelberg, Lorena**

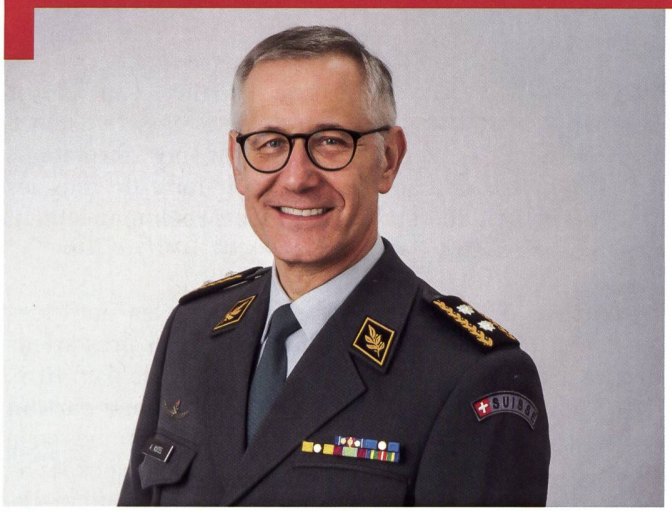
Objekttyp: **Preface**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2022)**

Heft [2]: **Numéro Thématique 2**

PDF erstellt am: **22.07.2024**



© 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.