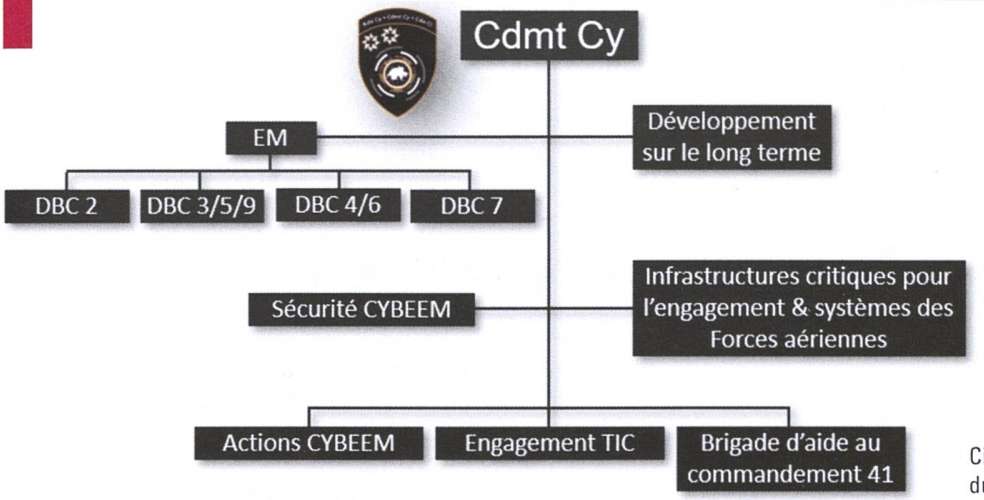
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2023)
Heft: 5

Artikel: Le système nerveux central de l'armée
Autor: Vuitel, Alain
DOI: https://doi.org/10.5169/seals-1055308



Ci-contre : Structure simplifiée du Commandement Cyber.

Cyber

Le système nerveux central de l'armée

Divisionnaire Alain Vuitel
Chef Projet Commandement Cyber

Une armée est comme un être humain. Pour agir, elle a besoin d'un système nerveux central qui connecte ses organes sensoriels – ses capteurs – avec ses membres – ses effecteurs. La qualité et la rapidité de fonctionnement de cet ensemble conditionne le succès à l'engagement. Privée de tout ou partie des fonctionnalités de son système nerveux central, une armée se voit atteinte d'un grave handicap qui la paralyse complètement ou, pour le moins, péjore notablement sa capacité d'agir en un tout cohérent ; indépendamment de la qualité individuelle des divers éléments qui la composent.

L'espace cyber et électromagnétique (CYBEEM) constitue le substrat sur lequel ce système nerveux central est aujourd'hui bâti et constamment nourri ; il innerve toutes les sphères d'opérations et autorise ainsi la conduite multi-domaine. Il constitue dès lors un espace décisif qu'il convient de contrôler en tout temps pour permettre la mise en réseau de nos capteurs avec nos effecteurs au travers de la boucle OODA (observer, évaluer, décider et agir[1]).

Ses attributs lui confèrent de plus une aptitude marquée comme source de renseignement d'une part et comme élément de manœuvre d'autre part en agissant directement sur l'une ou l'autre partie du système nerveux central de l'adversaire pour le paralyser ou restreindre sa capacité d'action. Cette importance cruciale du CYBEEM en fait un espace de confrontation par excellence et ceci dès la situation normale, 24 heures sur 24, 365 jours par an.

Les attributs du CYBEEM

Les caractéristiques fondamentales du CYBEEM lui confèrent quatre attributs clés :

- **Porosité** : que ce soient les acteurs (activistes, cybercriminels, « mercenaires cybers » ou unités CYBEEM militaires), les technologies (hardwares et softwares), les vecteurs (fournisseurs de services) ou encore les cibles, le CYBEEM est un domaine perméable entre les domaines civils et militaires. Cette porosité complique la lutte contre les cybermenaces. La coopération public-privée ainsi qu'avec les partenaires internationaux est primordiale, couplée au développement de ses propres outils IT forensiques, sur mesure, pour pouvoir détecter, comprendre et contrer des attaques CYBEEM de manière indépendante et sur la durée.

- **Temporalité** : le CYBEEM est ouvert tous azimuts et fait l'objet d'interférences permanentes pour tenter d'y gagner un avantage. Bien avant le déclenchement d'un conflit ouvert, les parties impliquées cherchent à y créer des conditions favorables pour leurs actions ultérieures, indépendamment de leur mode d'action, classique ou/et dans le CYBEEM. Si les actions qui s'y déroulent nécessitent un temps de préparation plus ou moins long, le déploiement de leurs effets peut être foudroyant. En conséquence, le CYBEEM se doit de disposer de permanences, qu'il s'agisse de veille pour s'assurer que les systèmes-clés fonctionnent ou de disponibilité pour mener des contre-actions.

- **Versatilité** : rien n'est acquis dans le CYBEEM où les transformations interviennent constamment et très rapidement. Dans le domaine électromagnétique, les nouvelles technologies civiles permettent l'échange rapide de données, par exemple avec la 5G. Dans le domaine cyber, le développement de l'intelligence artificielle révolutionne la façon de concevoir le rôle de la machine.

- **Ubiquité** : dans le CYBEEM, le lieu géographique revêt une dimension à la fois importante et futile. Importante, car dans le domaine électromagnétique, la localisation

[1] John Boyd (1976). *Destruction and Creation*. U.S. Army Command and General Staff College.

de l'attaquant et de sa cible détermine les moyens mis en œuvre (fréquence, intensité du signal, etc.). Futile, car dans le domaine cyber, un accès Internet permet de mener des attaques depuis n'importe où dans le monde.

Fortes de ces attributs, les actions dans le CYBEEM se déclinent en trois phases. La première consiste à assurer le savoir et la capacité de décision grâce à la mise à disposition, en toutes circonstances, des prestations CYBEEM (y inclus TIC, Technologies de l'information et de la communication) en tant que moteur du système nerveux central. La seconde phase a pour but d'élargir ce savoir et cette capacité de décision grâce à l'acquisition de renseignements-clés.

Enfin, la troisième phase vise à paralyser l'adversaire, en se focalisant sur la manœuvre plutôt que l'application brute de la force. Il s'agit de l'approche manœuvriste des opérations décrite par John Kiszely.[2] Elle a pour but de briser la cohésion globale de l'adversaire et sa volonté de combattre, plutôt que son matériel. Elle repose sur l'attaque des systèmes de commandement et de contrôle (C2) de l'adversaire, nécessitant ainsi d'appliquer à ces actions un tempo élevé et un haut degré de simultanéité.

Le commandement Cyber, des prestations uniques au sein d'un réseau national

En Suisse, la lutte contre les cybermenaces concerne un nombre croissant d'acteurs fédéraux ou cantonaux. On y distingue trois domaines qui sont la cyberdéfense (commandement Cyber, Service de renseignement de la Confédération), la cybersécurité (Centre national pour la cybersécurité) et la poursuite pénale visant la cybercriminalité (polices et ministères publics cantonaux, Police fédérale, Ministère public de la Confédération).

Loin de faire cavalier seul, les missions du commandement Cyber, héritier de la Base d'aide au commandement, s'inscrivent donc dans des stratégies nationales régulièrement mises à jour pour répondre aux développements de la menace et inclure les retours sur expérience. On peut par exemple citer le *Rapport sur la politique de sécurité ou la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)* ainsi que l'Orientation à long terme de l'armée « *Zielbild 2030+* » et la *Conception générale cyber (CG cyber).*

Les prestations CYBEEM du commandement Cyber sont soumises à des bases légales[3] et un contrôle permanent d'instances fédérales dédiées. Cette particularité s'explique par la nature même des actions CYBEEM qui incluent notamment des prestations pour le domaine du renseignement.

[2] Major General John Kiszely MC (1998) « The meaning of manoeuvre », *RUSI Journal.*

[3] Il s'agit notamment de la Loi fédérale sur le renseignement (LRens ; RS 121), l'Ordonnance sur la guerre électronique et l'exploration radio (OGE ; RS 510.292) et l'Ordonnance sur la cyberdéfense militaire (OCMil ; RS 510.921).

Pour une structure tournée vers l'engagement au quotidien

Le commandement Cyber comprend un état-major militaire classique incluant les domaines de base de conduite (DBC) 2 à 7. Une des particularités du commandement Cyber est l'importance accordée au développement sur le long terme avec une unité dédiée, directement subordonnée au remplaçant du chef commandement Cyber. Le domaine de prestations comprend les Actions CYBEEM, l'Engagement des technologies de l'information et de la communication ainsi qu'une large composante de milice avec la Brigade d'aide au commandement 41. Ces unités sont secondées par la Sécurité CYBEEM ainsi que les Infrastructures critiques pour l'engagement et les systèmes des Forces aériennes.

Ligne de défense essentielle, le commandement Cyber assure en permanence la veille et la protection des systèmes informatiques critiques pour l'engagement de notre armée et de ses partenaires.

A. V.