Études de l'Ifri

Focus stratégique 90

REGARDS CROISÉS SUR LA GUERRE ÉLECTRONIQUE

Olivier LETERTRE

Patrick JUSTEL

Romain LECHÂBLE

Stéphane DOSSÉ

Juillet 2019

ifri 1979 2019

Laboratoire de Recherche sur la Défense

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

ISBN : 979-10-373-0052-2

Comment citer cette publication :

Olivier Letertre, Patrick Justel, Romain Lechâble et Stéphane Dossé, « Regards croisés sur la guerre électronique », *Focus stratégique*, n° 90, Ifri, juillet 2019.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Focus stratégique

Les questions de sécurité exigent une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection ***Focus stratégique***, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, ***Focus stratégique*** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

Auteurs

Le lieutenant-colonel **Olivier Letertre** est officier de l'arme des transmissions de l'armée de Terre et est diplômé de l'école de guerre – promotion général de la Lafayette.

Le colonel **Patrick Justel** a commandé le 54e Régiment de Transmission. Il est diplômé de l'Ecole de Guerre et du CHEM, dont il était auditeur au moment de la rédaction de l'article.

Le commandant **Romain Lechâble** est actuellement détaché de l'armée de l'air au sein de Dassault Aviation où il occupe la fonction d'expert opérationnel. Pilote de chasse affecté sur Mirage 2000N en 1999 puis sur Rafale en 2006, il a exercé les fonctions d'officier rapporteur entre 2012 et 2017 au centre d'expertise aérienne militaire, avant son détachement.

Le colonel **Stéphane Dossé** est spécialisé dans le domaine de la maîtrise de l'information et a commandé le 54e régiment de transmissions. Il est co-auteur d'*Attention cyber : vers le combat cyber-électronique* (Economica, 2013).

Comité de rédaction

Résumé

Quelque peu négligée depuis la fin de la guerre froide, la guerre électronique est redevenue un aspect crucial des conflits contemporains. Tirant désormais pleinement profit de la dynamique de numérisation du champ de bataille, le spectre électromagnétique est profondément modifié par la révolution des technologies de l'information, et présente à ce titre un très fort potentiel militaire. Mais ces perspectives sans précédent s'accompagnent de menaces et de besoins inédits, auxquels devront répondre de nouvelles exigences capacitaires et opérationnelles. Face à des adversaires de plus en plus performants, l'approche occidentale de la guerre électronique doit être réinventée. En particulier, la proximité croissante entre télécommunications et informatique suscite un véritable continuum cyber-électronique, dont la convergence opérationnelle pourrait être davantage exploitée. Pour préserver leur domination informationnelle, les armées occidentales doivent alors se donner les moyens de développer des systèmes de guerre électronique toujours plus innovants.

Abstract

Although somewhat neglected since the end of the Cold War, electronic warfare has become a crucial aspect of contemporary conflicts again. But as modern battlefield is now undergoing widespread digitization, so is the electromagnetic spectrum which has been deeply transformed through the information technology revolution, thus showing an even greater military potential. However, these unprecedented opportunities come along with new threats and challenge, which only to be met by intensive capability and operational developments. Faced with increasingly tough opponents, Western approach to electronic warfare must be reinvented. In particular, the growing proximity between telecommunications and the digital realm has brought about a cyber-electronic continuum, whose operational convergence could be better used. To preserve their information dominance, Western militaries must equip themselves with the means of developing ever more innovative electronic warfare systems.

Sommaire

INTRODUCTION 9

GUERRE ÉLECTRONIQUE OU GUERRE DANS L'ENVIRONNEMENT ÉLECTROMAGNÉTIQUE ? (O. LETERTRE) 11

Un environnement électromagnétique bouleversé par la numérisation 11

Un cadre d'emploi de la guerre électronique toujours exigeant 14

LA GUERRE ÉLECTRONIQUE, UNE QUESTION D'AVENIR (P. JUSTEL) 17

Un champ marqué par l'évolution technologique 18

De nouvelles perspectives 21

Conclusion 31

LA GUERRE ÉLECTRONIQUE DANS L'ESPACE AÉRIEN (R. LECHÂBLE) 33

Un rapide aperçu historique 34

Perspectives stratégiques actuelles 36

Illustration technique 36

Exigences opérationnelles 39

Conclusion 43

L'AVÈNEMENT DU COMBAT CYBER-ÉLECTRONIQUE (S. DOSSÉ) 45

Le rapprochement de la guerre électronique et du domaine cyber ... 46

Une convergence opérationnelle 47

Le combat cyber-électronique et les principes de la guerre 49

Conclusion 51

Introduction

La « révolution dans les affaires militaires » qui a assuré le succès tactique et opératif des armées occidentales depuis la fin de la guerre froide était avant tout le produit d'une domination informationnelle, autrement dit la capacité à mieux comprendre l'environnement que son adversaire. Cela passe par une supériorité dans la connaissance de l'ennemi : avec le développement de capteurs en tous genres, capables de recueillir une grande quantité de données sur l'adversaire et de les transmettre en un temps aussi réduit que possible à ses effecteurs, lesquels ainsi renseignés pourront traiter les cibles de façon de plus en plus précise. Mais il s'agit aussi d'une supériorité dans la « connaissance de soi » : le positionnement de ses propres forces et celui de ses alliés, ainsi que la capacité à communiquer avec eux pour manœuvrer avec une rapidité fulgurante, imposant ainsi le tempo des opérations.

Quel que soit le milieu concerné, cette supériorité informationnelle passe par une domination de l'environnement électromagnétique à travers lequel circulent ces informations. Le développement continu depuis le milieu des années 1990 de capacités de guerre électronique susceptibles de contester l'exploitation du champ électromagnétique et par là même de remettre en cause la domination informationnelle, est apparu au grand jour et de façon spectaculaire au cours des dernières années. Les récentes opérations en Ukraine, en Syrie et ailleurs ont transformé notre perception du « rapport de force électronique » vis-à-vis de puissances militaires étatiques comme la Russie ou la Chine mais aussi de certains acteurs non étatiques, parfois qualifiés d'« hybrides » dans la littérature stratégique. Cette réévaluation de la menace doit nous interroger sur la soutenabilité d'un modèle de plus en plus dépendant des technologies de l'information qui tient encore trop souvent pour acquise la sécurité des communications et l'avantage en matière de renseignement, de surveillance, de reconnaissance et d'acquisition de cibles (regroupées en anglais sous l'acronyme ISTAR).

Pour autant, il demeure difficile, en France comme ailleurs, de traiter ces sujets, légitimement soumis au devoir de réserve, aux contraintes du secret industriel et de la sécurité opérationnelle. Dans ce domaine comme dans d'autres, ceux qui savent s'expriment peu et ceux qui écrivent manquent d'accès aux informations. C'est la raison pour laquelle la collection *Focus stratégique* a fait le choix de donner la parole à quatre officiers spécialistes de guerre électronique afin qu'ils apportent chacun leur

perspective à ces « regards croisés ». Le lieutenant-colonel Olivier Letertre propose ici une introduction générale à la problématique de la guerre électronique en la replaçant dans les évolutions perpétuelles de l'environnement électromagnétique. À sa suite, le colonel Patrick Justel fait le point sur l'état des enjeux stratégiques et capacitaires actuels de la guerre électronique avant de tracer des axes d'évolutions à l'avenir. Le commandant Romain Lechâble se concentre quant à lui sur la guerre électronique dans l'espace aérien, tirant lui aussi des conclusions prospectives pour ce milieu concerné au premier chef par la lutte informationnelle. Enfin, le colonel Stéphane Dossé conclut en s'attachant à mettre en avant la réalité comme les limites d'une « grande convergence » cyber-électronique.

Guerre électronique ou guerre dans l'environnement électromagnétique ?

Par le Lieutenant-colonel Olivier Letertre

Au moment où le rôle clé de la guerre électronique française durant le premier conflit mondial est mis en lumière[1], la guerre électronique constitue toujours un élément incontournable du champ de bataille moderne. Cet état de fait perdure parce que la guerre électronique possède une capacité de mutation souple pour rester pleinement efficace dans deux mondes, militaire et technologique, régulièrement bouleversés par des révolutions successives. Les indices de cette évolution réussie apparaissent aussi nombreux que récents. La mise en œuvre d'équipements de guerre électronique rapportée à plusieurs reprises dans les crises ukrainienne et syrienne en est un exemple. Elle met ainsi en avant l'influence directe et indirecte sur les actions militaires d'une composante vouée d'habitude à la plus grande discrétion[2]. Assurer un état des lieux synthétique et global de la guerre électronique implique de présenter la complexité du spectre électromagnétique, puis de mettre en exergue les difficultés présentes face à un adversaire toujours plus connecté, réactif et résilient et d'examiner enfin les facteurs clés qui pérennisent cette capacité reconnue mais exigeante.

Un environnement électromagnétique bouleversé par la numérisation

Au cours du siècle écoulé, depuis les balbutiements des réseaux radios militaires de la Première Guerre mondiale qui ont marqué la première exploitation militaire du spectre électromagnétique, son usage s'est considérablement étoffé avec une très nette accélération sur les quarante dernières années. Cet usage se caractérise désormais par l'utilisation de toutes les gammes de fréquences utilisables dont l'acquisition et la mise à

1. J.-M. Degoulange, *Les Écoutes de la victoire. L'histoire secrète des services d'écoute français (1914-1918)*, Paris, Pierre de Taillac, 2019.
2. L. Lagneau, « La guerre électronique prend de plus en plus d'importance dans les opérations navales », *Zone militaire*, 13 août 2008, disponible sur : www.opex360.com.

disposition sont devenues des enjeux majeurs pour une industrie mondiale des télécommunications devenue un acteur économique de premier lui-même tiré par un marché du numérique en constante expansion[3]. Un simple exemple pour illustrer cela : en 2016, la dernière vente réalisée en France des « fréquences en or » (gamme des 700 MHz) a rapporté à l'État 2,8 milliards d'euros – soient 300 millions d'euros de plus qu'escompté[4]. Cette transaction particulièrement favorable à l'État est destinée à promouvoir la téléphonie 4G et à mieux préparer l'arrivée prochaine de la 5G a ainsi démontré le poids financier de cette industrie au sein de l'hexagone.

L'exploitation toujours plus poussée du spectre électromagnétique est la conséquence de l'évolution accélérée des nouvelles technologies de l'information et de la communication (NTIC). La diversité toujours plus grande des moyens de communication, l'affirmation d'internet comme un des vecteurs planétaires de l'information, l'émergence rapide de la téléphonie mobile[5] ont suscité une densification massive des données avec une nécessité de garantir des débits qui ne cessent de croître.

Les conséquences militaires de ces évolutions ne se sont pas fait attendre : dès 2003, la mise en œuvre d'un drone MALE de type MQ-1 *Predator* depuis les États-Unis utilisait en moyenne cinq fois plus de bande passante que ce que consommait l'ensemble des forces américaines pendant la première guerre du Golfe moins de quinze ans auparavant[6]. En parallèle, l'émergence de la téléphonie mobile bouleversait durablement le quotidien de chacun et permettait de passer en l'espace de 10 ans de communications exclusivement phoniques (2G) à des échanges massifs de données (4G) avec des débits près de 15 000 fois supérieurs : le téléchargement d'un fichier DivX passant ainsi théoriquement de 7,2 jours à seulement quelques minutes[7]. Les médias échangés sont ainsi devenus de plus en plus nombreux, plus variés, pour constituer un « mur de données » qui n'a eu de cesse de s'accroître.

Cette augmentation phénoménale des débits et de la masse d'information échangée par les ondes en format numérique a aussi renforcé les synergies avec le cyberespace qui prolonge le spectre électromagnétique. Il ne s'agit plus seulement de communiquer, de transmettre ou de stocker

3. B. Texier, « Numérique : un marché mondial de 4 261 milliards d'euros », *Archimag*, 7 juin 2016, disponible sur : www.archimag.com.
4. P. Manière, « Vente de fréquence 4G : c'est terminé ! », *La Tribune*, 17 novembre 2015.
5. « Le nombre d'abonnés au téléphone mobile dans le monde », *Journal du Net*, 21 juin 2018, disponible sur : www.journaldunet.com.
6. *Annuaire stratégique et militaire* 2004, Paris, Fondation pour la Recherche Stratégique/Odile Jacob, 2004, p. 58.
7. D. Nussbaum, « Le débit des téléphones portables : de la 1G à la 4G », *Futura Sciences*, 11 décembre 2015, disponible sur : www.futura-sciences.com.

mais aussi de recevoir et de donner des instructions. Les applications sont nombreuses, dans le monde militaire comme dans le monde civil. La maturité des technologies permet ainsi d'envisager à court terme le passage de la numérisation à l'info-valorisation sur le champ de bataille laquelle offre au chef militaire un niveau d'appréciation encore jamais vu de la situation et de l'évolution de son environnement de combat. Les applications civiles ou dérivées sont encore plus rapides, plus nombreuses allant de la domotique à la robotique en passant aujourd'hui le nouvel internet des objets connectés.

Dynamisé par ce marché mondial du numérique innovant, le champ d'application théorique de la guerre électronique ne cesse de s'élargir. C'est aussi ce contexte particulièrement favorable qui est offert à un belligérant qui peut aisément mettre en œuvre des systèmes d'information et de communication (SIC) dont il a besoin.

Pour les armées conventionnelles, cette évolution résulte de la nécessité absolue de raccourcir les processus décisionnels, d'optimiser l'action militaire en préservant ses effectifs, de prendre et de conserver l'ascendant et l'initiative sur l'adversaire dans une course opérationnelle stratégique et tactique dont le rythme s'est considérablement accéléré. En ce qui concerne les acteurs irréguliers (guérillas, groupes armés, organisations terroristes), la maîtrise des NTIC leur permet par exemple de s'assurer d'une couverture médiatique plus large après une action violente et de compenser leurs faiblesses opérationnelles intrinsèques. Si les buts et les moyens sont différents, le passage par les SIC est désormais universel et commun.

L'armée américaine a été la première à accorder une place prépondérante à la numérisation dans le quotidien de ses opérations. Jamais depuis lors, cette place prépondérante n'a été remise en cause. Bien au contraire. Selon la *Defense Advance Research Projects Agency* (DARPA), le combat de demain sera piloté à distance par l'intelligence artificielle dans un espace entièrement numérisé au sein d'un *cloud* interarmées[8]. Les SIC y joueront alors nécessairement un rôle clé. Mais le Pentagone a aussi pris conscience de ses vulnérabilités dans ce domaine. Les crises ukrainienne et syrienne ont ainsi mis en avant l'existence très probable de capacités de guerre électronique des plus performantes. Cela a entraîné *ipso facto* un réinvestissement dans le domaine de la guerre électronique passé au second plan depuis quinze ans et les guerres contre insurrectionnelles d'Irak et en Afghanistan[9].

L'existence de moyens de guerre électronique suffisamment performants avec les capacités nécessaires pour délivrer les effets tactiques

8. N. Pauline, « L'armée américaine livre sa vision de la guerre du futur », *Les Échos*, 11 septembre 2018.
9. L. Lagneau, « L'*US Army* a testé des capacités de guerre électronique en Europe lors de l'exercice Saber Strike », *Zone militaire*, 3 juillet 2018, disponible à l'adresse : www.opex360.com.

escomptés ne présente toutefois pas une garantie absolue d'efficacité. La dualité des technologies et le foisonnement des solutions techniques offrent de nombreuses possibilités d'esquive pour un ennemi apte et déterminé : il s'avère par exemple difficile, voire impossible, d'interdire à l'ennemi de communiquer. Se fondant dans la masse du trafic de données pour garantir son anonymat, optimisant les plateformes alternatives comme le *Dark Web* ou assurant plus simplement l'exploitation maîtrisée des systèmes de communication disponibles dans le monde entier, l'ennemi peut assurer la pérennité de ses échanges à moindre coût et avec un risque mesuré. Daech l'a bien compris : recourant vraisemblablement à des accès internet fournis par satellites[10] et à des applications d'échanges, il a pu durablement poursuivre la diffusion de ses vidéos de propagande.

Un cadre d'emploi de la guerre électronique toujours exigeant

Portés directement ou indirectement par une industrie numérique en croissance exponentielle, les progrès techniques permanents ont démultiplié le champ d'action possible de la guerre électronique. Pour rester pertinente, celle-ci doit agir et évoluer selon des priorités et des axes déterminés ; un espace global normé au sein duquel elle doit concentrer l'ensemble de ses efforts.

Un cadre réglementaire et doctrinal doit être défini car l'intégration de la guerre électronique en appui aux opérations nécessite des règles d'engagement et une coordination toujours plus fine pour optimiser les effets. Un cadre réglementaire tout d'abord car la guerre électronique, comme toutes les composantes militaires, de par l'importance des incidences possibles de son action sur l'adversaire et sur l'environnement, se doit d'être bornée pour permettre d'en conserver l'entière maîtrise en conformité avec ce qu'autorise le droit. Pour la France, la loi du 24 juillet 2015 relative au renseignement[11] constitue une de ces garanties formelles de la bonne adéquation entre les moyens employés, l'effet recherché et la préservation des libertés. Un cadre doctrinal aussi car dans le spectre capacitaire souvent large de la guerre électronique, il faut prévoir, concevoir, formaliser et mettre en œuvre son apport, en association avec d'autres composantes ou seules, pour le succès de la mission confiée dans des cas spécifiques et attentivement étudiés. C'est ce que tendrait à démontrer la plupart des actions militaires récentes. La mise en œuvre de moyens de

10. J. Darmanon, « L'État islamique passerait par des satellites européens pour se connecter au web », *Le Figaro*, 10 décembre 2015.
11. « Loi du 24 juillet 2015 relative au renseignement », 1er décembre 2015, disponible à l'adresse : www.vie-publique.fr.

guerre électronique vraisemblablement utilisés sur des objectifs sélectionnés a eu récemment pour effet notable de contribuer à entretenir une forme de brouillard de la guerre à un moment de l'action militaire où la connaissance reste un point clé de celle-ci[12].

Cette réalité capacitaire passe toutefois par un investissement technique – et donc financier – important qui s'avère vital pour maintenir des capacités de guerre électronique qui, dans un monde SIC et numérique en constante évolution, se doivent d'être évolutives.

À défaut d'anticiper systématiquement chaque évolution des SIC, la guerre électronique se doit tout au moins de les suivre afin de s'adapter à l'adversaire et à ses modes d'action. Cela nécessite une base industrielle et technologique de défense (BITD) capable d'élaborer et de conduire, seule ou en association, de grands programmes de guerre électronique avec la volonté d'un investissement conséquent dans la durée. En 2017, la société russe KRET aurait ainsi reçu mandat pour moderniser près de 60 % des équipements de guerre électronique russe à l'horizon 2020[13], un objectif programmatique qui démontre l'ambition de Moscou. L'armée américaine estime pour sa part que son sous-investissement relatif dans la guerre électronique – 0,8 % de son budget militaire[14] – a suscité un retard indéniable dans certaines capacités. Cet effort programmatique peut s'accompagner utilement d'une démarche proactive d'achat d'équipements sur étagère voire de nouvelles technologies en fonction de leur apparition sur le marché. Il convient ainsi de tout mettre en œuvre afin de contrer un immobilisme technologique synonyme, à très court terme, de décrochage capacitaire difficilement réversible.

Par-delà ces enjeux matériels, les performances opérationnelles de la guerre électronique dépendent des spécialistes qui la mettent en œuvre. Leurs profils sont d'emblée remarquables et requièrent des qualités techniques et tactiques particulières, souvent de très haut niveau.

Ces opérateurs doivent en effet pouvoir servir tout une gamme d'équipements pour obtenir des effets de renseignement et d'agression déterminés sur une vaste gamme d'ennemis. Leurs savoir-faire techniques ne sont jamais figés. Le spécialiste guerre électronique peut être ainsi amené, en quelques années, à servir plusieurs matériels faisant appel à des technologies différentes qu'il doit impérativement maîtriser. Les savoir-faire tactiques sont aussi nécessaires qu'ils sont variés et exigeants. Le spécialiste guerre électronique doit savoir appuyer tout type d'unité à différents niveaux

12 « Moscou cible le C4I et les missiles de croisière de l'OTAN », *TTU*, 27 avril 2018.
13 « Guerre électronique : le laboratoire ukrainien », *TTU*, 19 juin 2017.
14 « Le bel avenir de la guerre électronique », *TTU*, 20 avril 2016.

et fournir des effets différenciés selon qu'il agit pour un commandement stratégique ou pour un groupe tactique, seul ou bien encore associé à d'autres composantes de recherche du renseignement ou d'action. Le grand écart est ainsi double : par la diversité des équipements servis et par la diversité des effets à produire, seuls ou intégrés à une manœuvre d'ensemble plus large impliquant d'autres acteurs. De fait et notamment pour la guerre électronique française, la spécialité « guerre électronique » passe pour le personnel des trois armées par des parcours professionnels, des formations et des écoles spécifiques. Cela exige un investissement important en formation spécialisée, complexe et réactive afin de garantir un vivier de ressource humaine pleinement opérationnel.

Jamais la matière première de la guerre électronique – l'information – n'aura été aussi importante en volume comme en diversité. Jamais la portée même des actions de la guerre électronique n'a été potentiellement aussi déterminante. La pleine exploitation du terreau numérique, de la digitalisation et de l'info-valorisation nécessite de suivre au plus près des progrès technologiques qu'il faut immédiatement intégrer, décliner pour maintenir des équipements hautement performants, servis par des spécialistes aux compétences complètes, évolutives et maîtrisées.

Ces enjeux sont aujourd'hui essentiels car pour l'ensemble des belligérants, la libre utilisation du spectre électromagnétique conditionne en partie l'affirmation de leur puissance[15].

15. « Guerre électronique : la réponse aux menaces hybrides ? », *TTU*, 26 octobre 2017.

La guerre électronique, une question d'avenir

Par le Colonel Patrick Justel

La doctrine française définit la guerre électronique comme « tout ce qui a trait aux opérations de combat effectuées dans l'environnement électromagnétique[16] ». En effet, cet environnement est utilisé en permanence pour de nombreuses capacités opérationnelles, telles que les télécommunications, le recueil du renseignement ou la navigation. Comme dans tout champ de bataille, on peut y attaquer[17] et surveiller[18] l'ennemi, ou au contraire s'en défendre[19]. Historiquement, les premières actions de guerre électronique datent de la guerre russo-japonaise de 1904-1905[20]. En France, elles débutent avec la Première Guerre mondiale, apportant des contributions décisives au cours de batailles cruciales, à l'instar de Verdun[21]. Elle a également joué un rôle clé pendant la Seconde Guerre mondiale[22] et a fait l'objet d'une attention particulière dans les deux blocs au cours de la guerre froide[23]. Malgré cet héritage relativement ancien, la guerre électronique est aujourd'hui confrontée à de nombreux défis.

---

16. 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. PIA-3.6.1, *Maîtrise de l'environnement électromagnétique*, Paris, CICDE, 6 avril 2016 ; DIA 3-6, *La Guerre électronique*, Paris, CICDE, 20 octobre 2017.
17. L'attaque électronique consiste en l'emploi de l'énergie électromagnétique à des fins offensives.
18. La surveillance électronique consiste à employer l'énergie électromagnétique afin de contribuer à la connaissance de situation et à la collecte de renseignement.
19. La défense électronique 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.
20. A. Bonnemaison et S. Dossé, *Attention : Cyber ! Vers le combat cyber-électronique*, Paris, Economica, 2014, p. 70.
21. 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 guerre électronique pendant ce conflit. « Hommage aux hommes de l'ombre », *Association de la guerre électronique de l'armée de Terre*, 3 janvier 2015, disponible sur : ageat.asso.fr.
22. Par exemple, le service « Y » britannique s'illustra en Afrique face à Rommel. A. Clayton, « Le Renseignement militaire britannique pendant la Seconde Guerre mondiale », *in* G.-H. Soutou, J. Frémeaux, O. Forcade (dir.), *L'Exploitation du renseignement*, Paris, Economica, 2001, p. 172.
23. C. Andrew et V. Mitrokhine, *Le KGB contre l'Ouest, 1917-1991*, Paris, Arthème-Fayard, 2000, pp. 495-522.

Un champ marqué par l'évolution technologique

Face à la menace de la guerre électronique, la première réponse consiste souvent à arrêter complètement les émissions, ou à basculer sur des moyens 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 belligérant plus organisé pourra également essayer d'intoxiquer son adversaire en diffusant de fausses informations. C'est ainsi par exemple qu'en 1944, les Alliés parvinrent à induire en erreur le renseignement allemand sur l'imminence du Débarquement[24]. Plus récemment, lors des opérations de la Force Internationale d'Assistance à la Sécurité (FIAS) en Afghanistan, les Talibans se sont souvent livrés à des tentatives d'intoxication par le biais d'émissions radio pour détourner l'effort des forces de la coalition vers d'autres secteurs quand ils étaient mis en difficulté.

Ce défi peut être aggravé par la publicité parfois donnée à l'information recueillie par surveillance électronique. En effet, le besoin de communiquer sur nos succès ou la nécessité d'expliquer certaines actions peuvent révéler à l'ennemi qu'il est surveillé. Ce fut le cas par exemple lors de l'assaut sur le *Tanit* en avril 2009, au cours duquel l'un des otages perdit la vie. La décision d'intervenir fut justifiée publiquement par le contenu de la surveillance électronique, les écoutes montrant « un durcissement très net de la position des pirates qui évoquaient de manière plus insistante l'exécution des otages et la destruction par explosif du bateau et leur volonté inflechissable de se rapprocher des côtes[25] ».

La deuxième évolution notable tient à la complexité croissante des moyens de communication et de détection. Des techniques aujourd'hui largement diffusées comme le chiffrement[26] ou l'évasion de fréquence peuvent rendre la tâche ardue aux opérateurs de guerre électronique, 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 actuels de guerre électronique.

24. A. Cave Brown, *La Guerre secrète. Le jour J et la fin du IIIe Reich*, Paris, Perrin, 2012, pp. 94-95.
25. « Tanit : pourquoi les commandos ont donné l'assaut », *Le Parisien*, 10 avril 2009, disponible sur : www.leparisien.fr.
26. S. Seibt, « Attentats de Paris : Bitcoin, crypto et une start-up américaine critiqués », *France 24*, 20 novembre 2015, disponible sur : www.france24.com.

La guerre électronique, orpheline de la guerre froide

Au cours des opérations de la période 1990-2010, la guerre électronique française s'est souvent concentrée 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 tenir pour acquis ce qui était considéré, du temps de la guerre froide, comme un enjeu majeur : la protection des moyens de commandement et de navigation.

En effet, dans les opérations de contre-insurrection menées contre des adversaires irréguliers d'un niveau technologique limité, les forces occidentales disposaient d'une liberté d'action quasi-totale dans l'environnement électromagnétique. La défense électronique des moyens de communication s'est donc concentrée sur l'utilisation de technologies sécurisées, en mettant de côté d'autres méthodes de protection ou l'entraînement à travailler dans un environnement électronique dégradé. Dans une étude sur les modes d'action russes dans le conflit ukrainien, l'*Asymmetric Warfare Group* de l'*US Army* liste les faiblesses occidentales face à la guerre électronique adverse[27] :

- des postes de commandement trop grands, facilement détectables et peu mobiles, donc particulièrement vulnérables face à la guerre électronique et aux attaques d'un ennemi symétrique ;
- un commandement trop centralisé et trop dépendant des systèmes de communication ;
- un manque d'entraînement au combat en ambiance de brouillage.

L'attaque électronique (brouillage de l'adversaire, écoute et intoxication) a, elle aussi, été progressivement délaissée au cours des années de « basse intensité », à quelques exceptions près. Ainsi, la multiplication des engins explosifs improvisés (EEI) radiocommandés a entraîné un regain d'intérêt pour le brouillage terrestre en vue de la protection des véhicules. Dans ce nouveau contexte, l'attaque électronique contre les réseaux adverses a aussi pu être employée, mais toujours de manière limitée.

27. U.S. Army, Asymmetric Warfare Group, *Russian New Generation Warfare Handbook*, Version 1, Washington, décembre 2016.

En France, les capacités de brouillage offensif existent dans le milieu terrestre mais restent insuffisantes. Elles sont en revanche inexistantes dans les milieux aérien et maritime[28]. Il s'agit sans doute des domaines où les armées françaises connaissent les carences les plus graves. Le constat de ce retard, partagé par la plupart des armées de l'OTAN, a d'ailleurs conduit le général Breedlove, alors Commandant Suprême des forces alliées en Europe (SACEUR), à tirer la sonnette d'alarme en février 2016, appelant les membres de l'Alliance atlantique à réagir[29].

La guerre électronique remise en cause par la cyberdéfense ?

Le lien entre la guerre électronique et la cyberdéfense militaire est la conséquence logique du rapprochement des mondes des télécommunications et de l'informatique[30]. Cette convergence n'est que la nouvelle étape d'un long processus : les différents domaines du combat sur les réseaux étaient jusqu'alors séparés pour des raisons historiques et de formation du personnel. Aujourd'hui, la convergence des réseaux filaires et radio, associés aux chiffrements, implique un nécessaire rapprochement de la guerre électronique et du cyber[31]. C'est pourquoi certains pays ont fait le choix de subordonner leurs unités de guerre électronique à des commandements cyber. Afin de coordonner les compétences de la Bundeswehr en matière de cyberdéfense, l'Allemagne a par exemple décidé de se doter d'un Commandement du Cyberespace et de l'Information (KdoCIR) qui exerce également son autorité sur les unités de guerre électronique[32]. Ce choix peut aussi s'expliquer par des contraintes budgétaires et humaines, les deux domaines pouvant faire appel aux mêmes spécialités rares (linguistes, analystes, etc.). Sur ce terrain, la guerre électronique s'est retrouvée en compétition avec la cyberdéfense.

28. Certains bâtiments de la marine nationale disposent néanmoins de capacités de brouillage radar à vocation défensive, qui pourraient être utilisées de manière offensive.
29. D. Majumdar, « Electronic Warfare: Russian Gains Threaten to 'Disconnect' US Forces », *The Buzz*, 25 février 2016, disponible à l'adresse : nationalinterest.org/blog.
30. DIA 3-20, *La cyberdéfense*, Paris, CICDE, 21 juin 2016. 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.
31. A. Bonnemaison et S. Dossé, *Attention : Cyber ! Vers le combat cyber-électronique*, *op. cit.*
32. L. Lagneau, « L'armée allemande se dote d'un commandement « Cyberespace et Information », *Zone militaire*, 1er avril 2017, disponible à l'adresse : www.opex360.com.

De nouvelles perspectives

À partir de 2014, les pays de l'OTAN ont pris conscience du retard qu'ils avaient accumulé face à la Russie. Le changement de posture de cette dernière en 2014 a été révélateur de l'atout majeur que peuvent constituer les unités de guerre électronique dans les nouvelles formes de conflictualité. Cette évolution a notamment conduit l'*US Army* à redéployer des moyens de guerre électronique terrestres en Europe[33]. L'importance de l'environnement électromagnétique est aussi apparue lors des opérations au Levant, avec notamment la nécessité pour les forces de la Coalition de s'adapter à des environnements où le brouillage était très présent[34].

Un nouvel environnement, de nouvelles menaces

Le conflit en Ukraine à partir de 2014 a été l'occasion de constater les progrès de la guerre électronique russe, employée en appui des forces séparatistes. Son efficacité a surpris non seulement l'armée ukrainienne mais aussi les observateurs occidentaux. Ils illustrent la manière dont la Russie a tiré les leçons des derniers conflits où les armées occidentales ont été engagées. Sa stratégie vise ainsi à tirer le meilleur parti des vulnérabilités de ce que l'on présente habituellement comme leur principal avantage – leur capacité à travailler en réseau et à frapper avec précision[35].

Toujours d'après l'étude de l'Asymetric Warfare Group de l'*US Army*, L'armée russe a transformé son modèle de guerre électronique en l'intégrant dans un complexe « reconnaissance-frappe » combinant les capacités les plus modernes (drones, snipers, artillerie longue portée[36]). En Ukraine, la guerre électronique a trouvé des applications sur l'ensemble du spectre capacitaire, avec des dominantes comme le brouillage en vue de la protection de force ou le leurrage de l'adversaire. Dans le cas du brouillage, les capacités de guerre électronique servaient à leurrer les missiles adverses ou à déclencher l'explosion prématurée des munitions. Il s'agissait également

33. C. Heininger, « U.S. Army's new electronic warfare capabilities hit the ground in Europe », *U.S. Army*, 6 février 2018, disponible sur : www.army.mil.
34. 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. PIA-3.6.1, *Maîtrise de l'environnement électromagnétique*, Paris, CICDE, 6 avril 2016.
35. P. Breedlove, cité *in* D. Majumdar, « Electronic Warfare: Russian Gains Threaten to 'Disconnect' US Forces », *op. cit.*
36. R.N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*, Tallinn, International Centre for Defence and Security, Estonian Ministry of Defence, septembre 2017.

d'attaquer les moyens de communication, de localisation (GPS) et de renseignement ennemis (drones) afin de rendre ce dernier aveugle[37].

Les forces russes se sont aussi montrées très habiles pour exploiter de la guerre électronique à des fins de déception ou de manipulation. Une étude récente évoquait la diffusion massive des SMS personnalisés annonçant à des soldats ukrainiens la mort d'un proche. En plus de provoquer la démoralisation, cette manœuvre pouvait conduire les soldats ukrainiens à émettre avec leur téléphone portable et de cette manière révéler leur position pour permettre le guidage de l'artillerie[38].

Le milieu terrestre n'a pas été le seul concerné par la guerre électronique sur le théâtre ukrainien. L'incident américano-russe survenu en mer Noire le 30 avril 2014 illustre l'aspect dissuasif et psychologique que peuvent recouvrir les actions de guerre électronique dans le domaine aéronaval. Un avion SU-24 équipé d'un pod *Khibiny* serait ainsi parvenu à éteindre le radar et le système de transmission de données de dernière génération qui équipent l'*USS Donald Cook*. Si cette information a été démentie par l'*US Navy*[39] et semble relever de la propagande[40], elle illustre aussi la vulnérabilité des armées occidentales face à une menace qui pourrait les déconnecter de leurs réseaux.

Des actions de guerre électronique 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 perturbé[41]. Ces incidents ont été considérés comme le résultat d'actions de brouillage russes lors de l'exercice

37. U.S. Army, Asymmetric Warfare Group, *Russian New Generation Warfare Handbook*, Version 1, Washington, décembre 2016.

38. J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, *Les Manipulations de l'information : un défi pour nos démocraties*, Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018

39. « NavWeek: Jammed Up », *Aviation Week*, 25 novembre 2014, disponible sur : aviationweek.com.

40. Plusieurs sites américains et russes affirment que le complexe Khibiny évoqué dans les médias n'équipe que les SU-35, SU-34 et SU-30 et sert à l'autoprotection. G. Leopold, « Fake Russian EW attack unmasked », *defensesystems.com*, 12 mai 2017, disponible sur : defensesystems.com ; Р. Скоморохов, « Комплекс РЭБ «Хибины» чудо-оружие армии России? », *Военное обозрение*, 31 octobre 2017, disponible sur : topwar.ru.

41. J. Trevithick, « Russia Jammed Phones and GPS in Northern Europe During Massive Military Drills, *The Drive*, 16 octobre 2017, disponible sur : www.thedrive.com.

Zapad 2017[42]. Dans la même région, les téléphones mobiles des militaires de l'OTAN ont fait l'objet d'attaques ciblées également attribuées à la Russie[43].

L'autre théâtre dans lequel la guerre électronique est redevenue un sujet brûlant est la Syrie, où les forces russes ont également démontré leur savoir-faire et leurs moyens en la matière. Outre les capacités embarquées à bord des aéronefs et des bâtiments[44], on peut citer le déploiement de moyens terrestres *Krasukha-4* disposant de capacités de brouillage GPS et radar, et de lutte anti-drones[45]. Initialement destinées à gêner les aéronefs et les moyens de renseignement de la Coalition, ces capacités semblent également avoir été utilisées contre les treize mini-drones armés qui ont attaqué la base Hmeimim en janvier 2018[46].

Mais la guerre électronique russe n'est pas la seule à opérer au Levant. Des acteurs non étatiques tels que le Hezbollah ont démontré leurs capacités en la matière, et ce depuis la guerre de 2006 contre Israël. L'une des grandes surprises de ce conflit avait 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 du Hezbollah 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[47].

Plus récemment, les membres de la Coalition internationale contre l'État islamique ont aussi utilisé des moyens de guerre électronique[48]. Peu à peu, les puissances militaires occidentales prennent conscience que

42. 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. T. Nilsen, « Norway well prepared to meet Russian jamming », *The Barents Observer*, 14 décembre 2017, disponible à l'adresse : thebarentsobserver.com. Les autorités lettones ont quant à elles estimé que le réseau mobile avait été brouillé par les Russes depuis l'enclave de Kaliningrad, mais que ce brouillage visait plutôt l'île suédoise de Gotland. G. Gelzis et R. Emmott, « Russia May Have Tested Cyber Warfare on Latvia, Western Officials Say », *Reuters*, 5 octobre 2017, disponible sur : www.reuters.com.

43. T. Schultz, « Russia Is Hacking and Harassing NATO Soldiers, Reports Say », *dw.com*, 6 octobre 2017, disponible sur : www.dw.com.

44. D. E. Meadows, « Modern EW Capabilities Accompany Russian Forces Into Syria », *Signal Magazine*, 13 octobre 2015, disponible sur : www.afcea.org.

45. « Des armes de guerre électronique russes aperçues en Syrie », *Sputnik News*, 5 octobre 2015, disponible sur : sputniknews.com.

46. « Who Is Attacking Russia's Main Base in Syria? À New Mystery Emerges in the War », *The Washington Post*, 10 janvier 2018.

47. M. Perry et A Crooke, « Comment le Hezbollah a vaincu Israël », *conflictsforum.org*, 17 février 2011, disponible sur : www.conflictsforum.org.

48. L. Lagneau, « La guerre électronique, un autre aspect important de la lutte contre l'État Islamique », *opex360.com*, 19 décembre 2016, disponible sur : www.opex360.com.

l'environnement électromagnétique dont ils avaient librement disposé depuis la guerre du Golfe, est à nouveau un terrain contesté. La bataille de Mossoul de 2016-2017 a montré la nécessité de déployer des moyens de guerre électronique jusqu'au plus bas niveau[49]. Cette bataille est considérée par les experts américains comme un exemple de « combat multi-milieux » face à un ennemi hybride en zone urbaine[50]. Considérant que les adversaires potentiels des États-Unis ont appris à contrer leur supériorité dans les milieux qu'ils dominaient, le concept de « multi-domain operations » vise à réagir en étendant le combat simultanément à l'ensemble des milieux interarmées. Cette doctrine propose également de compléter les cinq milieux traditionnels – terre, air, mer, espace et cyberespace dans la doctrine américaine – par trois nouveaux domaines : l'environnement informationnel, la dimension cognitive et l'environnement électromagnétique.

Cette évolution est étroitement liée à la numérisation croissante des adversaires potentiels qui, en l'espace de quelques années, ont considérablement amélioré leurs capacités de commandement et de renseignement, ainsi que les possibilités de diffuser de la propagande ou d'attaquer nos propres systèmes. 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[51] ». Mais cette numérisation de l'ennemi et son recours à la guerre électronique pourraient aussi bien constituer une faiblesse, offrant en retour de nouvelles opportunités.

De nouveaux combats à mener avec de nouvelles armes

Témoignant de l'intérêt chinois pour la guerre électronique, les colonels Qiao Liang et Wang Xiangsiu affirmaient dans leur ouvrage *La Guerre hors limites* que « le spectre électromagnétique est un nouveau type d'espace de combat fondé sur la créativité technique et qui dépend de la technique[52] ». Les évolutions tactiques et technologiques doivent en effet conduire les forces françaises à adapter leur approche de la guerre électronique, en favorisant l'innovation. On pourra lister ici un certain nombre d'axes d'investissement pour s'assurer un rang de puissance de guerre électronique à l'avenir.

- L'une des priorités absolues est peut-être aujourd'hui le développement de **la lutte contre la guerre électronique adverse**. Il s'agit d'abord

49. « Éléments de RETEX de l'armée des États-Unis en guerre électronique suite à la bataille de Mossoul », Fiche, Paris, CICDE, 15 janvier 2018.
50. *Multi-Domain Battle: Combined Arms for the 21st Century. White Paper*, U.S. Army, Training and Doctrine Command (TRADOC), février 2017.
51. D. Thomson, *Les Revenants*, Paris, Seuil, 2016, p. 105.
52. Q. Liang, W. Xiangsiu, *La Guerre hors limites*, Paris, Payot & Rivages, 2006, p. 77.

de mieux s'en prémunir par les moyens classiques de défense électronique[53]. Ce combat pourrait aussi prendre des formes plus élaborées et offensives, par un ciblage systématique des moyens de guerre électronique adverses, ainsi que l'explique l'*Asymmetric Warfare Group* de l'*US Army* dans son analyse des capacités russes en la matière[54] :

> L'armée russe considère ses systèmes de guerre électronique et d'artillerie sol-air comme des capacités intégrées à tous les niveaux. En réalité, les quantités sont limitées. Ces systèmes sont souvent nouveaux et n'ont pas pu être mis en dotation dans toutes les unités. En général, la tactique de l'armée russe consiste à positionner ses systèmes de guerre électronique et de défense aérienne sur des lieux stratégiques puis à les déplacer dès la fin de leur mission pour limiter leur vulnérabilité. Perdre ne serait-ce qu'un seul de ces systèmes serait un coup significatif aux forces russes et créerait une brèche dans leur bulle de déni d'accès et d'interdiction de zone, qui pourrait être exploitée.

La localisation de ces moyens de guerre électronique pourrait apporter des renseignements intéressants sur la manœuvre adverse. En outre, compte tenu du faible nombre de ces moyens et de leur importance dans les dispositifs adverses, leur destruction pourrait perturber la manœuvre ennemie, tandis que leur leurrage aurait un fort impact sur l'appréciation de situation. Outre la destruction physique, le ciblage de ces moyens pourrait passer par des actions de déception[55] ou de masquage[56] électroniques, qui pourraient être étendues à une plus grande gamme de cibles. À titre d'exemple, les actions de déception sont plutôt utilisées dans le domaine des radars, mais rarement dans celui des communications. De telles actions pourraient alors être préparées avec un entraînement adéquat et s'appuyer sur des équipements adaptés comme des simulateurs de réseaux déployables sur le terrain[57].

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. U.S. Army, Asymmetric Warfare Group, *Russian New Generation Warfare Handbook*, *op. cit.*

55. DIA 3-6, *La Guerre électronique*, Paris, CICDE, 20 octobre 2017. 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.

56. *Ibid*. 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.

57. Ce type de simulateurs existent aujourd'hui et sont utilisés pour l'entraînement des unités de guerre électronique. Ils pourraient l'être pour des opérations de déception.

- Sur un plan plus offensif, **l'attaque électronique aéroportée**[58] est peut-être aujourd'hui l'une des principales lacunes à combler. Elle concerne les capacités aéroportées de brouillage offensif. La France ne dispose plus de tels moyens, contrairement à plusieurs de ses alliés ou adversaires potentiels. Or, ces moyens contribuent de manière déterminante aux missions de neutralisation des défenses aériennes ennemies (SEAD), qui s'attaquent au système de défense aérienne intégré de l'adversaire, composé des radars au sol (veille et engagement), des systèmes d'alerte avancée, des nœuds de communications critiques et des systèmes de défense aérienne surface-air multicouches (longue, moyenne et courte portées). La SEAD constitue en effet l'une des réponses aux capacités de déni d'accès et d'interdiction de zone en cours de dissémination, alors même que la *Revue Stratégique* de 2017 rappelle que « contrer les postures de déni d'accès et conquérir la supériorité aérienne redevient un objectif préalable à toutes les opérations[59] ». Les contributions classiques de la guerre électronique[60] comme la localisation des émetteurs ou le brouillage pourront également être complétées par des cyber-attaques[61], afin de désorganiser en profondeur le système de défense aérienne adverse.
- **La lutte contre les drones et robots** constitue un champ prometteur de la guerre électronique. Des moyens destinés à brouiller les liaisons de drones sont déjà mis en œuvre par plusieurs armées. Ils ont principalement pour effet de les aveugler ou de les obliger à se poser[62]. Ils pourraient encore être développés par la prise de contrôle des drones ou la modification des flux vidéo[63]. Les drones renvoient également à un autre domaine à explorer pour la guerre électronique de demain : la robotisation. « En 2030, les robots et systèmes autonomes seront devenus des acteurs ordinaires des opérations militaires. Ils agiront dans les champs d'affrontement physiques et le cyberespace[64] ». La guerre

58. *Ibid.*
59. *Revue stratégique de défense et de sécurité nationale - 2017*, Paris, La documentation française, octobre 2017, p. 49.
60. DIA 3-6, *La Guerre électronique*, *op.cit.* La SEAD résulte de la combinaison de deux capacités : la guerre électronique et un ensemble d'armes conventionnelles.
61. Entretien avec M. 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 S. Taillat, « Coercition et dissuasion dans le cyberespace », *Défense & Sécurité Internationale*, n° 110, janvier 2015, pp. 44-49.
62. « La *New Generation Warfare* russe à l'épreuve de la guerre en Ukraine », *Lettre du RETEX,* CDEC, n° 30, septembre 2016, pp. 5-6.
63. En obligeant par exemple un drone suicide à revenir sur celui qui le commande.
64. *Chocs Futurs : Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité*, Secrétariat général de la Défense et de la Sécurité nationale (SGDSN), avril 2017, p. 187.

électronique pourra alors naturellement trouver son utilité face à des robots télé-opérés ou télé-supervisés, avec des techniques similaires à celles de la lutte anti-drones. Elle pourrait également jouer un rôle face aux systèmes entièrement autonomes grâce à de nouveaux outils comme les armes à énergie dirigée[65]. À l'inverse, les robots pourront aussi servir de vecteurs de guerre électronique, pour des actions à proximité des cibles ou à des fins de déception électronique.

- **L'espace et les systèmes de localisation** constituent un autre axe d'avenir de la guerre électronique, alors que la compétition internationale s'accélère dans ce domaine où la dépendance informationnelle des armées ne cesse de s'accroître (communication, navigation, renseignement, etc.). Il s'agira demain de se protéger des attaques contre les systèmes de navigation comme le GPS, en se rendant capable de détecter, de localiser et de neutraliser les moyens de brouillage adverses. À l'inverse, notre guerre électronique de demain devra aussi développer ses capacités offensives, en visant d'autres systèmes de navigation que le GPS[66] et d'autres fonctions que la localisation[67]. Ces actions posent la question de la guerre électronique *dans* l'espace. En effet, si des actions sont déjà menées vers l'espace, des actions de guerre électronique entre engins spatiaux pourraient aussi être envisagées[68]. À l'heure où « s'affichent des velléités d'action militaire dans l'espace, tandis que s'y déroulent des opérations qui laissent peu de doute sur leur finalité réelle[69] », la guerre électronique dans l'espace permettrait d'y agir en étant difficilement détectable et sans causer de débris.

- **Armes à énergie dirigée :** l'autre type d'action que prévoit la doctrine mais qui n'est pas réalisé faute d'équipement est la neutralisation électronique[70]. Celle-ci pourra devenir une réalité avec le développement

65. « 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) » cité in *Chocs Futurs*, *op.cit.*, p. 192 ; DIA 3-6, *La Guerre électronique*, *op. cit.* Le recours offensif aux armes à énergie dirigée entre dans le cadre de l'attaque électronique.

66. Systèmes GALILEO européen, GLONASS russe, COMPASS-Beidou chinois, IRNSS indien ou QZSS japonais.

67. 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.

68. Satellites d'écoute (depuis) ou aveuglement d'un satellite au moyen d'un laser (vers). Centre National d'études spatiales (CNES), « Un satellite d'espionnage américain aveuglé par un laser chinois », *Futura Sciences*, 12 octobre 2006, disponible sur : www.futura-sciences.com.

69. *Chocs Futurs*, *op.cit.*, p. 127.

70. DIA 3-6, *La Guerre électronique*, *op. cit.* 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

des armes à énergie dirigée, dont « l'apparition dans les unités opérationnelles pourrait bien être l'amorce de la prochaine révolution militaire[71] ». Cela renforcera les capacités offensives de la guerre électronique, par la possibilité de neutraliser à distance l'adversaire.

- **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 l'intelligence artificielle[72]. Ces systèmes pourront aider les analystes à reconstituer les réseaux, à identifier des signatures électroniques ou des comportements types et à détecter des anomalies. Cependant, si ces évolutions sont annoncées depuis plusieurs années, elles restent encore à consolider et le rôle de l'être humain devrait demeurer central dans l'avenir prochain[73].

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

De nouvelles organisations en complémentarité avec la cyberdéfense

Les conflits de ces dernières années ont confirmé la nécessité d'intégrer des unités de guerre électronique jusqu'aux plus bas échelons tactiques. Un autre enseignement a été de rattacher la guerre électronique à des structures multi-capteurs[74]. 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 guerre électronique ou l'imagerie. Le choix d'une guerre électronique intégrée dans des structures multi-capteurs au sein des forces semble pertinent pour l'avenir. La principale question pour la future

arme à énergie dirigée délivrant suffisamment d'énergie électromagnétique à sa cible (ou aux composants électroniques de celle-ci) pour la rendre inutilisable.

71. *Chocs Futurs*, *op.cit.*, p. 187.

72. Des outils de ce genre sont déjà en cours de développement pour l'imagerie. *Chocs Futurs*, SGDSN, *op.cit.*, p. 106.

73. J.-C. Noël, « L'Intelligence Artificielle : vers une révolution militaire », *Focus stratégique*, n° 84, Ifri, octobre 2018.

74. La capacité multicapteurs se retrouve dans plusieurs plateformes aéroportées. Voir Allegre, « Le renseignement militaire peut-il émerger du brouillard de la guerre ? », *lavoixdunord.fr*, 7 février 2017, disponible sur : defense.blogs.lavoixdunord.fr. Elle se retrouve également dans les forces terrestres. En France, les 44e et 54e régiments de transmissions sont subordonnés au Commandement du renseignement et en Grande-Bretagne le *14th Signal Regiment* à la *1st Intelligence, Surveillance and Reconnaissance Brigade*.

organisation de la guerre électronique sera dès lors celle de son lien avec la cyberdéfense. « D'ici une vingtaine d'années, dans nombre d'armées modernes les fonctions de lutte informatique, de guerre électronique, et de transmissions auront convergé vers des organisations globales de combat cyber-électronique[75] ».

Compte tenu de l'évolution rapide des deux domaines et des multiples possibilités envisageables, les futures organisations devront procéder d'une approche empirique appuyée par une réflexion sur les différences et la complémentarité de la guerre électronique et de la cyberdéfense. 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[76] : le cyberespace[77] et le spectre électromagnétique. 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, les ondes ne sont pas le vecteur privilégié de la cyberdéfense, qui agit principalement via des réseaux filaires (fibre optique, par exemple).

Les méthodes et les procédés peuvent également être très différents, avec, pour chacun des domaines, des avantages et des inconvénients. Par exemple, les effets de la guerre électronique 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 cyberattaque peut se prolonger dans le temps. Ce fut le cas par exemple du virus *Stuxnet* qui a mis plusieurs mois à produire des effets sur la cible visée, et qui a par la suite « infecté » de nombreux autres systèmes non ciblés. La guerre électronique agit localement, à proximité de l'adversaire : c'est essentiellement un outil tactique. La cyberdéfense peut en revanche agir à distance, à grande échelle et aux niveaux tant stratégique qu'opératif ou tactique. La prise en compte de ces différences doit alimenter le développement de nouveaux modes

75. C. Malis, *Guerre et stratégie au XXIe siècle*, Paris, Éditions Fayard, 2014.
76. Dans la *Multi-domain Battle* l'environnement électromagnétique est clairement distingué du cyberespace.
77. DIA 3-20, *La Cyberdéfense*, Paris, CICDE, 21 juin 2016. Cyberespace : espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

d'action en recherchant la complémentarité de la guerre électronique et de la cyberdéfense pour l'attaque[78], la surveillance[79] et la défense[80].

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 également être utilisées dans l'avenir contre des réseaux fermés auxquels les cyberarmes n'ont pas accès. La surveillance électronique pourrait quant à elle alimenter le renseignement d'intérêt cyber en apportant des informations techniques sur les réseaux informatiques adverses. La défense électronique contribuerait enfin à la cyberprotection de nos réseaux transitant par le spectre électromagnétique, en les mettant à l'abri de la guerre électronique adverse.

En sens inverse, la cyberdéfense pourrait concourir aux actions de guerre électronique 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 cyberattaque de réseaux transitant par des câbles pourrait obliger l'adversaire à utiliser des moyens rayonnants, le rendant ainsi vulnérable à la guerre électronique. De même, un logiciel malveillant transmis par les ondes pourrait servir à attaquer la guerre électronique 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 que l'un d'entre eux ne s'efface au profit de l'autre. L'*US Army* travaille sur leur intégration dans le concept de *Cyber-Electromagnetic Activities* (CEMA), qu'elle détaille dans un manuel dédié aux « opérations dans le cyberespace et de guerre électronique[81] ». Il s'agit, à travers la complémentarité des effets cyber et guerre électronique, de transposer dans le cyberespace la logique du combat interarmes notamment par l'intégration. Ainsi les équipes cyber-électroniques américaines intègrent des spécialistes du cyber, du

78. *Ibid*. 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.
79. *Ibid*. 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.
80. *Ibid*. 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.
81. FM3-12, *Cyberspace and Electronic Warfare Operations,* Washington, Department of the Army, 11 avril 2017.

renseignement militaire, de la guerre électronique, du renseignement d'origine électromagnétique (ROEM) et parfois de l'espace pour produire ensemble des effets au profit de la manœuvre[82].

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[83]. Au niveau tactique, où notre cyberdéfense est actuellement cantonnée à la protection, des capacités de surveillance et d'attaque cyber pourraient être développées en s'appuyant sur les structures de guerre électronique des forces. Pour le niveau opératif, 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 déjà présent[84]. Ces sections peuvent notamment solliciter les capacités d'attaque et de surveillance cyber des échelons supérieurs au profit de la manœuvre de leur unité, et coordonner leurs effets avec leurs propres moyens. Dans un second temps, les unités de guerre électronique pourraient utiliser leurs capacités pour mieux exploiter le renseignement d'intérêt cyber, et servir de vecteurs pour des actions cyber offensives coordonnées au travers du spectre électromagnétique. Cette évolution aurait un double avantage : elle faciliterait la coordination des cyberattaques avec le reste de la manœuvre de la force, ainsi que l'intégration des actions de surveillance cyber dans des dispositifs de recherche multi-capteurs, en profitant de structures déjà conçues à cet effet.

Une telle solution permettrait d'éviter de disperser les ressources au niveau stratégique et d'étoffer au niveau tactique la complémentarité entre guerre électronique et cyberdéfense en appui des opérations.

Conclusion

La guerre électronique et l'environnement électromagnétique sont redevenus des enjeux d'avenir. Cette évolution est attestée par les conflits en Ukraine et au Levant, qui ont suscité une prise de conscience de nos faiblesses mais qui offrent aussi des pistes d'opportunité pour l'avenir. Face

82. Propos du général John B. Morrison Jr., chef du *Cyber Center of Excellence* à Fort Gordon, cité *in* D. Vergun, « Integrated Army Cyber Activities Teams Playing Pivotal Role in Warfare », *U.S. Army*, 9 janvier, 2018, disponible sur : www.army.mil.

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

84. « 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 » in FM3-12, *Cyberspace and electronic warfare operations, op. cit.*

à des adversaires qui n'ont jamais cessé de progresser et dans un contexte de numérisation croissante de l'ensemble des acteurs, notre approche de la guerre électronique doit être repensée tant dans ses 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. Si l'évolution actuelle se poursuit, leur emploi sera plus offensif et complémentaire avec les actions de cyberdéfense au niveau tactique. Ces évolutions doivent également nous amener à réfléchir autrement au réalisme de notre entraînement, à notre relation à la numérisation, et à notre conception du commandement en opérations.

La guerre électronique dans l'espace aérien

Par le Commandant Romain Lechâble

L'espace aérien, tel que défini par la NASA, est compris entre la surface de la Terre et 100 kilomètres d'altitude. C'est un milieu particulièrement propice à la guerre électronique, car dépourvu de frontière et favorable à la propagation des ondes. Néanmoins, les reliefs peuvent gêner leur propagation dans les basses couches de l'atmosphère, tandis que la puissance d'émission, la sensibilité des capteurs, les conditions de propagation, les contre-mesures ennemies et, à plus longue distance, la rotondité de la Terre peuvent en limiter les actions.

L'allonge particulière de la guerre électronique lorsqu'elle est portée par l'arme aérienne en altitude et en profondeur, se conjugue avec les enjeux de la maîtrise du ciel. Perdre cette bataille dans les airs, c'est alors risquer de perdre celles en surface. Depuis Verdun en 1916, la démonstration est faite que la supériorité opérationnelle en surface ne peut être obtenue que si l'espace aérien est maîtrisé[85].

Mener la guerre électronique dans l'espace aérien nécessite cependant une approche interarmées pour optimiser les effets, ainsi qu'une coordination complexe pour éviter les interférences non désirées. Par ailleurs, le combat aérien impose l'emport d'outils optimisés pour être embarqués (taille, résistance aux contraintes physiques) et pouvant être régulièrement améliorés (avantage opérationnel, contre-adaptation). Il s'agit de garantir la capacité de pénétration de n'importe quelle défense aérienne ennemie, mais aussi la capacité à protéger les espaces aériens nationaux et alliés.

85. La demande du Général Pétain au Commandant de Rose début 1916 pendant la bataille de Verdun le démontre et est considérée comme le moment fondateur de l'aviation de chasse française : « Je suis aveugle Rose, balayez-moi le ciel ! ». Charles de Tricornot de Rose réorganise alors la chasse nationale en escadrilles et élimine l'aviation allemande du ciel de Verdun : parmi ses pilotes se trouvent Jean Navarre, Charles Nungesser et Georges Guynemer. Ce n'est qu'après que les forces au sol du Général Nivelle reprennent progressivement l'avantage sur l'ennemi.

Un rapide aperçu historique

« La guerre est un caméléon qui change de nature à chaque engagement ». Cette formule de Clausewitz n'a jamais été démentie dans le domaine de la guerre électronique. Depuis son apparition au XXe siècle, elle s'est continuellement transformée, au rythme des avancées technologiques et de la ruse des belligérants, démontrant l'avantage très net qu'elle peut offrir à celui qui en fait usage. Quatre étapes historiques marquent l'exploration des options technologiques dans le milieu aérien : l'invention des premières contre-mesures, le contournement des défenses aériennes adverses grâce à l'extension du domaine de vol des appareils, la chasse systématique des défenses aériennes ennemies et enfin la pénétration des défenses grâce à la maîtrise de la détectabilité.

La première étape voit l'apparition des leurres électromagnétiques et des premiers brouilleurs au cours de la Seconde Guerre mondiale. En 1943, les Alliés développent, face aux radars allemands, les programmes *Window* pour les premières paillettes électromagnétiques (*chaff*), et *Carpet* pour les premiers moyens de brouillage. Ils préfigurent l'approche contemporaine de la guerre électronique par les forces aériennes occidentales. Les paillettes sont de fines lamelles d'aluminium aérolarguées, qui amplifient considérablement l'écho radar au point de saturer ce dernier. Le brouillage électromagnétique consiste pour sa part en un émetteur destiné à dégrader les capacités de détection ou de poursuite du radar adverse. En France, ces deux technologies apparaissent dans les années 1960 avec les programmes *Mirage* IV puis *Mirage* F1[86]. Aujourd'hui, le Système de Protection et d'Évitement des Conduites de Tir du Rafale (SPECTRA) assure le brouillage et le leurrage avec un niveau d'efficacité très élevé comme le démontrent régulièrement les performances réalisées lors de campagnes internationales spécialisées telles que l'exercice *Mace* organisé annuellement par l'OTAN[87].

La seconde étape intervient dans les années 1950, lorsque les États-Unis mettent en œuvre l'avion de renseignement U-2, pour survoler l'Union soviétique. Capable d'évoluer à très haute altitude, le U-2 impose à ses pilotes le port d'une combinaison pressurisée[88] ; ce faisant, il défie les capacités de détection, se tient hors d'atteinte des missiles sol-air et des intercepteurs soviétiques. Cette période se clôt lorsque le 1er mai 1960,

86. Comité Historique Guerrelec, *La Guerre électronique sur Mirage IV – 40 années de guerre secrète racontée par ses acteurs*, Limoges, Lavauzelle, 2006.
87. Lors de l'exercice *Mace* XIII en Slovaquie, un Rafale B a pu survoler « sans encombre » un système S-300. B. Etchenic, « Le Rafale, prochain avion de combat canadien ? », *portail-aviation.com*, 21 mars 2014, disponible sur : www.portail-aviation.com/blog.
88. Voir la « limite Amstrong » *in* E. M. Roth, *Rapid Decompression in Pressure-Suited Subjects*, Washington, NASA, novembre 1968.

l'Union soviétique abat un U-2 avec un missile sol-air haute altitude S-75 (SA-2) et développe les systèmes de défense aérienne intégrée multicouches qui prolifèrent aujourd'hui, notamment autour de l'Europe, s'articulant particulièrement autour des célèbres systèmes russes S-300 et S-400.

La troisième étape débute dans les années 1965 avec les premières missions de F-105F *Wild Weasel* II au-dessus du Vietnam, neutralisant les batteries de SA-2 avec les missiles anti-radar *Shrike*, afin d'ouvrir des corridors aux autres chasseurs et bombardiers jusqu'à leurs objectifs. Le concept d'opération de neutralisation des défenses aériennes ennemies (SEAD) passe progressivement de l'attaque des défenses aériennes adverses par les *Wild Weasel* au-dessus du Tonkin, au tir préventif de missiles antiradar (HARM) pendant la guerre du Kosovo. Au cours des 78 jours de l'opération *Allied Force* en 1999, 4 500 sorties SEAD[89] et le tir de 743 HARM[90] ont été nécessaires pour soutenir la campagne aérienne et limiter les pertes de la coalition à deux avions. Aujourd'hui l'US Air Force tend à préférer la combinaison d'appareils à très faible détectabilité (B-2 *Spirit*, F-22 *Raptor*, F-35 *Lightning*) et d'armements polyvalents de moyenne portée (GBU-39 SDB, GBU-53/B), au programme d'armement antiradar *Advanced Anti Radiation Guided Missile* (AARGM), développé avant tout par l'*US Navy*.

Enfin, le quatrième moment correspond à l'introduction du F-117 dans les années 1980, avec l'usage d'une peinture atténuant les réflexions électromagnétiques et l'adoption d'une forme limitant la surface équivalente radar (SER) de l'avion dans quelques « secteurs poubelles » au profit notamment du secteur avant de l'appareil. Cette technologie démontre particulièrement sa pertinence en 1991, pendant la guerre du Golfe où le chasseur-bombardier « furtif » F-117 *Nighthawk* se joue des défenses aériennes irakiennes de fabrication soviétique. Les appareils français *Jaguar*, non furtifs, se trouveront, pour leur part, contraints d'adapter leur profil de vol après que quatre d'entre eux aient été endommagés par des tirs de défenses aériennes subis pendant l'attaque en très basse altitude du terrain d'Al-Jaber. Après vingt ans de carrière, le F-117 est finalement retiré, sa technologie furtive ayant montré ses limites, notamment le 27 mars 1999, quand la défense aérienne serbe parvient à abattre un appareil avec une batterie de S-125 (SA-3).

Ces quatre étapes confirment que le duel du glaive et du bouclier s'applique aussi à la compétition des mesures et des contre-mesures de guerre électronique. L'inventivité, la ruse des opérateurs ainsi que les

89. 4 500 sorties de SEAD, soit environ 30 % des sorties de l'aviation de combat
90. C. Brustlein, E. de Durand, et E. Tenenbaum, *La Suprématie aérienne en péril – Menaces et contre-stratégies à l'horizon 2030*, Paris, La documentation française, 2014, p. 43.

développements technico-opérationnels des équipes militaro-industrielles s'avèrent des facteurs critiques. Lorsqu'un nouveau système de guerre électronique est déployé au combat, il peut offrir un avantage déterminant, mais ce dernier n'est jamais que temporaire. La guerre électronique est donc un domaine majeur de la tactique aérienne, si elle peut contribuer de manière décisive à la victoire, la délaisser revient au contraire à se condamner à la défaite.

Perspectives stratégiques actuelles

En leurrant, en trompant ou en aveuglant l'ennemi, la guerre électronique peut favoriser les victoires tactiques aux conséquences potentiellement stratégiques. Or, la supériorité électromagnétique n'est plus aujourd'hui aussi incontestée qu'elle pouvait l'être entre 1991 et 2010. La pause stratégique qui s'était ouverte après la dissolution de l'URSS s'est close avec le retour des États-puissances qui disposent de capacités de guerre électronique de premier plan. Ainsi, la capacité de localisation de navigation par satellite *Global Navigation Satellite System* (GNSS) sur laquelle s'appuient beaucoup les chasseurs et des armements de l'OTAN, est remise en cause.

La perspective d'un retour à des conflits plus symétriques impliquant nécessairement une contestation du spectre électromagnétique impose aux armées occidentales de redonner la priorité à ce domaine. Force est de constater que la dynamique de recherche et développement (R&D) en la matière, notamment à l'Est, fait courir le risque d'un déclassement rapide de la capacité occidentale à surveiller et maîtriser le spectre électromagnétique d'une part, et à y remporter des batailles d'autre part.

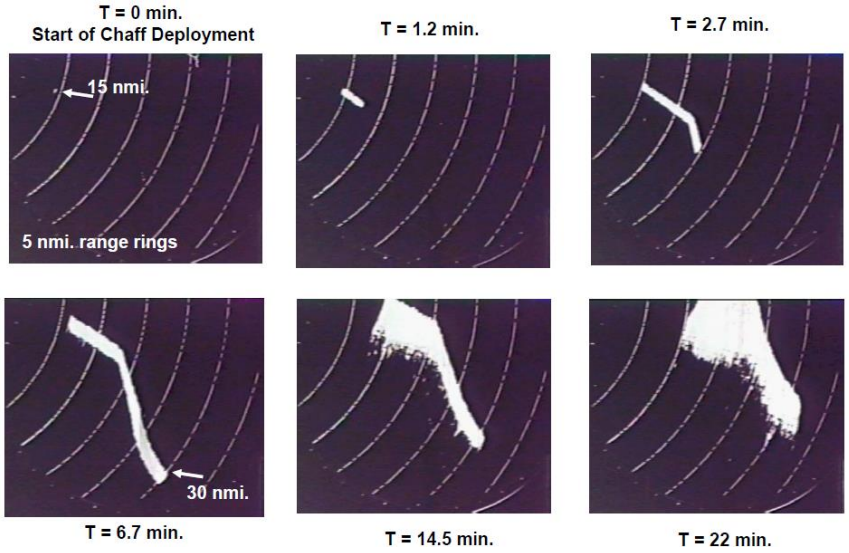
Une surprise tactique d'ampleur dans le domaine électronique est également possible. Le secret industriel qui entoure les performances des équipements de guerre électronique empêche bien souvent d'évaluer avec précision les capacités réelles de nos adversaires potentiels. Or, une remise en cause, même tactique, de la supériorité informationnelle occidentale ne manquerait pas d'avoir des conséquences stratégiques déterminantes sur l'équilibre général des forces. La dynamique actuelle de recherche et développement à l'Est, l'incertitude sur notre avantage opérationnel, et la place stratégique du combat aérien nous obligeront probablement à relancer nos efforts dans ce domaine.

Illustration technique

La capacité d'influence de la guerre électronique sur l'issue d'une bataille aérienne peut être illustrée au travers de deux grands types d'actions respectivement qualifiées de discrète ou d'indiscrète. Les paillettes (ou

chaff), sont un exemple classique de mode d'action « indiscret » comme l'illustre le schéma n° 1.

Schéma n° 1 : Action de guerre électronique indiscrète (plan horizontal d'un radar de veille)



Source : R.M. O'Donnell, « Radar Systems Engineering », Lecture 19, Aerospace and Electronic System Society (AESS), 2012.

L'exemple ci-dessus présente l'effet des *chaff* largués par un avion dans la zone sud-est d'un radar de veille dont le scope est orienté au nord, sur le plan horizontal. Le vent moyen du nord-est est de l'ordre de 55 kilomètres/heure. À la fin des 22 minutes de séquence, le nuage de *chaff* fait une zone blanche inexploitable sur l'écran radar d'environ 15 kilomètres de large sur 35 kilomètres de long. Si l'opérateur radar sait qu'il subit les effets d'une action de guerre électronique, il ne peut savoir ni ce qui se passe dans le secteur couvert par les *chaff*, ni réaliser un tir en aveugle tant la zone de surveillance est étendue. En revanche, s'il est intégré à une défense aérienne plus large, il peut donner l'alerte et favoriser l'efficacité globale du dispositif régional.

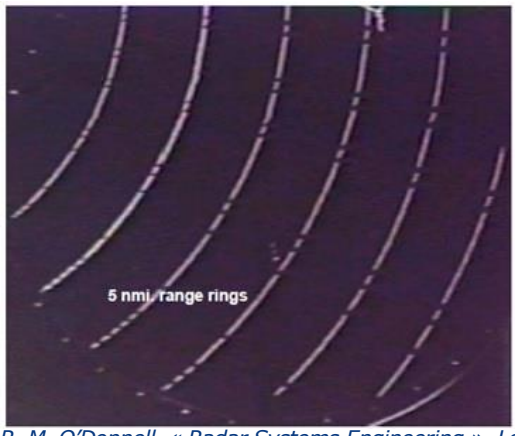
Les *chaff* ne sont plus aussi efficaces sur les radars modernes, notamment parce que ces derniers associent capacité de calcul, formes d'ondes adaptées et intégration dans un système multi-couches. Mais, sur un radar moderne, un brouillage offensif de dernière génération pourrait par exemple avoir un effet tout à fait comparable aux *chaff* sur le radar dont le scope est présenté ci-dessus. En revanche, une contre-mesure « indiscrète », si elle peut favoriser la pénétration d'un espace dénié par une défense aérienne, a pour conséquence d'alerter cette dernière qui peut ainsi focaliser ses efforts pour cibler les vecteurs ennemis dans sa zone d'engagement.

Par ailleurs, lorsqu'un procédé indiscret est employé, l'effort de guerre électronique (nombre de *chaff*, puissance du brouillage, etc.) doit être

d'autant plus important que la surface-équivalent-radar (SER) de l'avion est élevée, puisque le procédé doit être couvrant pour l'avion à protéger. On peut en déduire qu'un brouilleur a une efficacité d'autant plus assurée, que la SER de l'avion à protéger est faible. C'est l'une des forces du *Rafale*, dont la SER a été optimisée, notamment vers l'avant et le haut du chasseur.

Les actions de guerre électronique discrètes fonctionnent différemment. Comme leur nom le laisse supposer, elles ne permettent aucune détection électromagnétique. L'opérateur poursuit sa surveillance du scope, sans chercher à modifier la forme d'onde de sa veille électronique, ni demander le concours des autres radars régionaux.

Schéma n° 2 : Action de guerre électronique discrète (plan horizontal d'un radar de veille)



Source : R. M. O'Donnell, « Radar Systems Engineering », Lecture 19, Aerospace and Electronic System Society (AESS), 2012.

Il existe plusieurs modes tactiques permettant de conduire une action de guerre électronique discrète, et toutes sont réservées à un club capacitaire très exclusif lorsqu'il faut faire face à une défense aérienne de premier rang. À titre d'illustration, la pénétration à très basse altitude sous le seuil des radars de veille est une tactique qui nécessite des technologies de pointe[91] pour favoriser la survivabilité des chasseurs dans un système de défense aérienne intégrée multicouche. Mais le recours à une plateforme « furtive », avec une détectabilité (SER, SOPT[92], émission, etc.) très réduite, ou encore l'emploi de cyberarmes trompant le code informatique du système radar, vise le même objectif : l'opérateur radar ne doit pas pouvoir donner l'alerte aux autres moyens du réseau de défense aérienne et ainsi focaliser les efforts de ciblage. Un mode d'action discret peut donc permettre la pénétration d'un

91. Technologies de pointe nécessaires aujourd'hui à une pénétration en très basse altitude : capacité tout temps y compris sans visibilité, toute condition y compris sous les effets d'un brouilleur radar ou GPS, compatible avec un combat air-air, voire détecteur de départ missile et automatisme d'autoprotection efficace contre la menace de type *Manpads*…

92. SOPT : surface équivalente optronique, englobe les surfaces équivalentes dans toutes les bandes optiques (infra-rouge, visible et ultra-violet).

espace aérien interdit avec une efficacité militaire et une survivabilité renforcées par l'effet de surprise.

Exigences opérationnelles

À l'heure où le combat aérien repose plus que jamais sur la capacité à détecter l'ennemi avec un temps d'avance, il semble évident que les outils de guerre électronique offrent des avantages opérationnels déterminants. Pour être correctement associées au profit d'une stratégie de long terme, les conjugaisons technologiques accessibles doivent être identifiées en groupe de travail multi-compétence, multi-horizon et multi-niveau.

Mythes et promesses techniques

Les stratégies de guerre électronique doivent être régulièrement modernisées et combinées de manière à pouvoir mettre en échec systématiquement les défenses aériennes ennemies au fur et à mesure que celles-ci se modernisent.

L'avènement du combat au-delà de la portée visuelle (*beyond visual range* ou BVR) a consacré, parfois avec excès, le rôle central de la guerre électronique pour l'arme aérienne puisque celle-ci peut empêcher le ciblage de l'adversaire. En effet, un appareil dénué de capacités de détection BVR confronté à un avion qui en est doté est susceptible de perdre son combat avant même de l'avoir débuté.

Les systèmes russes de défense aérienne intégrée posent un problème similaire, en combinant des capacités cinétiques longue portée et du brouillage. Ainsi, le système russe S-300 récemment livré à des pays comme l'Iran, l'Algérie, le Venezuela et la Syrie, cherche à contraindre le ciblage et le tir à distance de sécurité *(stand-off*), en imposant soit une trajectoire risquée sous l'horizon radioélectrique (100 mètres d'altitude), soit un tir à très longue distance au-delà de la portée de ses missiles (soit environ 200 kilomètres pour les missiles 48N6E2). Si l'on ajoute l'usage par les systèmes russes d'un brouillage de signal GPS, l'attaquant est tenu de se doter en sus d'un armement autonome pouvant être tiré soit depuis la très basse altitude, soit depuis la moyenne altitude à distance de sécurité.

La combinaison de ces deux capacités doit contraindre l'adversaire à employer des armements de précision et de très longue portée (missile de croisière) coûteux et en faible dotation dans la plupart des arsenaux. Le risque est d'autant plus élevé que ces vecteurs peuvent également être interceptés par des systèmes de courte portée (typiquement les *Pantsir*/SA-22) placés en protection des dispositifs de haute valeur. La frappe du 6-7 avril

2017 réalisée avec 59 missiles de croisière *Tomahawk* en Syrie[93] a néanmoins rappelé certaines limites de cette approche face aux capacités de frappe saturante et *stand off* occidentales[94].

Les systèmes de défense aérienne intégrée présentent donc des failles face aux tactiques de saturation. Ils sont aussi vulnérables à la guerre électronique moderne. L'association de plusieurs procédés de guerre électronique (évitement, saturation, brouillage offensif, brouillage défensif, leurrage électromagnétique, utilisation de masques, etc.) peut alors s'avérer décisive. Pendant sa vie opérationnelle (1988-2018), le *Mirage* 2000N avait pour mission de pénétrer des environnements très hostiles, en profitant des masques du relief et d'un brouillage électronique performant (système *Caméléon*) pour frapper sa cible. Au cours de l'opération *Force Alliée* au-dessus du Kosovo en 1999, les Américains ont garanti la pénétration en moyenne altitude des avions de la coalition par l'association de brouilleurs offensifs et de systèmes antiradar. Si cette panoplie de moyens et de modes d'action de guerre électronique a suffi à mettre en défaut les systèmes des défenses aériennes ennemies et à garantir l'ascendant opérationnel occidental, il est clair que ces mêmes moyens seraient désormais insuffisants face aux menaces surface-air de dernière génération.

Lorsqu'elle fonctionne efficacement, la guerre électronique peut apporter des solutions pour la pénétration, le ciblage et le tir à des distances réduites d'armements air-sol moins complexes et moins chers que les missiles de croisière. La guerre électronique réduit alors significativement le coût des campagnes longues, où la capacité industrielle de production d'armements est déterminante. Par ailleurs, les capacités de frappe *stand off* offertes par les missiles de croisière ne doivent pas occulter le besoin opérationnel de traiter des cibles mobiles, ou non pré-localisées, dès lors que la plupart des systèmes sol-air de nouvelle génération disposent de châssis motorisés.

Plusieurs pistes de réflexion sont aujourd'hui envisagées pour revaloriser les moyens de guerre électronique face aux capacités d'interdiction longue portée des stratégies de déni d'accès. D'une part, l'extension des capacités de calcul autorisant des algorithmes avancés de prétraitement permettra d'analyser les données massives de capteurs de plus en plus fins. D'autre part, l'association de capteurs-émetteurs plus modernes et de meilleures capacités de calcul pourrait ouvrir le champ à de nouvelles ruses de guerre

93. R. Baheux, « Frappes US en Syrie : le Tomahawk, emblématique missile à 1,5 million de dollars », *Le Parisien*, 7 avril 2017.
94. Pour la France : une frégate multi-missions peut emporter 16 missiles de croisière naval (MdCN) ; huit *Rafale* peuvent emporter 16 missiles SCALP-E6 (système de croisière conventionnel autonome à longue portée).

électronique, tant pour la déception que pour le ciblage. Enfin, les algorithmes permettront la gestion optimisée des équipements de guerre électronique avec la trajectoire des chasseurs et de leurs armes, pour former un système de systèmes intégré.

Préparer la bataille électronique de demain

Face à la complexité croissante des matériels et des techniques de guerre électronique, les prochaines années poseront un défi majeur en termes de ressources humaines. En effet, les opérations de guerre électronique nécessitent des compétences avancées, entretenues par des spécialistes dont les connaissances reposent d'ores et déjà sur des années de travail.

Compte tenu de la sophistication des outils de guerre électronique proposés par les industriels nationaux ou européens d'une part, et le niveau des ruses et techniques déployées par nos adversaires potentiels d'autre part, il paraît indispensable de renforcer les partenariats technico-opérationnels. À moyen terme, un rapprochement entre les industriels et les opérationnels au sein d'équipes intégrées, partageant les données confidentielles, pour optimiser l'emploi des outils déployés et les évolutions techniques serait éminemment souhaitable. Certes, l'ingénieur concepteur des outils de guerre électronique n'est pas compétent pour programmer seul les équipements avant le départ des équipages au combat. Doté d'un niveau d'information adéquat et au contact des praticiens de la guerre électronique, il pourrait toutefois apporter une aide précieuse pour optimiser l'emploi de ces systèmes de plus en plus complexes.

L'humain au cœur du combat électronique

Que ce soit au cours d'une pénétration en très basse altitude ou d'un raid en moyenne altitude, l'emploi de la guerre électronique nécessite une importante préparation technique et cognitive. À l'avenir, il est probable que la préparation technique à la guerre électronique dans l'espace aérien nécessitera une gamme renouvelée de capteurs adaptés, des automatismes de prétraitement des données, des outils régulièrement modernisés et un entraînement contre des systèmes peu ou mal connus.

La connaissance des techniques et des contre-techniques de guerre électronique de l'adversaire nécessite d'acquérir des données précises sur le front, puis de les valoriser. En effet, pour être utiles, les données de guerre électronique doivent provenir d'un capteur très sensible, embarqué par un porteur agile, positionné au plus près de la menace, pour identifier les différents modes de combat et ainsi éviter une protection incomplète.

Une fois recueillies, les données massives de guerre électronique doivent être triées pour en identifier les extraits les plus utiles. Des moyens de stockage et des assistances adaptés seront alors probablement nécessaires pour que les spécialistes traitent des données de plus en plus complexes et nombreuses.

La programmation des automatismes de guerre électronique nécessite donc une compréhension développée des techniques et des contre-techniques de l'adversaire, mais aussi des outils de guerre électronique qui, pour garantir leur niveau opérationnel, doivent être régulièrement modernisés. Enfin, les compétences technico-opérationnelles de très haut niveau ne peuvent être développées en quelques mois par un individu ; elles sont le fruit d'un long travail réunissant un champ large de spécialistes.

L'entraînement des équipages est également une donnée essentielle pour leur permettre de faire face aux défis d'un engagement symétrique, même s'il est parfois difficile d'anticiper les capacités opérationnelles des équipements, dont la diffusion est étroitement contrôlée par la partie adverse. Force est de constater que l'optimisation des effets de guerre électronique en vol impose une coordination réactive des équipages, par exemple pour maintenir l'avion brouilleur sur un même axe que l'avion bombardier, y compris face à une menace mobile sol-air repositionnée. Pour les pilotes, la combinaison de l'analyse des données (certes fusionnées par le système mais très volumineuses dans un engagement de haute intensité), avec la conduite du chasseur et de son système d'armes nécessite un niveau de formation très élevé. La question de l'efficacité des entraînements se pose également face à une nouvelle génération de systèmes adverses encore mal connus – Su-57 PAK-FA, *Novator* KS-172, Chengdu J-20, *Krasukha*, Buk M1-2 (SA-17), S-400 *Triumph* (SA-21), etc.

Surtout, le combat électronique devra être conjugué avec plus de ressources cognitives. La bataille électronique renforce le brouillard de la guerre et complique la réalisation de choix en temps réel sur des fenêtres de décision qui sont de l'ordre de deux à trois secondes en combat aérien. Les conséquences de chacune de ces décisions, comme les vulnérabilités cyber (connectivité, automatisme face à l'imprévu), imposent probablement le maintien de l'humain en première ligne. Mais la tendance constatée[95] de l'augmentation de la durée des missions[96], qui conduit les équipages à engager le combat après plusieurs heures de vol en cabine étroite ainsi que

95. Tendance lourde de l'augmentation progressive de la durée des vols de combat : cette tendance offre aux autorités politiques une capacité d'action à distance précise, polyvalente et réactive, parfois directement depuis la métropole, sans nécessairement devoir engager de troupes physiquement.
96. La frappe SCALP-E6 réalisée contre des installations chimiques en Syrie en avril 2018 a nécessité la réalisation d'une mission aérienne complexe de nuit et longue de près de 10h.

la complexité de la bataille aérienne qui peut être la source d'une saturation intellectuelle, rendront probablement nécessaire le développement d'assistances avancées pour optimiser la ressource cognitive pendant le combat.

Pour faire face à cette complexité accrue, les humains devront à l'avenir être mieux assistés par les machines en préparation de mission, pendant le combat, puis lors de l'analyse des données. Grâce au projet *Man Machine Teaming* (MMT) lancé et financé par la Direction générale de l'armement (DGA), Dassault Aviation et Thalès animent déjà des travaux innovants s'appuyant sur un partenariat large, pour développer le système cognitif de combat aérien de demain[97]. Nul doute que ces études favorisant l'apprentissage rapide, voire instantané des situations rencontrées, l'adaptation en conséquence et le partage des informations pertinentes au sein du futur système de systèmes, apporteront une forte plus-value.

Conclusion

La guerre électronique est un domaine incontournable pour toute armée qui souhaite agir en autonomie stratégique dans des opérations aériennes de haute intensité. Cette tendance lourde est confirmée par la dynamique qui s'observe aujourd'hui tout autour de l'Europe et dans le Pacifique. Cette capacité à mener la guerre électronique dépendra notamment de la bonne prise en compte du besoin opérationnel par la recherche et le développement des industriels. Ce n'est pas tant le déploiement d'un « équipement-rupture » qui garantit l'efficacité d'une suite de guerre électronique, que la cohérence du système de systèmes de combat aérien. En effet, sa feuille de route doit placer en permanence les défenses aériennes des adversaires potentiels face à un paradoxe technique insurmontable le temps d'une campagne.

La création d'une « équipe France » militaro-industrielle, dédiée au niveau tactique de la guerre électronique dans l'espace aérien, pourrait permettre un partage décloisonné des informations opérationnelles et technologiques du plus haut niveau de confidentialité. Cette *task force,* qui devrait avoir un format nécessairement multi-horizon mais aussi suffisamment restreint, aurait tous les moyens pour favoriser les capacités de combat aérien d'aujourd'hui et de demain. À ce titre, elle contribuerait grandement au développement d'une intelligence artificielle dédiée à la guerre électronique.

97. J.-C. Noël, « L'Intelligence artificielle : vers une révolution militaire », *op. cit*. Voir aussi le projet MMT : man-machine-teaming.com.

La France dispose depuis de longues années d'un véritable savoir-faire dans le domaine de la guerre électronique qu'il convient de faire vivre et de préserver. À condition de moyens et d'une priorisation capacitaire, la France peut garantir la crédibilité opérationnelle de son aviation de combat face à n'importe quelle puissance, en donnant toute sa place à la guerre électronique dans une feuille de route pluri-décennale de combinaisons technico-opérationnelles. Cette approche, résolument asymétrique dans son coût par rapport aux programmes d'armement américains, est à la portée de la France, et donc de l'Europe.

L'avènement du combat cyber-électronique

Par le Colonel Stéphane Dossé

Amorcée dès le tournant des années 1970, la numérisation de l'espace de bataille et des opérations est aujourd'hui une réalité. Elle a été hâtée par l'explosion des techniques de télécommunication et de traitement de l'information, qui a touché de plein fouet tant la sphère militaire que l'ensemble de la société civile. La démocratisation de la téléphonie, de l'informatique et le développement de l'Internet civil favorisent une interaction croissante entre les individus. Une personne située au milieu du Sahara peut aujourd'hui aisément appeler en Chine, en passant successivement par des ondes et des réseaux filaires (fibres ou câbles téléphoniques). Le téléphone portable de l'auteur de l'appel peut ainsi se connecter sur une balise via les ondes, puis les données transitent sur un réseau filaire téléphonique, avant d'être relayées par satellite (ondes), puis de transiter sur des câbles internet transcontinentaux et finalement d'être fournis, par son fournisseur Internet, au correspondant. Dans une autre veine, le « *mobile banking* », extrêmement utilisé dans certains pays du Sud, est sur le point de supplanter le troc et les échanges bancaires classiques[98].

Ces changements s'inscrivent dans une convergence des technologies de télécommunication et de stockage de l'information dont l'objet le plus emblématique est le smartphone, qui peut aujourd'hui rassembler plus d'une dizaine de fonctions qui nécessitaient chacune des objets totalement distincts il y a moins de vingt-cinq ans. De cette convergence entre les communications, y compris celles exploitant le spectre électromagnétique, et le traitement de l'information découle un continuum « cyber-électronique » dont l'impact militaire est évident. Les Américains parlent ainsi désormais de *cyberelectronic warfare*[99], là où les Chinois utilisent le

98. A. Demirgüç-Kunt, L. Klapper, *et al.*, *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*, Washington, Banque mondiale, mai 2018. La visite des rues de certaines villes africaines, comme celles de Niamey, en 2017 et 2018, laisse penser que cette tendance est bien un changement de fond.

99. B. Krekel et S. DeWeese, *Capability of the People's Republic of China to conduct Cyber Warfare and Computer Network Exploitation*, McLean, The US-China Economic and Security Review Commission, octobre 2009.

terme de « guerre électronique à réseau intégré[100] ». Dans cette perspective, il faut considérer la guerre électronique et la lutte informatique comme l'ossature d'une action pouvant être appuyée par des capacités plus classiques (maritimes, terrestres, aériennes) ou pour des opérations d'influence. Plus on descend au niveau tactique, plus la guerre électronique prend d'importance, en raison de la mobilité des unités qui combattent. Plus on monte vers le niveau stratégique, plus la lutte informatique devient déterminante.

Le rapprochement de la guerre électronique et du domaine cyber

L'évolution du combat moderne incite à faire une place croissante aux aspects cyber dans les organisations militaires. Déjà prise en compte dans les échelons stratégiques, cette montée en puissance au sein des armées se construit le plus souvent de manière empirique. Aux États-Unis où l'organisation du domaine cyber est déjà bien avancée au niveau stratégique, les différentes armées intègrent de plus en plus le cyberespace dans leurs concepts d'emploi. L'*US Army* a ainsi fait part de son intérêt croissant pour cette problématique dès la publication en janvier 2013 de l'*Army Strategic Planning Guidance* et de l'*Army Capstone Concept*[101]. Dès lors, l'attribution des responsabilités au sein des armées et la construction de structures adaptées aux plus bas niveaux se mettent progressivement en place. Le caractère transverse du cyber – toutes les armées dépendant et exploitant les systèmes d'information – le place difficilement sous la seule responsabilité d'une seule armée ou d'une seule spécialité. La création de commandements unifiés pour la cyberdéfense, comme c'est le cas désormais pour la plupart des puissances militaires majeures, permet de structurer et d'intégrer des forces qui historiquement relèvent des transmissions ou du renseignement.

La guerre électronique, spécialité à la doctrine bien établie, n'échappe pas à la règle. Elle est aujourd'hui massivement transformée par la numérisation croissante des systèmes d'armes (traitement informatique des signaux électroniques notamment). Ceci a conduit, depuis les années 2000, à une coordination étroite et parfois même à une intégration entre le SIGINT et la guerre électronique.

100. D. Sharma, « Integrated Network Electronic Warfare: China's New Concept of Information Warfare », *Journal of Defense Studies*, vol. 4, n° 2, avril 2010 ; *Military and Security Developments Involving the People's Republic of China 2017*, Annual Report to Congress, Washington, Office of the Secretary of Defense, 2017 et rapports précédents depuis 2010 ; S. Dossé, O. Kempf et C. Malis, *Le Cyberespace, nouveau domaine de la pensée stratégique*, *op. cit.* ; A. Bonnemaison, S. Dossé, *Attention : cyber ! Vers le combat cyberélectronique*, *op. cit.*
101. Army Strategic Planning Guidance 2013, février 2013, disponible sur : www.phibetaiota.net.

Il faudra vraisemblablement aller plus loin en intégrant cyber, renseignement technique et guerre électronique dans les mêmes cellules de coordination. La structure classique d'état-major sous forme de branches (personnel, renseignement, opérations, etc.) doit donc être complétée de structures de coordination transverses pour le cyberespace qui peuvent s'apparenter à ce qui est mis en place pour la guerre électronique et le renseignement d'origine électromagnétique dans l'OTAN. Afin d'assurer la coordination, les centres d'opérations de renseignement d'origine électromagnétique (ROEM) et de guerre électronique pourraient être facilement transformés en centre d'opération de combat cyber-électronique. Un centre des opérations de type *cyberelectronic operation center* pourrait assumer cette tâche de coordination, en étendant les compétences des SEWOC (*SIGINT electronic warfare operation center*)[102].

Une convergence opérationnelle

En 2014 et en 2015, des forces pro-russes ont été soupçonnées d'avoir mené avec un appui extérieur des actions combinées cyber et guerre électronique, lors du conflit dans l'est de l'Ukraine. Lors de la réunion extraordinaire OTAN-Ukraine du 26 janvier 2015, le Secrétaire général de l'OTAN avait déclaré que la Russie appuyait les séparatistes avec des moyens de guerre électronique. Quelques jours plus tard, le général Hodges, commandant des forces terrestres américaines en Europe, reconnaissait que les forces ukrainiennes souffraient des moyens offensifs de guerre électronique dont leurs adversaires disposaient, c'est-à-dire une capacité exceptionnelle et importante de brouillage. Le même jour, le Premier ministre ukrainien Arseni Iatseniouk, lors d'une visite à l'Institut militaire ukrainien des télécommunications et de l'informatique, sous-entendait la même chose, tout en évoquant les attaques cyber dont la défense du pays faisait l'objet. Cet exemple récent et public incite à se poser la question de la convergence entre la lutte informatique et la guerre électronique. À cet égard, il semble opportun d'étudier l'articulation de ces capacités, sous la forme du triptyque opérationnel classique « surveillance, attaque et défense ».

La surveillance tout d'abord vise à extraire du renseignement des réseaux numériques, de leurs composants et des ondes électromagnétiques qui les véhiculent. Elle contribue ainsi au renseignement de documentation

102. Les manuels de l'*US Army* FM 3-38 *Cyber electromagnetic activities* (février 2014) et FM 3-12 *Cyberspace and electronic warfare operations* (avril 2017), suggèrent ainsi la mise en œuvre d'un Cyber ElectroMagnetic Activities (*CEMA*) *Working Group* pour les niveaux tactiques bas. Cette organisation peut être complétée par des groupes de travail transverses de type cyber SIGINT *electronic warfare working group* (CSEW-WG).

et d'anticipation, apporte une meilleure appréciation de situation, et fournit des informations à des fins d'alerte et d'action pour les troupes qui manœuvrent. Il convient ici de distinguer le renseignement d'origine cyber (c'est-à-dire extrait des réseaux, des objets connectés et des systèmes d'armes) du renseignement d'intérêt cyber permettant de planifier, de conduire et d'évaluer des opérations cyber. Dans tous les cas, la surveillance se déclinera, dans un premier temps au moins, essentiellement au niveau stratégique. Il est néanmoins très prévisible qu'elle s'étende ensuite au niveau tactico-opératif. Elle devra alors pouvoir s'appuyer sur des capacités variées et très évolutives.

L'attaque nécessite d'investir un vaste champ des possibles pour agresser l'adversaire : dégradation et neutralisation des architectures de commandement et de renseignement, attaque virale, destruction par rayonnement des composants, intrusion, substitution et leurrage des systèmes d'information et de commandement, brouillage des moyens de navigation, attaques informatiques ciblées… Dans ce domaine plus qu'ailleurs, nul doute que l'innovation technologique et l'imagination opérationnelle des acteurs offriront des opportunités d'agression dont l'efficacité ne sera pas nécessairement liée à la puissance traditionnelle et officielle des armées. La virulence de l'attaque dépendra davantage d'une réelle prise de conscience de l'existence d'un nouvel espace de combat et d'une agressivité exacerbée. Les attaques les plus avancées combinent ainsi les attaques électroniques, informatiques et informationnelles comme le montrent certaines analyses de la campagne de Crimée en Ukraine au printemps 2014[103].

La défense aspire enfin à protéger les armées de la menace cyber-électronique sous tous ses aspects. Elle a pour finalité d'empêcher tout adversaire d'extraire des informations des systèmes utilisés pour les armées et elle vise à les prémunir au mieux contre des attaques virales et des opérations de déni de service. Elle s'assure de la fiabilité des composants et des logiciels utilisés dans les systèmes d'armes. Elle repose donc autant sur la sensibilisation des divers utilisateurs de systèmes d'armes et exploitants des systèmes d'information (volet SSI, formation, entraînement), que sur le durcissement, la protection des moyens, la résilience des architectures de commandement et même sur la vérification des systèmes et leur redondance pour ne pas permettre de rupture de « service » (par des plans de continuité du service). Par extension, elle pourrait couvrir aussi tous les systèmes d'autoprotection tels que le brouillage anti engins explosifs improvisés, les moyens de leurrage déjà intégrés tant sur les véhicules tactiques terrestres

103. M. Connell et S. Vogler, *Russia's Approach to Cyber Warfare*, Arlington County, CNA, mars 2017 ; R. N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic*, *op. cit.*

que sur les bâtiments de la Marine et les aéronefs. La lutte contre les opérations militaires d'influence fait partie intégrante de la défense au regard de la médiatisation de leurs méfaits par certains attaquants. Il s'agit alors de développer une véritable sécurité cognitive qui intègre les réseaux mais aussi les objets civils ou militaires qu'ils raccordent[104].

Ce triptyque forme finalement un tout : les volets surveillance, défense et attaque interagissent en permanence. L'efficacité dans la durée dépend de leur combinaison et du respect des règles fondamentales du combat. La tactique s'appuie toujours sur des invariants tels que la prise et la conservation de l'initiative, la recherche de l'effet de surprise, la prédilection pour la manœuvre (en combinant les mouvements avec des feux et des effets immatériels) et l'optimisation dans l'emploi des armes. Celui qui veut prendre l'ascendant, cherchera encore à perturber l'unicité et la permanence du commandement ennemi. Il s'efforcera de couper ses liaisons avec ses alliés ou ses renforts. Il désorganisera les forces adverses dans toutes leurs dimensions et trompera leurs moyens de renseignement et de surveillance. À ce titre, il est frappant de constater que le combat cyber-électronique ne s'affranchit pas des grands principes de la guerre énoncés par Foch que sont la liberté d'action, la concentration des efforts et l'économie des moyens.

Le combat cyber-électronique et les principes de la guerre

La **liberté d'action** favorise la surprise et la discrétion, qui sont fondamentales pour l'ensemble des actions attenant au combat cyber-électronique. Le défenseur cherche à avoir en permanence accès à l'ensemble de son système. L'assaillant cible souvent le maillon faible, grâce à des actions de renseignement, si possible très discrètes.

Le manuel de tactique générale des forces terrestres françaises[105] considère ainsi que la surprise peut revêtir plusieurs formes successives de manœuvres coordonnées, qui concourent à l'acquisition et au maintien de la liberté d'action : innovation technique, constitution de réserves d'intervention, utilisation de nouvelles organisations ou de procédés tactiques modifiés par rapport à l'habitude. La guerre électronique permet alors de renforcer cette liberté d'action, en détectant l'ennemi potentiel et en contribuant à la suppression ou à la neutralisation tactique des menaces.

104. Y. Challal, « Sécurité de l'Internet des Objets : vers une approche cognitive et systémique », *Réseaux et télécommunications*, Université de Technologie de Compiègne, 2012.
105. FT-02, *Tactique Générale*, Paris, CDEF, Armée de Terre, 2009.

Le principe de **concentration des efforts** permet de maximiser les effets dans le cadre de la manœuvre cyber-électronique. En effet il ne faut jamais oublier, aussi bien en planification qu'en conduite, que les capacités cyber sont liées à des unités militaires ou paramilitaires qui les mettent en œuvre. Même si la notion de distance est plus complexe que dans les autres espaces, il s'agit bien de manœuvrer des unités avec des capacités, et non d'appliquer des techniques. Il faut penser en termes d'« action des unités » plus que « déploiement de systèmes techniques ».

La manœuvre cyber-électronique est autonome lorsqu'elle combine des capacités cyber, de guerre électronique ou d'influence numérique pour réaliser des effets sur l'ennemi dans le cyberespace. Cette manœuvre est intégrée lorsque la guerre cyber-électronique appuie (ou est appuyée par) au moins une autre composante tactique (terre, air, mer, espace) sur le mode de la manœuvre interarmes ou interarmées. Cela se traduit par des ordres ou des plans cyber dans le cadre d'une manœuvre autonome ou par des annexes cyber à des plans et ordres de niveau opératif ou de composantes tactiques en vue d'une manœuvre intégrée.

Si le cyber contribue à l'approche directe de la manœuvre (priorité à la destruction de l'ennemi par attrition progressive), sa contribution est maximale dans le cadre de l'approche indirecte (qui privilégie une manœuvre globale pour briser la cohésion adverse). Les cibles dans le cyberespace, compte tenu de la résilience de la plupart des réseaux, doivent prioritairement être traitées dans une approche systémique. Une telle approche appliquée à nos propres réseaux doit permettre d'améliorer notre protection et l'organisation de notre défense. Elle favorise ainsi l'**économie des moyens,** qui est fondamentale pour les organisations militaires dont les besoins en unités de cyberdéfense ne sont pas encore totalement couverts par la ressource réelle[106]. Cela permet de faire effort sur les zones clés du cyberespace (*cyberspace key terrain*) de la zone d'action considérée. Dans le cyberespace, la convergence des effets doit être préférée à la convergence des moyens, en raison du caractère immatériel du domaine. La notion de rapport de force n'y est pas aussi intuitive que dans les champs matériels, mais elle existe. Il s'agit de mettre en regard la capacité à mettre en œuvre des réseaux opérationnels, et la capacité de perturbation ou de destruction de ces réseaux par l'adversaire. Cela permet de déterminer, pour cette action, les moments cruciaux pour chaque zone clé du cyberespace.

106 Loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.

Conclusion

L'enjeu actuel n'est donc pas de développer de nouvelles tactiques de guerre sur les réseaux, mais de suivre l'évolution des technologies de l'information et la démocratisation de l'usage des télécommunications, qui ont profondément transformé l'emploi de la force armée au cours des cinquante dernières années. En 1992, le général Marc Monchal, alors chef d'état-major de l'armée de terre, déclarait qu'à l'avenir, le maître de l'électron l'emporterait sur le maître du feu. En attendant l'éventuelle réalisation de cette prophétie, le maître du feu devra aussi s'assurer d'être le maître des données.

Institut français
des relations
internationales