La guerre électronique : question du passé ou d'avenir ?

Patrick JUSTEL

Colonel de l'Armée de terre, auditeur de la 67e session du Centre des hautes études militaires (CHEM).

Un domaine confronté à de nombreux défis

Dans la doctrine française [1], la guerre électronique (GE) désigne « tout ce qui a trait aux opérations de combat effectuées dans l'Environnement électromagnétique (EME) » [2]. En effet, cet environnement est utilisé en permanence pour de nombreuses capacités opérationnelles, comme les télécommunications, le recueil du renseignement, ou la navigation. Comme dans tout champ de bataille, on peut y attaquer [3] et surveiller [4] l'ennemi ou s'en défendre [5]. Les premières actions de GE datent de la guerre-russo japonaise de 1904-1905 [6]. En France, elles débutent avec la Première Guerre mondiale, la GE apportant des contributions décisives au cours de batailles comme celle de Verdun [7]. Elle a également joué un rôle clé pendant la Seconde Guerre mondiale [8] et a fait l'objet d'une attention particulière dans les deux blocs au cours de la guerre froide [9]. Cependant, elle est aujourd'hui confrontée à de nombreux défis.

Difficultés liées à la rapidité d'adaptation de l'adversaire et à l'évolution des technologies

Un adversaire qui se sait confronté à la GE prend des mesures pour limiter l'efficacité de nos actions voire les rendre contre-productives. La première réponse consiste souvent à arrêter complètement les émissions ou à basculer sur des moyens

(1) *Doctrine interarmées DIA 3-6, La Guerre électronique*, du 20 octobre 2017.

(2) La notion d'environnement électromagnétique (EME) est de l'ordre de l'emploi militaire, tandis que la notion de spectre électromagnétique (EMS) est d'ordre scientifique. *Publication interarmées PIA-3.6.1, Maîtrise de l'environnement électromagnétique*, du 6 avril 2016.

(3) L'attaque électronique (AE) consiste en l'emploi de l'énergie électromagnétique à des fins offensives.

(4) La surveillance électronique (SE) consiste à employer l'énergie électromagnétique afin de contribuer à la connaissance de situation et à la collecte de renseignement.

(5) La défense électronique (DE) consiste en l'emploi de l'énergie électromagnétique afin de protéger et de garantir la liberté d'usage du spectre électromagnétique face aux attaques électroniques de l'adversaire.

(6) Actions de brouillage et d'écoute des réseaux radio adverses. Cf. BONNEMAISON Aymeric et DOSSÉ Stéphane, *Attention : Cyber ! Vers le combat cyber-électronique*, Économica, 2014, p. 70.

(7) L'Association de guerre électronique de l'Armée de terre présidée par le général (2S) Degoulange a procédé à de nombreuses recherches et reconstitutions sur l'action de la GE pendant ce conflit. Voir notamment « Hommage aux hommes de l'ombre – Du lieutenant Delavie, officier réserviste inventif au Soldat "écouteur-interprète" Pierre Hoff », 3 janvier 2015 (http://ageat.asso.fr/spip.php?article175).

(8) Par exemple, le service « *Y* » britannique s'illustra en Afrique face à Rommel. Cf. CLAYTON Anthony, « Le renseignement militaire britannique pendant la Seconde Guerre mondiale », *in* SOUTOU Georges-Henri, FRÉMEAUX Jacques et FORCADE Olivier (dir.), *L'Exploitation du renseignement*, Économica, 2001, p. 172.

(9) ANDREW Christopher et MITROKHINE Vassili, *Le* KGB *contre l'Ouest, 1917-1991*, Arthème-Fayard, 2000, p. 495-522.

mieux protégés. Ces comportements ont pu être observés sur la plupart des théâtres où les armées françaises ont été engagées depuis la fin de la guerre froide. Mais un ennemi plus organisé pourra également essayer de nous intoxiquer en échangeant de fausses informations sur des moyens qu'il sait écoutés. En Afghanistan, les *Talibans* se sont ainsi souvent livrés à des tentatives d'intoxication pour détourner nos forces vers d'autres secteurs quand ils étaient mis en difficulté. L'histoire du XX^{e} siècle est riche en exemples d'opérations sophistiquées ayant parfaitement réussi à tromper un ennemi bien organisé (10). Ce défi est aggravé par une plus large diffusion de l'information sur la surveillance électronique. En effet, le besoin de communiquer sur nos succès pour justifier l'acquisition de ces capacités ou la nécessité d'expliquer certaines actions (11) peuvent révéler à l'ennemi qu'il est surveillé.

La seconde évolution qui met la guerre électronique en difficulté est la complexité croissante des moyens de communication et de détection. Des techniques aujourd'hui largement diffusées comme le chiffrement (12) ou l'évasion de fréquence peuvent rendre la tâche ardue, empêchant souvent l'accès au contenu des communications. En parallèle, la croissance exponentielle du nombre d'émetteurs et des débits d'information peut saturer rapidement les moyens de GE.

Un domaine partiellement délaissé après la guerre froide

Dans les opérations récentes, notre GE s'est souvent centrée sur l'acquisition du renseignement au détriment de la défense et de l'attaque électroniques.

Pour la défense électronique, des moyens de brouillage d'autoprotection ont continué à être mis en œuvre sur les plateformes aériennes et navales. Néanmoins, les armées occidentales ont eu tendance à délaisser ce qui était considéré avant comme un enjeu majeur : la protection de nos moyens de commandement et de navigation. En effet, dans les dernières opérations de contre-insurrection, face à des adversaires d'un niveau technologique très éloigné du leur, les armées occidentales ont pu disposer d'une quasi-totale liberté d'action dans l'environnement électromagnétique. La défense électronique de nos moyens de communication s'est donc concentrée sur l'utilisation de technologies sécurisées en mettant de côté d'autres ou l'entraînement. Dans une étude sur les modes d'action russes dans le conflit ukrainien, l'*US Army* liste ses faiblesses face à la GE adverse, parmi lesquelles on peut citer (13) :

– des postes de commandement trop grands, facilement détectables et peu mobiles, donc particulièrement vulnérables face à la GE et aux attaques d'un ennemi symétrique ;

(10) Cf. l'exemple de l'intoxication du renseignement allemand par les Alliées avant le débarquement en Normandie. Cave Brown Anthony, *La guerre secrète, T. 2, Le Jour J et la fin du III^{e}* Reich, Perrin, 2012, p. 94-95.
(11) Ce fut le cas par exemple pour justifier l'assaut sur le *Tanit* en avril 2009, au cours duquel l'un des otages perdit la vie. « *Tanit* : pourquoi les commandos ont donné l'assaut », *Le Parisien*, 10 avril 2009 (www.leparisien.fr/faits-divers/tanit-pourquoi-les-commandos-ont-donne-l-assaut-10-04-2009-474944.php).
(12) Seibt Sébastian, « Attentats de Paris : Bitcoin, crypto et une start-up américaine critiqués », *France 24*, 20 novembre 2015 (www.france24.com/).
(13) *Asymetric Warfare Group, Russian New Generation Warfare Handbook*, Version 1, décembre 2016.

– un commandement trop centralisé et trop dépendant des systèmes de communication ;
– un manque d'entraînement au combat en ambiance de brouillage.

L'attaque électronique a également été progressivement délaissée même si la multiplication sur les théâtres d'opérations des engins explosifs improvisés radiocommandés a entraîné un regain d'intérêt pour le brouillage terrestre. Après l'avoir utilisé pour la protection des véhicules, des attaques contre les réseaux adverses ont également été menées mais toujours de manière limitée. En effet, si les capacités de brouillage offensif existent mais restent insuffisantes dans le milieu terrestre, elles sont actuellement inexistantes dans les milieux aérien et maritime (14). C'est sans doute le domaine où les Armées françaises ont le plus de faiblesses.

Le retard pris par la plupart des armées de l'Otan en matière de GE est tel qu'il a conduit, en février 2016, le général de l'*US Air Force* Philip Breedlove, alors Commandant en chef des forces alliées en Europe (*SACEUR*), à tirer la sonnette d'alarme (15).

Une guerre électronique remise en cause par la cyberdéfense ?

Le lien entre la GE et la cyberdéfense militaire (16) paraît logique compte tenu du rapprochement des mondes des télécommunications et de l'informatique. Il est illustré par le nouvel objet de la vie quotidienne qu'est devenu le *smartphone*.

« L'actuelle convergence de l'informatique et des télécommunications constitue une nouvelle étape d'un long processus. Ainsi, les domaines de ce combat sur les réseaux étaient anciennement séparés pour des raisons historiques et de formation du personnel. Dans le temps long, force est de constater que la convergence des réseaux filaires et radio, associés aux chiffrements, impliquent une convergence de la GE et du cyber » (17).

Certains pays ont ainsi fait le choix de subordonner leurs unités de GE à des commandements cyber. Afin de coordonner les compétences de la *Bundeswehr* en matière de cyberdéfense, l'Allemagne a ainsi décidé de se doter d'un Commandement du Cyberespace et de l'Information (*KdoCIR*) qui a également sous son autorité les unités de GE (18). Ce choix peut aussi s'expliquer par des contraintes budgétaires et surtout humaines, les deux domaines pouvant faire appel aux mêmes spécialités rares

(14) Certains bâtiments de la Marine nationale disposent néanmoins de capacités de brouillage radar à vocation défensive, qui pourraient être utilisées de manière offensive.
(15) Majumdar Dave, « Electronic Warfare: Russian Gains Threaten to 'Disconnect' U.S. Forces », *The National Interest*, 25 février 2016 (http://nationalinterest.org/blog/the-buzz/electronic-warfare-russias-gains-threaten-disconnect-us-15323).
(16) Cyberdéfense militaire : ensemble des actions défensives ou offensives conduites dans le cyberespace en préparation ou dans la planification et la conduite des opérations militaires, notamment pour garantir l'efficacité de l'action des forces armées et le bon fonctionnement du ministère des armées. *Doctrine interarmées DIA 3-20, Cyberdéfense*, du 21 juin 2016.
(17) Bonnemaison Aymeric et Dossé Stéphane, *op. cit.*, p. 71.
(18) Lagneau Laurent, « L'armée allemande se dote d'un commandement "Cyberespace et Information" », *Zone militaire, Opex360*, 1er avril 2017 (www.opex360.com/).

(linguistes, analystes…). Sur ce terrain, la guerre électronique s'est retrouvée en compétition avec la cyberdéfense.

Face à tous ces défis, la GE est-elle vouée à disparaître ? Les conflits récents montrent qu'il n'en est rien et nous invitent à réinvestir ce domaine [19].

De nouvelles perspectives

À partir de 2014, alors que les pays de l'Otan avaient délaissé leurs capacités de guerre électronique, ils ont pris conscience, que d'autres pays comme la Russie avaient développé les leurs. Moscou en a fait un atout majeur d'une nouvelle forme de guerre à laquelle nos pays ne semblent plus préparés. Cela a notamment conduit l'*US Army* à redéployer des moyens de GE en Europe [20]. Les opérations au Levant ont aussi mis en évidence l'importance de la maîtrise de l'environnement électromagnétique [21].

De nouvelles menaces électroniques et un nouvel environnement électromagnétique

En Ukraine, l'emploi de la GE russe en appui des forces séparatistes a surpris non seulement l'Armée ukrainienne mais aussi les observateurs occidentaux. Le premier événement mentionné par les médias a lieu en mer Noire et date d'avril 2014 : les Russes annoncent qu'un avion *Su-24 Fencer* a réussi à brouiller le radar de l'*USS Donald Cook*. Cette information est toutefois démentie par l'*US Navy* [22]. Elle semble en réalité relever de la désinformation [23], preuve du lien étroit entre la GE et la guerre psychologique. En revanche, les actions de la GE russe au sol et son emploi combiné avec l'artillerie ont retenu toute l'attention des spécialistes occidentaux. Ils illustrent la manière dont la Russie a tiré les leçons des derniers conflits où les armées occidentales ont été engagées et cherche à faire de nos forces une faiblesse : « *Russia knows how we roll. They have invested a lot in electronic warfare because they know we are a connected and precise force and they need to disconnect us to make us imprecise* » [24].

D'après l'étude de l'*Asymetric Warfare Group* de l'*US Army* [25], l'armée russe s'est transformée et a repris des principes du modèle soviétique des complexes

(19) « Le bel avenir de la guerre électronique », *Lettre d'information TTU*, 20 avril 2016 (www.ttu.fr/bel-avenir-de-guerre-electronique/).

(20) Heininger Claire, « U.S. Army's New Electronic Warfare Capabilities hit the Ground in Europe », US Army, 6 février 2018 (www.army.mil/article/200175/us_armys_new_electronic_warfare_capabilities_hit_the_ground_in_europe).

(21) Cet enjeu est également identifié dans la doctrine française. Il a conduit à développer la notion « d'opérations électromagnétiques » dont fait partie la guerre électronique. Cf. la publication interarmées *PIA-3.6.1, Maîtrise de l'environnement électromagnétique*, du 6 avril 2016.

(22) « NavWeek: Jammed Up », *Aviation Week Network*, 25 novembre 2014 (http://aviationweek.com/blog/navweek-jammed).

(23) Plusieurs sites américains et russes mettent en avant que le complexe Khibiny évoqué dans les médias n'équipe que les *Su-35*, *Su-34* et *Su-30* et sert à l'autoprotection. Voir, en anglais, Leopold George, « Fake Russian EW attack unmasked », *Defense Systems*, 12 mai 2017, (https://defensesystems.com/articles/2017/05/12/fakeew.aspx), ou en russe, « Комплекс РЭБ "Хибины" чудо-оружие армии России? », *Военное Обозрение*, 31 octobre 2017 (https://topwar.ru/128491-kompleks-reb-hibiny.html).

(24) Propos du général Philip Breedlove, cité par Majumdar Dave, *op. cit*.

(25) *Asymetric Warfare Group, Russian New Generation Warfare Handbook*, *op. cit*.

« reconnaissance-frappe » [26]. Elle les a adaptés au XXIe siècle par un mélange sophistiqué de drones, de GE, de *snipers* et d'artillerie à longue portée. En Ukraine, la GE russe apporte les contributions suivantes [27] :

- protection des forces amies en leurrant les missiles, en brouillant les systèmes de guidage ou en causant l'explosion prématurée des munitions ;
- acquisition d'objectifs en localisant les postes de commandement adverses ;
- brouillage des communications de l'ennemi pour le fixer avant les frappes d'artillerie ;
- perturbation des moyens de navigation comme le *GPS* ;
- brouillage des liaisons des drones pour empêcher leur emploi ;
- appui aux opérations d'information, notamment par la diffusion de *SMS* personnalisés afin de déstabiliser leurs adversaires ou de les inciter à émettre pour révéler leur position.

Des actions de GE russe ont également pu être constatées autour de la mer Baltique. En septembre 2017, des perturbations des signaux *GPS* ont gêné le trafic aérien civil en Norvège. Le réseau de téléphonie mobile letton a également été affecté [28]. Ces problèmes ont été considérés comme le résultat d'actions de brouillage russes lors de l'exercice *Zapad 2017* [29]. Dans la même région, les téléphones mobiles des militaires de l'Otan ont fait l'objet d'attaques ciblées également attribuées à la Russie [30].

L'autre théâtre dans lequel la GE est redevenue un sujet d'actualité est le Levant. En Syrie, des moyens de GE russes ont également été mis en œuvre. Outre les capacités embarquées à bord des aéronefs et des bâtiments [31], on peut citer le déploiement de moyens terrestres *Krasukha-4* disposant de capacités de brouillage *GPS* et radar mais également de lutte anti-drones [32]. Initialement destinées à gêner les aéronefs et les moyens de renseignement de la Coalition, ces capacités semblent également avoir été utilisées contre une attaque d'une dizaine de mini-drones armés sur la base de

(26) Ce modèle prévoyait d'organiser des « complexes reconnaissance-frappe » afin de frapper l'ennemi dans la profondeur. Bihan Benoist, « *Apocalypse? No!* Ou comment renoncer à la guerre nucléaire », *Guerre & Histoire*, n° 38, août 2017, p. 39-41.

(27) *Asymetric Warfare Group, Russian New Generation Warfare Handbook*, *op. cit*.

(28) Trevithick Joseph, « The War Zone - Russia Jammed Phones and GPS in Northern Europe During Massive Military Drills », *The Drive*, 16 octobre 2017 (www.thedrive.com/).

(29) Dans le cas de la Norvège, le chef du renseignement militaire a estimé que son pays n'était probablement pas directement visé mais que ces perturbations étaient une conséquence collatérale de l'exercice. Cf. Nielsen Thomas, « Electronic warfare: Norway well prepared to Meet Russian Jamming », *The Barents Observer*, 14 décembre 2017 (https://thebarentsobserver.com/en/node/3327).
Les autorités lettones ont quant à elles estimé que son réseau mobile avait été brouillé par les Russes depuis l'enclave de Kaliningrad, mais que ce brouillage visait plutôt l'île suédoise de Gotland. Gelzis Gederts et Emmott Robin, « Russia may have tested Cyber Warfare on Latvia, Western Officials say », *Reuters*, 5 octobre 2017 (www.reuters.com/).

(30) Shultz Teri, « Russia is hacking and harassing NATO Soldiers, Report says », *Deutsche Welle*, 6 octobre 2017, (www.dw.com/en/russia-is-hacking-and-harassing-nato-soldiers-report-says/a-40827197).

(31) Meadows David E., « Modern EW Capabilities Accompany Russian Forces Into Syria », *Signal*, 13 octobre 2015, (www.afcea.org/content/?q=Blog-modern-ew-capabilities-accompany-russian-forces-syria).

(32) « Des armes de guerre électroniques russes aperçues en Syrie », *Sputnik News*, 5 octobre 2015 (https://fr.sputniknews.com/international/201510051018601095-syrie-russie-armes-electroniques/).

Hmeimim en janvier 2018 (33). Mais la GE russe n'est pas la seule au Levant. D'autres acteurs l'ont largement pratiquée dans le passé comme Israël ou le *Hezbollah* (34). Plus récemment, les membres de la Coalition ont aussi utilisé des moyens de GE pour lutter contre l'État islamique (EI) (35). Ce conflit leur a surtout fait prendre conscience que l'environnement électromagnétique dont ils avaient librement disposé lors des précédentes opérations était redevenu un terrain contesté. La bataille de Mossoul de 2016-2017 leur a aussi permis de constater qu'il fallait s'y battre avec des moyens de GE détachés jusqu'au plus bas niveau (36). Cette bataille a ainsi été considérée par les États-Unis comme un exemple de *Multi-Domain Battle* face à un ennemi hybride en zone urbaine. Ce concept à vocation interarmées a été développé par l'*US Army* et l'*US Marine Corps* pour faire face à l'ennemi de 2025-2040 (37). Considérant que les adversaires potentiels des États-Unis ont appris à contrer leur supériorité dans les milieux qui faisaient leur force, il s'agit de les dépasser en étendant le combat simultanément à l'ensemble des milieux interarmées (38) auxquels le concept propose d'en ajouter trois : « l'environnement informationnel, la dimension cognitive et l'environnement électromagnétique ».

Cette évolution est étroitement liée à la numérisation croissante de l'ennemi. Celle-ci est certes une force pour lui : meilleures capacités de commandement et de renseignement, possibilités accrues pour diffuser sa propagande (39) et moyen d'attaquer nos propres systèmes. Mais cette numérisation de l'ennemi et son recours à la GE pourront aussi constituer une faiblesse et nous offrir de nouvelles opportunités.

De nouveaux combats à mener avec de nouvelles armes

Les colonels chinois Qiao Liang et Wang Xiangsiu écrivaient dans *La Guerre hors limites* : « l'espace du spectre électromagnétique est un nouveau type d'espace de combat fondé sur la créativité technique et qui dépend de la technique » (40). Les évolutions tactiques et technologiques doivent nous amener à réinventer notre GE, en encourageant l'innovation.

---

(33) Sly Liz, « Who is attacking Russia's bases in Syria? A new mystery emerges in the war », *The Washington Post*, 10 janvier 2018 (www.washingtonpost.com/).

(34) L'une des grandes surprises de ce conflit a été la découverte des capacités de surveillance électronique mises en œuvre par le *Hezbollah*. « L'aptitude du *Hezbollah* à intercepter et à "lire" les actions israéliennes a eu un impact décisif sur l'offensive terrestre qui allait se produire à la fin de la guerre. Les responsables du renseignement hezbollahi avaient perfectionné leur capacité à déchiffrer les signaux ennemis à un tel point qu'ils étaient en mesure d'intercepter les communications terrestres entre commandants israéliens ». Perry Mark et Crooke Alastair, « Comment le *Hezbollah* a vaincu Israël » (traduit de l'anglais par Marcel Charbonnier et révisé par Fausto Giudice), *Conflicts Forum*, 12-14 octobre 2006 (www.conflictsforum.org/2006/comment-le-hezbollah-a-vaincu-israel/).

(35) Lagneau Laurent, « La guerre électronique, un autre aspect important de la lutte contre l'État islamique », *Zone Militaire Opex360*, 19 décembre 2016 (www.opex360.com/).

(36) Centre interarmées de concepts de doctrines et d'expérimentations (CICDE), Fiche « Éléments de Retex de l'armée des États-unis en guerre électronique suite à la bataille de Mossoul », 15 janvier 2018.

(37) Training and Doctrine Command (TRADOC), *Multi-Domain Battle: Combined Arms for the 21st Century. White Paper*, 24 février 2017, US Army (www.arcic.army.mil/).

(38) Terre, air, mer, espace et cyberespace dans la doctrine américaine.

(39) Pour l'année 2015, « l'EI à lui seul revendiquait la diffusion de 800 vidéos, 15 000 photos, 18 magazines en 11 langues et des dizaines de milliers de tweets quotidiens ». Thomson David, *Les Revenants*, Éditions du Seuil, 2016, p. 105.

(40) Liang Qiao et Xiangsiu Wang, *La Guerre hors limites*, Payot & Rivages, 2006, p. 77.

SEAD [41] **:** l'une des principales lacunes à combler concerne les capacités aéroportées de brouillage offensif, dont la France ne dispose pas, contrairement à plusieurs de nos alliés ou adversaires potentiels. Or ces moyens contribuent à trois domaines clés : la suppression des défenses aériennes ennemies (*SEAD*), la guerre du *C2* et les opérations d'information. Les combats menés dans les deux derniers domaines ont déjà été évoqués dans l'étude du conflit ukrainien. Dans un autre registre, la *SEAD* constitue l'une des réponses aux « capacités de déni d'accès et d'interdiction de zone en cours de dissémination », alors que « contrer les postures de déni d'accès et conquérir la supériorité aérienne redevient un objectif préalable à toutes les opérations » [42]. Les contributions classiques de la GE [43] comme la localisation ou le brouillage des émetteurs pourront être complétées par des actions combinant ses effets à ceux du cyber [44], afin de désorganiser en profondeur tout le système de défense aérienne adverse.

NAVWAR **et Espace :** nos armées devront être capables de se protéger des attaques contre nos systèmes de navigation, non seulement en limitant leur dépendance à ce genre de moyens mais également en étant capables de détecter, de localiser et de neutraliser les moyens de brouillage adverses. Elles pourraient également développer leurs capacités offensives, en visant d'autres systèmes de navigation que le *GPS* [45] et d'autres fonctions que la localisation [46]. Mais ces actions face à des dispositifs basés sur des satellites renvoient à un autre sujet à explorer : celui de la GE dans l'Espace. En effet, si des actions sont déjà menées depuis ou vers [47] l'Espace, des actions de GE entre engins spatiaux pourraient aussi être envisagées. Alors que « d'ores et déjà s'affichent des velléités d'action militaire de l'Espace, tandis que s'y déroulent des opérations qui laissent peu de doute sur leur finalité réelle » [48], la GE permettrait d'y agir en étant difficilement détectable et sans causer de dégâts matériels.

Drones et robotisation : des moyens destinés à brouiller les liaisons de télécommande des drones sont déjà mis en œuvre par plusieurs armées. Ils ont principalement pour effet de les aveugler [49] ou de les obliger à se poser. Ils pourraient encore

(41) *Suppression of Ennemi Air Defences*. La *SEAD* s'exerce à l'encontre du système intégré de défense aérienne de l'adversaire : radars au sol et systèmes *C4* d'alerte avancée qui leur sont associés, interceptions contrôlées du sol, nœuds de communications critiques et les systèmes de défense aérienne de surface longue portée (*DIA 3-6*).

(42) Danjean Arnaud (dir.), *Revue stratégique de défense et de sécurité nationale*, Dicod, 2017, p. 49.

(43) La *SEAD* résulte de la combinaison de deux capacités : la guerre électronique et un ensemble d'armes conventionnelles (*DIA 3-6*).

(44) Entretien avec Joseph Henrotin. Ce type d'attaque combinant guerre électronique et cyber aurait été mise en œuvre par Israël lors de l'opération *Orchard* : le *raid* aérien israélien contre les installations nucléaires syriennes de Deir er-Zor le 6 septembre 2007. Voir aussi Taillat Stéphane, « Coercition et dissuasion dans le cyberespace », *Défense & Sécurité Internationale*, n° 110, janvier 2015, pp. 44-49.

(45) Systèmes *Galileo* européen, *Glonass* russe, *Compass-Beidou* chinois, *IRNSS* indien ou *QZSS* japonais.

(46) L'une des principales fonctions du *GPS* n'est pas la localisation mais la synchronisation des systèmes. Une attaque sur cette fonction peut permettre de désorganiser un réseau.

(47) Satellites d'écoute (depuis) ou aveuglement d'un satellite au moyen d'un laser (vers). Centre nationale d'études spatiales (Cnes), « Un satellite d'espionnage américain aveuglé par un laser chinois », *Futura Sciences*, 12 octobre 2006 (www.futura-sciences.com/sciences/actualites/univers-satellite-espionnage-americain-aveugle-laser-chinois-9774/).

(48) Secrétariat général de la défense et de la sécurité nationale (SGDSN), *Chocs futurs – Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité*, 2017, p. 127 (www.sgdsn.gouv.fr/uploads/2017/04/sgdsn-document-prospectives-v5-bd.pdf).

(49) Landreau Alexis et Aboville (d') Foulques, « La *New Generation Warfare* russe à l'épreuve de la guerre en Ukraine », *Lettre du Retex* n° 30, Centre de doctrine et d'enseignement du commandement (CDEC), septembre 2016, p. 5-6.

être développés en visant la prise de contrôle des drones (50) ou la modification des flux vidéo. Les drones renvoient également à un autre domaine à explorer pour la GE de demain : celui de la robotisation.

« En 2030, les robots et systèmes autonomes seront devenus des acteurs ordinaires dans le domaine des opérations militaires télé-opérés ou entièrement autonomes, ils agiront dans les champs d'affrontement physiques et le cyberespace » (51). La GE pourra en effet naturellement trouver son utilité face à des robots téléopérés ou télé-supervisés avec des techniques similaires à celles de la lutte anti-drones. Elle pourrait également jouer un rôle face aux systèmes autonomes grâce à de nouveaux outils comme les armes à énergie dirigée (52). À l'inverse, les robots pourront aussi servir de vecteurs de GE, pour des actions à proximité des cibles ou pour de la déception électronique.

Lutte anti-GE : un autre domaine à développer est la lutte contre la GE adverse. Il s'agit d'abord de mieux s'en prémunir par les moyens classiques de défense électronique (53). Mais ce combat pourrait prendre des formes plus élaborées et offensives par un ciblage systématique des moyens de GE adverse. Ce ciblage pourrait présenter plusieurs intérêts : « *The Russian Army displays key weapon systems, like electronic warfare (EW) and air defense artillery (ADA) platforms, as universal capabilities. In reality, however, these exist in limited capacity quantities. These systems are new and have not been fielded to their entire force. Generally, Russian tactics are to emplace EW and ADA assets in key operational and strategic locations then move them as soon as their mission is complete to limit their vulnerability. […] Losing even one of these systems is a significant blow to Russian Forces and creates a gap in their A2AD bubble that can be exploited* » (54).

Ainsi, la localisation de ces moyens pourrait apporter des renseignements intéressants sur la manœuvre adverse. En outre, compte tenu de leur faible nombre et de leur importance dans les dispositifs adverses, la moindre destruction pourrait perturber sa manœuvre, tandis que leur leurrage aurait un fort impact sur l'appréciation de situation de l'ennemi. Outre la destruction physique, le ciblage de ces moyens pourrait passer par des actions de déception (55) ou de masquage (56) électroniques, qui ne sont

(50) En obligeant par exemple un drone suicide à revenir sur celui qui le commande.

(51) SGDSN, *Chocs futurs*, *op. cit.*, p. 187.

(52) « On appelle arme à énergie dirigée, une arme capable de faire se propager vers une cible, à la vitesse de la lumière, un faisceau d'ondes électromagnétiques (laser ou micro-ondes), le cas échéant avec une grande directivité (arme laser) », SGDSN, *Chocs futurs*, *op. cit.*, p. 192. Le recours offensif aux armes à énergie dirigée entre dans le cadre de l'attaque électronique (*DIA 3-6*).

(53) Par exemple : utiliser des moyens protégés, rendre la plus discrète possible son empreinte électronique, savoir reconnaître une action de brouillage et réagir en conséquence, être capable de naviguer sans *GPS* ou de manœuvrer en silence radio, alléger les postes de commandement pour pouvoir les déplacer régulièrement, pratiquer la subsidiarité du commandement pour réduire la dépendance aux moyens de communication, etc.

(54) *Asymetric Warfare Group, Russian New Generation Warfare Handbook*, *op. cit.*

(55) La déception électronique consiste en l'émission délibérée, en l'altération, en l'absorption ou en la réflexion d'énergie électromagnétique en vue de perturber un adversaire ou un de ses systèmes électroniques, ou détourner, ou capter leur attention (*DIA 3-6*).

(56) Le masquage électronique consiste en l'émission contrôlée de rayonnement électromagnétique sur les fréquences amies, dans le but de protéger les émissions de communications et les systèmes électroniques amis contre la surveillance électronique de l'ennemi (*DIA 3-6*).

pas mises en œuvre au niveau où elles le pourraient [57]. Ces actions pourraient être préparées avec un entraînement adapté et s'appuyer sur des équipements adaptés comme des simulateurs de réseaux déployables sur le terrain [58].

Armes à énergie dirigée : l'autre type d'action que prévoit la doctrine et qui n'est pas réalisé faute d'équipement est la neutralisation électronique [59]. Celle-ci pourra devenir une réalité avec le développement des armes à énergie dirigée, dont « l'apparition dans les unités opérationnelles pourrait bien être l'amorce de la prochaine révolution militaire » [60]. Cela renforcera les capacités offensives de la GE avec la possibilité de neutraliser à distance l'électronique adverse.

Intelligence artificielle : même si le domaine de la surveillance électronique a été le moins délaissé, il devrait lui aussi connaître des évolutions importantes. Face aux risques de saturation et aux difficultés croissantes pour accéder au contenu des communications, l'effort des moyens de surveillance pourra porter sur la détection, l'identification et la localisation de menaces à l'aide de systèmes d'intelligence artificielle [61]. Ces systèmes pourront aider les analystes à reconstituer les réseaux, à identifier des signatures électroniques ou des comportements types et à détecter des anomalies. Le travail des linguistes pourra également être facilité. Cependant, si ces évolutions sont annoncées depuis plusieurs années, elles restent encore à consolider et le rôle de l'être humain devrait encore rester central.

Ces quelques exemples montrent toute l'étendue des défis que la GE aura à relever dans les prochaines années. Cela nécessitera d'adapter son organisation et ses modes d'action.

De nouvelles organisations pour de nouveaux modes d'action en complémentarité avec la cyberdéfense

Les derniers conflits ont confirmé le besoin de disposer d'une guerre électronique intégrée aux forces jusqu'aux plus bas échelons tactiques. Un autre enseignement a été de rattacher la GE à des structures multicapteurs [62]. En effet, face à des adversaires qui se dissimulent ou leurrent nos systèmes de surveillance, nos armées ont développé la capacité à faire travailler ensemble différents types de capteurs comme la recherche humaine, la GE ou l'imagerie. Le choix d'une GE intégrée dans des structures

(57) Elles peuvent être utilisées dans le domaine des radars, mais rarement dans celui des communications.

(58) Ce type de simulateurs existent aujourd'hui et sont utilisés pour l'entraînement des unités de GE. Ils pourraient l'être pour des opérations de déception.

(59) La neutralisation électronique consiste en l'usage délibéré d'énergie électromagnétique en vue d'endommager les systèmes adverses qui fonctionnent exclusivement grâce au spectre électromagnétique. Elle est généralement effectuée au moyen d'une arme à énergie dirigée délivrant suffisamment d'énergie électromagnétique à sa cible (ou aux composants électroniques de celle-ci) pour la rendre inutilisable (DIA 3-6).

(60) SGDSN, *Chocs futurs*, *op. cit.*, p. 187.

(61) Des outils de ce genre sont déjà en cours de développement pour l'imagerie. SGDSN, *Chocs futurs*, *op. cit.*, p. 106.

(62) La capacité multicapteurs se retrouve dans plusieurs plateformes aéroportées. BERGER Olivier, « Le renseignement militaire peut-il émerger du brouillard de la guerre ? », *blog Défense globale*, 7 février 2017, *La Voix du Nord* (http://defense.blogs.lavoixdunord.fr/archive/2017/02/07/renseignement-militaire-et-brouillard-15078.html).
Par exemple, les 44e et 54e Régiments de transmissions sont subordonnés au Commandement du renseignement et le *14th Signal Regiment* (*British Army*) à la *1st Intelligence, Surveillance and Reconnaissance Brigade*.

multicapteurs au sein des forces semble pertinent pour l'avenir. La principale question pour la future organisation de la GE sera celle de son lien avec la cyberdéfense.

« D'ici une vingtaine d'années, dans nombre d'armées modernes les fonctions de lutte informatique, de GE, de transmissions auront convergé vers des organisations globales de combat cyber-électronique » (63).

Compte tenu de l'évolution rapide des deux domaines et des multiples possibilités envisageables, les futures organisations devront être le résultat d'une approche empirique appuyée par une réflexion sur les différences et la complémentarité des deux domaines.

Concernant les différences, on peut tout d'abord noter que ces deux domaines agissent sur des milieux qui, s'ils ne sont pas disjoints, ne sont pour autant pas identiques (64) : le cyberespace (65) et le spectre électromagnétique. En effet, tout ce qui transite par la voie des ondes ne concerne pas directement la cyberdéfense (radar, balises de signalisation ou voix par exemple). À l'inverse, celles-ci ne sont pas le vecteur privilégié de la cyberdéfense, qui agit principalement *via* des réseaux filaires (fibre optique, par exemple). Les procédés et les méthodes peuvent également être très différents, avec, pour chacun des domaines, des avantages et des inconvénients. Par exemple, les effets de la GE sont souvent plus simples à contrôler que ceux de la cyberdéfense : un brouillage commence et s'arrête dès que l'ordre est donné, là où une attaque par un virus comme *Stuxnet* a mis plusieurs mois à produire des effets sur la cible visée et en a atteint de nombreuses autres non souhaitées. La GE agit principalement à proximité de l'adversaire et localement, c'est essentiellement un outil tactique. La cyberdéfense peut de son côté agir à distance et à grande échelle et donc à tous les niveaux, qu'ils soient stratégique, opératif ou tactique. La prise en compte de ces différences doit alimenter le développement de nouveaux modes d'action en recherchant la complémentarité de la GE et de la cyberdéfense pour l'attaque (66), la surveillance (67) et la défense (68).

Tout d'abord, la guerre électronique pourrait concourir aux opérations dans le cyberespace. Des attaques électroniques pourraient appuyer des opérations offensives dans le cyberespace, en perturbant des liaisons par du brouillage ou en utilisant des techniques d'intrusion pour offrir un accès à un réseau informatique adverse coupé d'*Internet*. Des armes à énergie dirigée pourraient demain également être utilisées contre des réseaux fermés auxquels la cyber n'a pas accès. La surveillance électronique

(63) Malis Christian, *Guerre et stratégie au XXIe siècle*, Éditions Fayard, 2014, 352 pages.

(64) Dans la *Multi-Domain Battle*, l'environnement électromagnétique est clairement distingué du cyberespace.

(65) Cyberespace : espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques (*DIA 3-20*).

(66) Lutte informatique offensive : actions non physiques entreprises dans le cyberespace contre des systèmes d'information ou des données pour les perturber, les modifier, les dégrader ou les détruire (*DIA 3-20*).

(67) Exploitation informatique : actions conduites dans le cyberespace en vue d'obtenir l'accès aux logiciels, configurations matérielles et données des réseaux informatiques. Elles visent à exploiter les données issues de systèmes d'information ou de réseaux cibles et à recueillir du renseignement (*DIA 3-20*).

(68) Lutte informatique défensive : surveiller, analyser, détecter et réagir face à des attaques, intrusions ou perturbations qui pourraient compromettre, paralyser ou détruire nos systèmes, réseaux et données (*DIA 3-20*).

pourrait alimenter le renseignement d'intérêt cyber en apportant des informations techniques sur les réseaux informatiques adverses. La défense électronique contribuerait de son côté à la cyberprotection de nos réseaux transitant par le spectre électromagnétique, en les mettant à l'abri de la GE adverse.

En sens inverse, la cyberdéfense pourrait concourir aux actions de GE et en démultiplier les effets. Le renseignement d'origine cyber pourrait fournir des informations techniques pour faciliter les attaques ou la surveillance électronique. La mise hors de service par une cyber-attaque de réseaux transitant par des câbles, pourrait obliger l'adversaire à utiliser des moyens rayonnants, le rendant ainsi vulnérable à la GE. De même, un logiciel malveillant transmis par les ondes servirait à attaquer la GE adverse, renforçant ainsi notre défense électronique.

Les pistes sont donc nombreuses et montrent tout l'intérêt de continuer à explorer la complémentarité des deux domaines sans forcément en faire disparaître l'un au profit de l'autre. L'*US Army* travaille sur leur intégration à travers le concept de *Cyber-Electromagnetic Activities* (*CEMA*), qu'elle détaille dans un manuel dédié aux « opérations dans le cyberespace et de guerre électronique » [(69)]. Il s'agit à travers la complémentarité des effets cyber et GE de transposer dans le cyberespace la logique du combat interarmes. « *The key word to remember about CEMA teams, is "integration". It's about integrating requirements, integrating capabilities and integrating formations so literally you can have a combined arms effect inside cyberspace. The CEMA teams themselves are becoming integrated as well, with specialists from cyber, military intelligence, electronic warfare, signals intelligence and sometime space coming together to deliver effects to the maneuver commander* » [(70)].

Comment favoriser cette complémentarité en termes d'organisation ? Au niveau stratégique, il conviendrait de regrouper les activités de cyber et de renseignement d'origine électromagnétique au sein des mêmes entités comme l'ont fait plusieurs pays [(71)]. Au niveau tactique, où notre cyberdéfense est cantonnée à la protection, des capacités de surveillance et d'attaque cyber pourraient être développées en s'appuyant sur les structures de GE des forces.

Pour le niveau tactique, il s'agirait dans un premier temps d'élargir le rôle des cellules de coordination de guerre électronique (CCGE) des états-majors. À titre d'exemple, l'*US Army* met en place des *CEMA sections* dans les états-majors de niveau brigade à corps d'armée en s'appuyant sur le personnel de GE déjà présent [(72)]. Ces sections peuvent notamment solliciter les capacités d'attaque et de surveillance cyber

(69) *Field Manual 3-12, Cyberspace and Electronic Warfare Operations*, 11 avril 2017.

(70) Propos du général John B. Morrison Jr., chef du *Cyber Center of Excellence* à Fort Gordon. Vergun David, « Integrated Army cyber activities teams playing pivotal role in warfare », US Army News Service, 9 janvier 2018 (www.army.mil/article/198871/integrated_army_cyber_activities_teams_playing_pivotal_role_in_warfare).

(71) Par exemple en Grande-Bretagne, le *Government Communications Headquarters*.

(72) « *CEMA section of the G-3 (S-3) from brigade to corps coordinates and synchronizes cyberspace and EW operations for effective collaboration across staff elements. This section includes the EWO (who has additional responsibility as the cyberspace planner), the spectrum manager, the EW technician, and EW noncommissioned officers. The CEMA section is key to the collaboration of cyberspace and EW operations* ». *Field Manual 3-12, Cyberspace and Electronic Warfare Operations*, 11 avril 2017, p. 3-6.

des échelons supérieurs au profit de la manœuvre de leur unité et coordonner leurs effets avec ceux de leurs propres moyens de GE. Dans un second temps on pourrait développer les capacités des unités de GE à mieux capter et exploiter le renseignement d'intérêt cyber et à servir de vecteurs pour des actions cyber offensives à travers le spectre électromagnétique, coordonnées avec le niveau supérieur. Cette évolution aurait un double avantage. Cela faciliterait la coordination des cyberattaques avec le reste de la manœuvre de la force et permettrait aux actions de surveillance cyber de s'intégrer dans des dispositifs de recherche multicapteurs, en profitant de structures déjà conçues à cet effet.

La solution proposée permettrait d'éviter de disperser les ressources au niveau stratégique (le plus consommateur). Au niveau tactique, elle permettrait d'avancer dans le développement de la complémentarité de la GE et de la cyberdéfense en appui des opérations.

⁂

La GE et l'environnement électromagnétique, qui constitue son champ de bataille, sont redevenus des enjeux d'avenir, que plusieurs responsables occidentaux ont invité à réinvestir. Cette évolution est liée aux conflits en Ukraine et au Levant, qui ont suscité une prise de conscience de nos faiblesses mais qui offrent aussi des pistes à explorer pour l'avenir. Face à des adversaires qui n'ont jamais cessé de progresser et dans un contexte de numérisation croissante de l'ensemble des acteurs, notre GE doit être réinventée tant dans ces outils, que dans ses modes d'action ou ses organisations. Dans un esprit d'innovation, ces évolutions pourront s'appuyer sur l'apport de nouvelles technologies comme les armes à énergie dirigée ou l'intelligence artificielle. Elles seront surtout le fruit d'une évolution vers un emploi plus offensif et une recherche de la complémentarité avec une cyberdéfense tactique, qui reste encore à développer. Ces évolutions doivent également nous amener à réfléchir autrement au réalisme de notre entraînement et surtout à notre relation à la numérisation et à notre conception du commandement en opérations.

Éléments de bibliographie

ANDREW Christopher et MITROKHINE Vassili, *Le* KGB *contre l'Ouest, 1917-1991*, Arthème-Fayard, 2000, 982 pages.

BONNEMAISON Aymeric et DOSSÉ Stéphane, *Attention : Cyber ! Vers le combat cyber-électronique*, Économica, 2014, 217 pages.

CAVE BROWN Anthony, *La Guerre secrète, T.2 : Le Jour J et la fin du III^e* Reich, Perrin, 2012, 714 pages.

FORCADE Olivier et LAURENT Sébastien, *Secrets d'État : pouvoirs et renseignement dans le monde contemporain*, Armand Colin, 2005, 238 pages.

LASTOURS (DE) Sophie, *La France gagne la guerre des codes secrets 1914-1918*, Tallandier, 1998, 262 pages.

LIANG Qiao et XIANGSIU Wang, *La Guerre hors limites*, Payot et Rivages, 2006, 309 pages.

LE PAGE Jean-Marc, *Les Services secrets en Indochine*, Nouveau Monde éditions, 2014, 522 pages.

MALIS Christian, *Guerre et stratégie au XXI^e siècle*, Fayard, 2014, 352 pages.

SOUTOU Georges-Henri, FRÉMEAUX Jacques et FORCADE Olivier (dir.), *L'Exploitation du renseignement*, Économica, 2001, 332 pages.

THOMSON David, *Les Revenants*, Seuil, 2016, 336 pages.