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

Artikel: Le cyberespace et l'espace électromagnétique
Autor: Michaud, Laurent
DOI: https://doi.org/10.5169/seals-1055307

Cyber

Le cyberespace et l'espace électromagnétique

Commandant de Corps Laurent Michaud
Chef du Commandement des Opérations

Après les articles sur les sphères d'opération sol, aérienne et orbitale, nous quittons le domaine des espaces géographiques pour nous intéresser aux espaces non-géographiques. Ce sont les espaces dématérialisés où l'Homme peut produire des effets, mais ne peut pas se déplacer.

Cet article traitera spécifiquement du cyberespace et de l'espace électromagnétique (CYBEEM). Il va de soi que l'un et l'autre sont intrinsèquement dépendants de la technologie qui les rend possibles. Ce sont de fait des espaces créés par l'ingéniosité de l'Homme lorsqu'il a réussi à maitriser les ondes. Ils sont donc relativement récents dans la conduite de la guerre par rapport aux autres espaces d'opération, à l'exception peut-être de l'espace orbital.

Nous pourrions traiter ces deux espaces séparément mais ce serait omettre le fait qu'ils sont intimement liés puisque l'un est le médium technologique permettant la fonctionnalité de l'autre. En effet, le cyberespace comprend tous les systèmes informatiques que les sociétés utilisent et exploitent, ainsi que les données qui y sont traitées. Une grande partie de celles-ci sont transmises par radio dont les ondes se propagent au travers de l'espace électromagnétique. Sans ondes et sans électricité, pas de cyber.

Du télégraphe...

Les révolutions industrielles puis technologiques ont permis dès le XIX^{e} siècle d'utiliser les ondes comme moyen de communication. Cela a bien entendu rapidement eu un impact important sur la conduite de la guerre. Grâce au télégraphe, puis à la radio, le chef militaire a pu déléguer la conduite des opérations aux commandants de terrain. La vitesse de communication a permis de mener des batailles, non plus de manière séquentielle mais en parallèle, et de faire porter l'effort d'un théâtre à un autre très rapidement. Les ondes ont permis d'agrandir les secteurs d'engagement, d'assurer une liaison plus étroite avec les organes de conduite et de disposer de représentations continues de la situation pour réduire considérablement les cycles de décision. Au-delà des transmissions, les ondes servent également aux capteurs, radars et senseurs permettant les activités de surveillance, d'exploration et de reconnaissance.

Les capacités dans l'espace électromagnétique peuvent servir à compenser des points faibles et une infériorité technique dans d'autres espaces. Elles peuvent être la condition même de toute production et synchronisation d'effets au sol, sur mer ou dans les airs puisqu'elles mettent en réseau les forces dans ces espaces. La maitrise des ondes a été de ce fait un contributeur important à la création d'un échelon opératif.

Mais qui dit émission, dit détection et brouillage. Les moyens de guerre électronique permettent de localiser de tels signaux, de les écouter, de les perturber, voire d'interrompre la transmission d'informations. Ils permettent d'explorer les moyens de l'adversaire et de l'entraver dans sa capacité de conduite, tout en maintenant libres ses propres fréquences radio. Grâce aux progrès de la miniaturisation et de la mobilité de la technologie radio et des satellites, les activités dans l'espace électromagnétique s'exercent aujourd'hui à l'échelle mondiale et de manière largement anonyme.

... à l'internet global

Les armées modernes n'échappent donc plus à l'ubiquité des réseaux et suivent les mêmes tendances que les sociétés. Réalité augmentée pour les soldats, systèmes de conduite numériques ou internet des objets par exemple, le cyberespace démultiplie aujourd'hui les capacités de mise en réseau offertes avant par l'espace électromagnétique.

Néanmoins, si l'interconnexion croissante crée des opportunités, elle crée également des vulnérabilités. De nombreux systèmes, civils ou militaires, sont équipés de

composants qui utilisent le cyberespace et qui sont par conséquent susceptibles d'être visés par des actions dans le cyberespace. Chaque porteur de technologie, que ce soit un soldat avec un smartphone ou un système d'arme complexe devient un potentiel point d'entrée pour une attaque. La généralisation des systèmes connectés à internet, mais insuffisamment protégés, entraîne une multiplication des objectifs susceptibles d'être espionnés, influencés ou perturbés.

Dans le cyberespace, le vandalisme, la criminalité, l'espionnage, le sabotage, la subversion ou le terrorisme profitent de ces vulnérabilités. Ces actions peuvent être du ressort d'une multitude d'acteurs puisque le cyberespace permet à presque n'importe qui d'avoir un effet et c'est une différence notable par rapport aux autres espaces d'opération. Chaque utilisateur d'internet disposant de l'intention et des moyens peut y générer des effets, et ce quel que soit son emplacement sur terre. Les capacités de mener des opérations dans le cyberespace ne sont donc pas l'apanage des Etats. Tous ces acteurs profitent du rythme de transformation très rapide des technologies, en particulier civiles, dans le cyberespace.

Des actions difficiles à attribuer

Les acteurs hostiles exploitent donc les caractéristiques de ces espaces pour passer inaperçus le plus longtemps possible et atteindre leurs objectifs, si possible, sans faire ouvertement usage de la violence. A cette fin, les cyberattaques et les actions dans l'espace électromagnétique constituent un moyen idéal, car elles agissent à distance et ne sont que difficilement attribuables. Elles se prêtent donc particulièrement bien à une approche hybride ou indirecte.

De plus, contrairement à l'usage des armes classiques, les moyens tant cyber que ceux relevant de la guerre électronique provoquent peu de dommages collatéraux physiques directs et se prêtent particulièrement bien à un engagement proportionné dans des zones bâties et habitées. Ils présentent en outre relativement peu de risques pour les propres troupes parce qu'ils agissent à distance de sécurité.

Néanmoins, leurs retombées peuvent être réelles et catastrophiques lorsque qu'elles impactent ou débordent sur des infrastructures critiques comme des réseaux énergétiques, des hôpitaux ou des centrales nucléaires. Aussi, plusieurs Etats et alliances s'efforcent de faire assimiler, dans le droit international public, les cyberattaques à des attaques physiques armées. Les ministres de la Défense des pays de l'OTAN ont ainsi décidé en 2021 qu'une attaque menée contre les réseaux informatiques des membres de l'Alliance pourrait entrainer éventuellement l'activation de la clause de défense mutuelle lorsque les effets de l'agression sont comparables «aux effets d'une agression physique».

Une cyberguerre au sens stricte est néanmoins peu probable parce qu'il est difficile de mettre à genou tout un système adverse sans combiner ces effets avec des actions dans les espaces physiques. La guerre en Ukraine a d'ailleurs montré, que malgré une supériorité russe supposée dans le cyberespace et l'espace électromagnétique, l'Ukraine et parvenue à assurer les conduites civiles et militaires moyennant une décentralisation, le recours à des moyens civils redondants comme Starlink, et l'intégration rapide d'innovations civiles.

Les actions menées aujourd'hui dans le cyberespace et l'espace électromagnétique sont néanmoins indispensables pour compléter, appuyer et renforcer considérablement les opérations militaires, pour préparer une attaque physique, pour perturber les infrastructures, armes et systèmes critiques avec la plus haute précision, et ce même plusieurs semaines ou mois avant le déclenchement d'opérations terrestres ou aériennes. De plus, elles accompagnent également les actions dans la sphère de l'information qui repose aujourd'hui presque entièrement sur les ondes et les systèmes informatiques.

A l'instar de tout autre Etat hautement développé, la Suisse peut être attaquée sans qu'un adversaire ne doive mener une action armée au sens conventionnel du terme depuis l'extérieur du pays. La Conception générale cyber, publiée en 2022, prend en compte cette réalité et définit les bases du nécessaire développement de nos capacités dans ce domaine. L'armée les a déjà considérablement renforcées au cours des dernières années. Néanmoins, le retour de la capacité de défense nécessitera encore un développement conséquent de ces capacités afin de garantir la pleine aptitude à la conduite de l'armée.

L. M.