Mémoire de recherche
2024-2025

LA GUERRE ÉLECTRONIQUE À L'ÈRE DU CYBER : EFFACÉE DES RADARS, MAIS TOUJOURS EN ONDE ?

Étude de l'articulation de deux armes invisibles dans la guerre moderne

Eva Le Gargasson
Majeure Stratégie, Intelligence économique et Gestion des Risques

Sous la direction de Audrey Hérisson

DÉCLARATION

Sciences po Lille n'entend donner aucune approbation ni improbation aux thèses et opinions émises dans ce mémoire de recherche. Celles-ci doivent être considérées comme propres à leur auteur.

J'atteste que ce mémoire de recherche est le résultat de mon travail personnel, qu'il cite et référence toutes les sources utilisées et qu'il ne contient pas de passage ayant déjà été utilisé intégralement dans un travail similaire.

RÉSUMÉ

Longtemps pilier discret des opérations militaires, la guerre électronique (GE) a vu émerger, au tournant du XXI^{e} siècle, le cyberespace. Tandis que ce dernier a rapidement capté l'attention des sphères médiatiques, politiques et académiques, la GE semble avoir été reléguée au second plan, à la fois dans les discours dominants et dans la littérature. Si les cas d'étude récents confirment la persistance de la GE en tant que moyen à part entière dans la guerre, la question de son articulation avec le domaine cyber demeure largement négligée. Ce mémoire de recherche entend retracer l'évolution de la GE face à l'essor du cyber, afin d'identifier la nature de leur relation : complémentarité, indépendance, substitution ? L'approche globale empruntée – historique, technique, stratégique, empirique – se propose de réactualiser les réflexions sur cette articulation cyber-électronique. L'analyse des trajectoires de ces deux objets ainsi que l'étude de cas emblématiques, notamment liés à la Russie, apporteront de la clarté à cette démonstration.

Mots-clés : guerre électronique, cyberespace, convergence, conflictualité, stratégie, transformation militaire, cas russe.

Long a discreet pillar of military operations, electronic warfare (EW) has, at the turn of the 21st century, faced the rise of cyberspace. While the latter has rapidly drawn the attention of media, political, and academic spheres, EW appears to have faded into the background, both in strategic discourse and in scholarly literature. Although recent cases confirm the continued strategic relevance of EW, its relationship with cyber remains insufficiently explored. This research seeks to trace the evolution of EW in light of cyberspace's growing prominence, and to clarify the nature of their interaction: complementarity, independence, or substitution? By adopting a comprehensive approach—historical, technical, strategic, and empirical—this study aims to renew the analytical framework surrounding this cyber-electromagnetic articulation. The analysis of both trajectories, combined with emblematic case studies, notably those involving Russia, sheds light on the complexity and strategic significance of their convergence.

Keywords: electronic warfare, cyberspace, convergence, conflictuality, strategy, military transformation, Russian case.

REMERCIEMENTS

Je tiens tout d'abord à remercier ma directrice de mémoire, Audrey Hérisson, pour avoir accepté de m'accompagner dans cette aventure. Sa disponibilité constante, ses conseils et sa bienveillance ont été une source de confiance et de sérénité tout au long de ce travail.

Je remercie aussi chaleureusement Lennig Pedron et Matthias Popoff, pour m'avoir transmis le virus du cyber avec passion.

Je suis particulièrement reconnaissante envers toutes les personnes avec qui j'ai pu échanger sur le sujet, et plus particulièrement, Éric Gomez, Serge Cholley, Pierre Baratault, Yannick Genty-Boudry et Jean-François Grandin, qui m'ont accordé des entretiens passionnants. Leur temps et leur expertise ont été précieux dans l'avancée de mes réflexions.

Merci infiniment à mes amies – Elisa, Julie, Marie-Ange, Manon – qui croient en moi comme ce n'est pas permis, et qui m'inspirent à me dépasser chaque jour. Merci aussi à Pauline, Sasha et Océane, d'avoir été là tout au long de l'année et d'avoir su créer une merveilleuse bulle de soutien réciproque et d'amitié.

Enfin, ma plus grande gratitude s'adresse à mes parents, Youna, Aël, mes grands-parents, et tous mes proches, sans qui je n'aurais jamais pu atteindre les ambitieux objectifs de ces dernières années. Merci pour votre soutien indéfectible, votre amour, et pour la légèreté que vous m'apportez quand tout me semble lourd. Et merci à toi, Pierre, pour la tranquillité du quotidien, pour ta patience inépuisable, et ta joie de vivre inconditionnelle.

LISTE DES ACRONYMES

C2 : Commandement et contrôle

CCDCOE : Centre d'Excellence de cyberdéfense coopérative de l'OTAN

CNC : Centre national de ciblage (France)

ComCyber : Commandement de la cyberdéfense (France)

COMINT : Communication intelligence – analyse du contenu des renseignements issus du ROEM

Communications GSM : *Global System for Mobile Communciations* (prédécesseur des réseaux 3G)

CPCO : Centre de Planification et de Conduite des Opérations (France)

DARPA : *Defense Advanced Research Projects Agency* (agence du département de la Défense des États-Unis)

DCA : Défense contre l'aviation ou lutte antiaérienne défensive (France)

DRM : Direction du renseignement militaire (France)

DST : Direction de la surveillance du territoire (actuelle DGSI, France)

ELINT : *Electronic intelligence* – renseignement technique d'origine électromagnétique

FSB : Service fédéral de sécurité de la fédération de Russie

FSO : Service fédéral de protection / Service de la garde fédérale (Russie)

GCHQ : *Government Communications Headquarters* (Royaume-Unie)

GE : Guerre électronique

GQG : Grand Quartier Général (France, Première Guerre mondiale)

GRU : Direction générale des renseignements de l'État-Major des Forces armées de la fédération de Russie

KGB : Comité pour la sécurité de l'État (Russie)

NSA : *National security agency* (États-Unis)

OSINT : Renseignement d'origine sources ouvertes

R&D : Recherche et développement

RAM : Révolutions dans les Affaires Militaires

ROEM : Renseignement d'origine électromagnétique

SDECE : Service de documentation extérieure et de contre-espionnage (actuelle DGSE, France)

SIGINT : *Signal intelligence* – ROEM en français

STR : Service technique de recherche (un des services de la DGSE, France)

TSF : Télégraphie sans fil

VDV : Troupes aéroportées de la fédération de Russie

VSAT : *Very Small Aperture Terminal*

SOMMAIRE

Introduction

Le 24 février 2022, le premier coup de feu du conflit russo-ukrainien est lancé : il est cyberélectronique. La cyberattaque sur le réseau Ka-Sat[1] avait en effet mis hors service environ 30 000 modems[2], qui permettaient de recevoir la connexion du satellite Ka-Sat. Tandis que la Russie prenait de l'avance, l'attaque avait déstabilisé la coordination de l'armée ukrainienne, établie par des moyens électroniques[3]. En d'autres termes, une cyberattaque – lancée initialement sur le réseau informatique utilisé par le satellite Ka-Sat – a affecté un modem employé par l'armée ukrainienne, et a de fait perturbé les télécommunications qui permettaient d'organiser et de coordonner les troupes au sol. Le caractère inédit de cette offensive réside dans la combinaison de cette cyberattaque avec des actions de brouillage électronique, qui visaient les communications radio, et l'engagement militaire conventionnel, mené simultanément sur le terrain. L'utilisation coordonnée de moyens distincts ne semble pourtant pas être, de prime abord, une situation novatrice dans la guerre. En effet, par définition, la guerre a recours à tous les moyens possibles pour provoquer la déstabilisation de son adversaire[4]. Les opérations de déception ne sont pas nouvelles et combinent des actions coordonnées dans le but de tromper le « système » de commandement et de décision de l'ennemi[5]. Ce principe de synergie entre les moyens n'est pas non plus nouveau dans les réflexions stratégiques : il est érigé en fondement dans les doctrines « multi-milieux multi-champs[6] » (M2MC), aussi connue comme « Joint All-Domain Command and Control[7] » (JADC2) aux États-Unis. Ces approches visent à penser la guerre dans la continuité des milieux et des champs, et prônent l'intégration de toutes les capacités pour atteindre un effet stratégique unifié. Dans ce cadre, une opération combinant GE et cyberespace ne saurait, en soi, constituer une rupture.

[1] Voir les détails de l'attaque sur la plateforme Cyber Law Toolkit du CCDCOE : "Viasat KA-SAT Attack". https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022)
[2] Martin Matishak, "Western powers blame Russia for Ukraine satellite hack", *The Record*, 10 mai 2022 (https://therecord.media/eu-uk-blame-russia-for-ukraine-satellite-hack).
[3] Anne Maurin, « La guerre en Ukraine et le théâtre spatial », *Les Cahiers de la Revue Défense Nationale*, n° 97, 2023, p. 35.
[4] Carl von Clausewitz, "Chapter II. End and Means in War", in *On War*, 1832.
[5] Rémy Hémez et Anthony Namor « L'apport des actions cyberélectroniques aux opérations de déception tactiques et opératives », *Stratégique*, vol. 128, n° 1, 2022, p. 200.
[6] Philippe Gros, Vincent Tourret, Nicolas Mazzucchi, Thibault Fouillet et Paul Wohrer « Intégration multimilieux / multichamps : enjeux, opportunités et risques à horizon 2035 », *Fondation pour la recherche stratégique*, Rapport n°35/FRS/M2MC, 2022, p. 108-110.
[7] Department of Defense, *Summary of the Joint All-Domain Command & Control* (JADC2), Strategy, p. 3-5.

Et pourtant, l'analyse de leur interaction laisse entrevoir plus qu'une simple juxtaposition d'effets. Le cas cyber-électronique se distingue par l'ambiguïté intrinsèque qui persiste entre le spectre électromagnétique et le domaine cyber[8]. Ces deux moyens paraissent davantage reliés dans leurs utilisations au sein des conflits. Contrairement à d'autres formes de synergies interarmées ou interdomaines[9], la convergence entre guerre électronique (GE) et cyberespace s'opère à travers des médiums, des effets et des temporalités parfois similaires, au point de rendre leur séparation analytique délicate. Tous deux exploitent des couches techniques imbriquées, notamment les ondes électromagnétiques, les infrastructures de communication et les réseaux numériques[10]. La frontière entre les effets induits par les opérations cyber et ceux des actions électromagnétiques peut ainsi se brouiller, tant dans leur mode d'action que dans leurs résultats opérationnels. Ce constat, bien qu'évident pour certains praticiens, reste toutefois peu exploré dans les cadres théoriques traditionnels, qui tendent à cloisonner les deux domaines : l'analyse du spectre électromagnétique d'une part, souvent réalisée par les domaines militaires et industriels, et l'étude du cyber d'autre part, dont les écrits sont plus récents, plus nombreux et multi-sectoriels. Le phénomène inverse se produit dans la sphère médiatique et journalistique. Cette dernière décennie, les analyses de conflits grand public mentionnent uniquement la question cyber, l'utilisation du monde de l'informatique et ses conséquences dans les guerres, sans aborder le concept de GE. Il est difficile de dire s'il s'agit là d'une confusion sémantique involontaire, qui induirait une méconnaissance de la distinction et de l'articulation GE-cyber, ou d'une conséquence de la vulgarisation journalistique qui appelle à l'omission des aspects techniques de cette relation GE-cyber pour rendre le sujet plus simple. En 2014, l'ouvrage *Attention : Cyber !* marquait un nouveau point de départ dans la manière de comprendre la GE et le cyberespace. L'objectif était clair : analyser l'articulation de ces deux moyens.

> *L'utilisation des ondes électromagnétiques a en effet révolutionné l'art de la guerre au XX^e^ siècle bien autant que le char ou l'avion, au moins dans sa première moitié. Le numérique révolutionnera celui du XXI^e^ siècle dans la continuité du siècle précédent. La révolution numérique poursuit et amplifie la révolution analogique dans l'histoire de l'humanité*[11].

[8] Jacob Cox et al., "The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence", *The Cyber Defense Review*, vol. 4, n° 2, 2019, p. 81-83.
[9] Par exemple l'articulation entre manœuvre terrestre et appui aérien.
[10] Olivier Kempf, « Du cyber et de la guerre », *Fondation pour la Recherche Stratégique*, note n°17/19, 2019, p. 5-7.
[11] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, Paris : Economica, 2014, p. 9.

Pourtant, cette idée de prolongement se heurte à un constat paradoxal : dans les représentations générales, notamment médiatiques, l'attention se centre largement sur le cyber[12], tandis que la GE en est quasiment éclipsée. Cette rupture dans les représentations interroge. D'un point de vue chronologique, il est tentant de penser que la GE, prédominante dans les conflits du XX^{e} siècle[13], aurait pu être progressivement remplacée par le cyber et son émergence fulgurante au début du XXI^{e} siècle[14]. Pourtant, cette hypothèse ne semble pas refléter les réalités opérationnelles, puisque la GE continue d'être massivement mobilisée dans les conflits actuels, et fait l'objet de développements capacitaires soutenus[15]. Ce décalage entre vitalité opérationnelle et faible traitement du concept conduit à interroger la manière dont l'émergence du cyber a pu modifier la perception, la compréhension ou la position de la GE dans les dynamiques contemporaines de conflictualité. Avant d'explorer cette articulation, il convient d'analyser comment ces deux domaines sont aujourd'hui pensés, représentés et parfois dissociés dans la littérature scientifique.

État de la littérature

Définir la guerre électronique

Dans les travaux scientifiques, la GE désigne l'ensemble des opérations militaires, menées dans tous les milieux, qui exploitent le spectre électromagnétique pour créer des effets à l'appui d'objectifs militaires, et dans le but de combattre un adversaire ou de s'en protéger[16]. Elle a été développée et est utilisée depuis la fin du XIX^{e} siècle : télégraphe optique, électrique, aérien, maîtrise de câbles, puis liaisons radios, technologie radar, communications satellitaires ou mobile, etc. Elle fut la première forme de combat immatériel et technique moderne[17].

---

[12] Frédérick Douzet, « Chapitre 21. Le cyberespace, un champ d'affrontement géopolitique », in Béatrice Giblin, *Les conflits dans le monde* : *Approche géopolitique*, Paris : Armand Colin, 2016, p. 327-343.
[13] Francis Queylar, « La guerre électronique, une réalité majeure (I) », *Revue Défense Nationale*, n° 340, p. 41-55.
[14] Gema Sanchez Medero, « Cyber-crime, cyber-terrorisme et cyber-guerre : les nouveaux défis du XXI^{e} siècle », *Revista Cenipec*, n° 31, 2012.
[15] Olivier Dujardin, « La guerre électronique dans les conflits aujourd'hui », *Institut d'Études de Géopolitique Appliquée*, 2021.
[16] I. R. Mirman, "Electronic Warfare", Ordnance, *National Defense Industrial Association*, vol. 53, n° 291, 1968, p. 297–301.
[17] Samir Ouali-Djerbi, « Guerre électronique et combat dans le cyber espace : quelle complémentarité ? », in *Réflexions sur le cyber : quels enjeux ?*. Paris : Centre d'études stratégiques aérospatiales, IRSEM, n° 32, 2015, p. 83.

Les objectifs et effets de la GE couvrent trois principaux domaines[18]. Tout d'abord, le soutien électronique – ou renseignement d'origine électromagnétique (ROEM) – correspond à la phase de détection des activités électromagnétiques, et donc à une activité de renseignement dans le champ électromagnétique. Ce premier domaine porte essentiellement sur l'activité des radars. Ensuite, l'attaque électronique – ou contre-mesures – permet de contrer les menaces du domaine électromagnétique, comme les radars ou autodirecteurs de missiles, à partir de brouilleurs et de leurrage. Cette phase peut servir de prévention des menaces électromagnétiques, ou permettre de passer à l'offensive. Enfin, la protection des activités électroniques – ou contre-contre-mesures – correspond à l'activité des radaristes ou concepteurs de plateforme pour préserver leurs propres installations et radars vis-à-vis de potentielles attaques, notamment des brouilleurs. Ces trois domaines sont très liés et le triptyque fait consensus chez les experts[19].

Le spectre électromagnétique par lequel sont perpétrées ces actions de GE est lui défini comme étant l'ensemble des types d'ondes électromagnétiques, classés selon des critères tels que la longueur d'onde, la fréquence ou la quantité d'énergie qu'elles transportent[20]. Après la découverte de l'infrarouge et de l'ultraviolet il y a deux cents ans, Maxwell proposa sa théorie des ondes électromagnétiques, aboutie par Hertz dont on se rappelle aujourd'hui la notion des ondes hertziennes[21]. Comme pour toute nouvelle découverte scientifique, l'avenir des ondes consistait à devenir exploitable pour répondre aux besoins de la civilisation moderne. De fait, « la naissance de la GE correspond aux débuts de l'utilisation des ondes électromagnétiques[22]. » Par ailleurs, « pour toutes les gammes d'ondes électromagnétiques, le processus qui conduit de la découverte à l'exploitation est toujours le même », à savoir : « découverte scientifique, développement technologique, puis application pratique, souvent initiée dans un cadre militaire[23]. »

---

[18] P. M. Grant and J. H. Collins, "Introduction to electronic warfare", *The Institution of Engineering and Technology Proceedings*, vol. 129, n° 3, 1982.
[19] Doug Richardson, *Electronic warfare. A revealing insight into one of the most closely guarded areas of military activity: the clandestine world where threat and countermeasure battle constantly for supremacy*, Londres : Salamander Books Limited, 1985, p. 16-83.
[20] Éric Gomez, « Focus 2. La guerre électronique », in Céline Marangé et Maud Quessard, *Les guerres de l'information à l'ère numérique*, Paris : Presses Universitaires de France, 2021, p.79.
[21] J. R. James, "Magical microwaves: the exploitation of the century", *The Institution of Engineering and Technology Proceedings*, vol. 136, n° 1, 1989.
[22] Jean-Paul Siffre, « La conquête du spectre des fréquences électromagnétiques et son utilisation en guerre électronique », in *La Guerre électronique en France au XX*e *siècle*, Paris : Centre d'études d'histoire de la Défense, 2002. Actes du colloque organisé le 20 avril 2000 à l'École militaire, p. 10.
[23] Jean-Paul Siffre, *ibid*., p. 11.

En 2001, le général Jean-Paul Siffre répertorie les dates d'utilisation des ondes électromagnétiques dans un but militaire. Ce tableau[24] permet de retracer l'évolution de l'exploitation militaire du spectre électromagnétique entre 1900 et 2010. Dans ses analyses, le Général associe chaque période à un nouvel usage stratégique du spectre.

Date	Le spectre des fréquences (ou des ondes) électromagnétiques									
	hm	m	cm	mm	IR2	IR1	visible	UV	X	γ
1900	OUI						OUI			
1910	OUI						OUI			
1920	OUI	OUI					OUI			
1930	OUI	OUI					OUI			
1940	OUI	OUI	OUI			OUI	OUI			
1950	OUI	OUI	OUI			OUI	OUI			
1960	OUI	OUI	OUI		OUI	OUI	OUI			
1970	OUI	OUI	OUI	OUI	OUI	OUI	OUI			
1980	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI		
1990	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI		
2000	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	?	
2010	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI	?	?

Source : Jean-Paul Siffre, « La conquête du spectre des fréquences électromagnétiques et son utilisation en guerre électronique », in *La Guerre électronique en France au XX^e siècle*, Paris : Centre d'études d'histoire de la Défense, 2002. Actes du colloque organisé le 20 avril 2000 à l'École militaire, p. 11.

Au début du XX^e siècle, seules les ondes longues, comme les ondes hectométriques et métriques, sont utilisées. Elles permettent de communiquer, principalement via la radiotélégraphie. Dès 1910, elles servent aussi à localiser des positions, ce qui marque les débuts de l'utilisation militaire du repérage radio. Dans les années 1920, l'usage s'élargit à la navigation, avec le développement de systèmes guidant les navires ou avions, puis en 1930, les progrès techniques permettent de détecter des objets à distance, et ouvrent ainsi la voie au radar. À partir des années 1940, de nouvelles bandes, notamment les ondes centimétriques et millimétriques, sont exploitées, et permettent alors d'identifier des cibles, grâce à des dispositifs plus précis capables de différencier les objets ou les ennemis. Ce phénomène s'accélère dans les années 1960 et 1970 avec l'apparition des premières applications militaires des ondes infrarouges (IR1 et IR2), rendues possibles par les avancées dans les capteurs thermiques, les radars de précision et les systèmes de guidage. Par ailleurs, plus les fréquences sont hautes, et plus les applications se complexifient : vision nocturne, radars Doppler, voire armes à énergie dirigée[25]. Cette évolution témoigne de la montée en

[24] Jean-Paul Siffre, ibid., p. 11.
[25] Jean-Paul Siffre, ibid., p. 11-13.

complexité et en précision des fonctions militaires liées aux ondes, parallèlement aux avancées technologiques[26]. Concernant les dégâts que la GE peut infliger, le général Jean-Paul Siffre relève trois étapes majeures. Dès son apparition autour de 1900, la GE permet une destruction dite « indirecte » des cibles : les écoutes d'émissions ennemies offrent la possibilité de guider des frappes contre des cibles précises, en optimisant le choix du moment et de l'objectif. Dans les années 1980, la destruction obtenue peut être « douce », en ciblant principalement les capteurs et les dispositifs de détection. Enfin, depuis les années 1990, la GE peut provoquer des destructions « dures », en visant directement la neutralisation physique de l'objectif, soit, des systèmes ou des infrastructures adverses. Depuis la découverte des ondes, chaque portion du spectre électromagnétique, une fois maîtrisée technologiquement, a rapidement été intégrée à des dispositifs militaires. Aujourd'hui, la maîtrise de l'énergie électromagnétique est fondamentale pour les armées. Dans la doctrine interarmées 3-6 française de 2017, il est écrit que :

> *L'essentiel de nos capacités dans les domaines de la surveillance, de l'acquisition d'objectifs, du renseignement et de la reconnaissance (SA2R) dépend de l'énergie électromagnétique. Il en est, de même, pour la capacité à délivrer des effets, à naviguer, à communiquer, à opérer, à commander, etc.*[27]

Définir le domaine cyber

Initialement dérivé de la cybernétique[28], puis associé au développement de l'informatique et des réseaux à partir des années 1970, le « cyber » désigne aujourd'hui bien plus qu'un simple domaine technologique. La définition du cyberespace ne fait pas consensus[29]. Celui-ci fait l'objet d'une grande diversité de représentations. En 2017, le Centre d'Excellence de cyberdéfense coopérative de l'OTAN (CCDCOE) a recensé une trentaine de définitions[30] qui regroupent les aspects conceptuel, technique, tactique, juridique. Certaines de ces définitions recoupent des caractéristiques identiques, mais

[26] Jean-Paul Siffre, *La Guerre électronique : Maîtres des ondes, maîtres du monde …*, Paris : Lavauzelle, 2003.
[27] *Doctrine interarmées – 3.6, La guerre électronique (GUERELEC)*, Paris : CICDE, EMA, ministère de la Défense, n°1522/DEF/EMA/EMP.1/NP, 2008.
[28] La cybernétique est la science qui utilise les résultats de la théorie du signal et de l'information pour développer une méthode d'analyse et de synthèses des systèmes complexes, de la biologie, et des sciences de l'information. Elle a été conceptualisée par Norbert Wiener dans les années 1940. (CNRTL ; Encyclopædia Universalis).
[29] Lance Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation", *Western Journal of Communication*, vol. 63, n° 3, 1999, p. 382–412.
[30] Brad Bigelow, *The Topography of Cyberspace and Its Consequences for Operations*. Tallin : NATO CCDCOE, 2018. 10th International Conference on Cyber Conflict.

d'autres se différencient fondamentalement. De manière générale, le cyberespace constitue un espace d'interaction global, fondé sur l'interconnexion de systèmes numériques, et structuré par des enjeux de pouvoir, de sécurité et de souveraineté[31]. Il regroupe l'ensemble des réseaux informatiques existants dans le monde[32], qu'ils soient interconnectés à Internet ou fonctionnant de manière isolée. Le cyberespace englobe à la fois les infrastructures de communication, les dispositifs terminaux connectés à ces réseaux, ainsi que les flux de données et les instructions qui y circulent[33]. Le cyberespace ne se limite pas à Internet : il recouvre également des systèmes fermés ou privés, utilisés par exemple dans les domaines industriel, militaire ou institutionnel.

La complexité du cyberespace se manifeste également à travers les désaccords de la littérature et des experts sur sa structure même. En fonction des auteurs, la composition du cyberespace peut aller de 3 à 7 couches[34]. Toutefois, la représentation du cyberespace selon trois grandes couches interdépendantes est la plus adoptée dans les définitions[35]. Sur chacune de celles-ci, des attaques cyber peuvent se dérouler, avec des modalités techniques spécifiques et des effets différenciés[36]. La première est la couche physique, où résident les infrastructures matérielles : réseaux, routeurs, câbles, processeurs, serveurs, satellites, terminaux, supports de stockage. Elle constitue la base tangible du cyberespace, est localisable géographiquement et relève de fait du champ de souveraineté d'un État[37]. Sur cette couche, les attaques peuvent par exemple prendre la forme de sabotages physiques, comme la destruction de serveurs ou de câbles. La seconde est la couche logique, qui regroupe les logiciels, les systèmes d'exploitation, les applications et l'ensemble des données. C'est celle-ci qui assure le traitement et la circulation de l'information. Ici, les attaques exploitent généralement des vulnérabilités dans les logiciels et consistent en des intrusions dans les systèmes, via des malwares, ransomwares, rootkits, chevaux de Troie, etc. ou des destructions, avec l'effacement de fichiers par exemple. Enfin, la troisième couche est sémantique, et elle renvoie aux contenus véhiculés : messages, données sensibles,

[31] Andrew N. Liaropoulos, "Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-Stakeholderism, and Power Politics." *Journal of Information Warfare*, vol. 15, n° 4, 2016, p. 14–26.
[32] Amer Eldebek, « Le cyber en Israël : quelle stratégie ? », in *Réflexions sur le cyber : quels enjeux ?*. Paris : Centre d'études stratégiques aérospatiales, IRSEM, n°32, 2015, p. 137.
[33] Lior Tabansky, "Basic Concepts in Cyber Warfare", *Military and Strategic Affairs*, vol. 3, n° 1, 2011.
[34] Frédérick Douzet. « La géopolitique pour comprendre le cyberespace », *Hérodote*, 2014/1, n° 152-153, 2014, p. 6-7.
[35] Martin C. Libicki, *Cyber deterrence and Cyberwar*, Santa Monica : RAND Corporation, 2009.
[36] Nicolas Mazzucchi, « La cyberconflictualité et ses évolutions, effets physiques, effets symboliques », *Revue Défense Nationale*, vol. 821, n° 6, 2019, p. 138-141.
[37]Frédérick Douzet. « La géopolitique pour comprendre le cyberespace », *op.cit.*, 2014, pp. 6.

images, vidéos. Les attaques perpétrées sur cette couche visent alors la manipulation de l'information, l'ingénierie sociale, ou la désinformation : elles exploitent les failles cognitives des usagers pour produire des effets psychologiques ou politiques. Cette modélisation met en lumière la complexité du cyberespace, à la fois technique, fonctionnelle et cognitive, et son ancrage à la fois dans le monde physique et dans l'espace informationnel. Du fait de ce triptyque, il existe une multiplicité de vecteurs pour des attaques cyber. Quant au spectre des effets produits par ces cyberattaques, il est très large. Il peut aller du simple ralentissement d'un système, avec des attaques en déni de service (DDoS[38]) jusqu'à l'altération de processus industriels, en passant par le vol de données ou la manipulation d'un environnement social ou politique. Dans tous les cas, les effets recherchés sont souvent cumulatifs, non immédiats, et distribués dans le temps et l'espace, ce qui renforce d'ailleurs la difficulté d'attribution et de riposte[39]. L'utilisation des cyberattaques ne vise pas nécessairement la destruction visible mais souvent la paralysie, la manipulation ou la subversion. En ce sens, le cyberespace permet d'exercer une forme de coercition indirecte, à distance, qui modifie profondément les modalités contemporaines de la conflictualité.

Le cyberespace a évolué au gré des mutations géopolitiques et technologiques pour devenir un véritable champ de conflictualité[40]. À partir des années 2000, la multiplication des cyberattaques a révélé les vulnérabilités systémiques du cyberespace. La prise de conscience par les États des capacités offensives du numérique, capables d'altérer la disponibilité, l'intégrité ou la confidentialité des systèmes adverses, a conduit à la militarisation progressive du cyberespace[41]. En 2016, l'OTAN a franchi un cap symbolique et stratégique en reconnaissant officiellement le cyberespace comme un cinquième domaine d'opérations militaires, aux côtés de la terre, de la mer, de l'air et de l'espace.

> *Aujourd'hui, à Varsovie, nous réaffirmons le mandat défensif de l'OTAN, et nous reconnaissons le cyberespace en tant que domaine d'opérations dans lequel l'OTAN doit se défendre aussi efficacement qu'elle le fait dans les airs, sur terre et en mer*[42].

[38] Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. (Wikipedia)
[39] Vincent Sébastien, « Qui s'y frotte, s'y pique : une stratégie intégrale pour réduire la subversion cyber », *Revue Défense Nationale*, Hors-série (HS3), 2022, p. 41-57.
[40] Didier Tisseyre, « Le cyberspace, nouveau théâtre de conflits », *L'ENA hors les murs*, vol. 504, n° 3, 2021, p. 40-42.
[41] Miguel Alberto N. Gomez, "Arming Cyebrspace: The Militarization of a Virtual Domain", *Global Security and Intelligence Studies*, vol. 1, n° 2, 2016, p. 43.
[42] Communiqué du Sommet de Varsovie publié à la suite de la réunion du Conseil de l'Atlantique Nord à Varsovie, les 8 et 9 juillet 2016, *OTAN*, Alinéa 7.

Sur le plan stratégique, l'institutionnalisation de la militarisation du cyberespace a légitimé la mobilisation de ressources militaires dans ce nouvel environnement, désormais envisagé comme un théâtre d'affrontement, au même titre que les milieux classiques, structuré par des doctrines, des unités spécialisées, et une compétition interétatique explicite[43]. Ce qui le différencie toutefois des milieux dits classiques – la terre, la mer, l'air et l'espace – c'est le fait que le cyberspace ne soit pas un bien commun mondial[44]. Il n'est pas délimité par des frontières géographiques, et il est un domaine créé par l'homme, dépourvu d'espace physique et donc de frontières. En tant que milieu, le cyber constitue un espace opérationnel spécifique, avec des caractéristiques propres : anonymat des attaquants, dissymétrie capacitaire, non-linéarité des effets, perméabilité civile-militaire, autonomisation technique des attaques[45]. En temps de conflits, le cyber permet d'agir en deçà du seuil de guerre déclaré, en menant des opérations de sabotage, d'espionnage ou de manipulation, sans franchir les lignes rouges du droit international humanitaire[46]. C'est pourquoi il est souvent décrit comme un milieu de confrontation indirecte, asymétrique, où la dissimulation, la ruse et l'effet de surprise prévalent sur la force brute[47]. Dans un contexte de compétition stratégique accrue entre grandes puissances, le cyberespace n'est plus seulement un espace de communication : c'est un outil stratégique, un vecteur de puissance, et un levier de coercition politique, économique ou militaire[48]. Il est devenu un véritable outil pour les États, un « multiplicateur de puissance[49] ». Ainsi, définir le « cyber » aujourd'hui revient à appréhender une réalité hybride, à la fois technique et stratégique, à la croisée de l'infrastructure numérique mondiale et des logiques de puissance.

L'articulation guerre électronique-cyber : rareté de la littérature académique

La GE, d'un côté, et le cyber, de l'autre, en tant qu'éléments à part entière de la guerre, ont suscité l'attention de nombreux chercheurs, associations, instituts, journaux. Pour se renseigner sur l'un ou l'autre, les ressources académiques, scientifiques, techniques et

[43] Lillian Ablon et al., *Operationalizing Cyberspace as a Military Domain: Lessons for NATO.* Santa Monica : RAND Corporation, 2019.
[44] David J. Betz and Tim Stevens, *Cyberspace and the state: toward a strategy for cyber-power*, Londres : Routlegde, 2011, p. 107.
[45] Chelsey Slack, "Wired yet disconnected: the governance of international cyber relations", *Global Policy*, vol. 7, n° 1, 2016, p. 69-78.
[46] Jean-Sun Luiggi, « Cyberguerre, nouveau visage de la guerre ? », *Stratégique*, vol. 2, n° 112, 2016, p. 91-100.
[47] Olivier Kempf, « Cyber et surprise stratégique », *Stratégique*, vol. 106, n° 2, 2014, p. 111-123.
[48] Hannes Ebert H and Tim Maurer, "Contested cyberspace and rising powers", *Third World Quarterly*, vol. 34, n° 6, 2013, p. 54-74.
[49] Olivier Kempf, « Du cyber et de la guerre », *op.cit*., 2015, p. 2.

médiatiques ne manquent pas. Il convient toutefois de noter que pour la GE, les ressources sont plus datées que pour le cyber, et restent souvent cantonnées aux aspects technique, industriel ou historique de la notion. Définir ces deux concepts de GE et de cyber consistait donc à passer en revue une grande quantité de ressources aux temporalités et aux angles différents. Mais la vraie complexité a plutôt été de trouver des sources qui évoquent, en même temps, pour un même sujet et une même période, la GE et le cyber. Il existe peu d'analyses qui comparent ces deux moyens et leur utilisation dans un même conflit. L'articulation GE-cyber n'apparait que dans de rares ouvrages, ou fait l'objet de courts chapitres qui se fondent souvent dans des rapports bien plus longs et généraux. Un ouvrage pionnier pour ce sujet est *Attention : Cyber !* de Aymeric Bonnemaison et Stéphane Dossé, publié en 2014. « Aujourd'hui, une nouvelle étape est franchie. Le monde des ondes et celui de l'informatique se rejoignent désormais dans le cyberespace.[50] » Par cette formule, le général Ract Madoux traduisait une intuition stratégique qui, en 2014, était encore peu partagée dans la littérature : celle d'une convergence irréversible entre deux sphères techniques longtemps pensées séparément. L'expression même de « monde des ondes » ou de « monde de l'informatique » souligne une dualité initiale, qui annonce en même temps leur convergence progressive dans un même espace d'action militaire. Ce livre a été l'un des premiers à analyser, comprendre et mettre en perspective la GE et le cyber, ensemble. L'ouvrage est cité dans de nombreuses sources gravitant autour de cette dynamique : papers de recherche, travaux académiques, rapports institutionnels et militaires. Avant de lier la GE et le cyber en tant que tels, les auteurs ont répertorié tout un historique de l'utilisation de la GE depuis la fin du XIX^{e} siècle. Ce point était également novateur à l'époque étant donné que les sources sur la GE, encore aujourd'hui, sont souvent très ciblées soit sur son aspect technique, de définition globale, ou de développement industriel.

Concernant la notion de distinction entre le cyber et la GE, les ressources se font rares également. Dans un article de la Revue Défense Nationale, Olivier Kempf relève plusieurs points clés pour distinguer l'espace électromagnétique et le cyberespace[51], et insiste sur leur différence de nature tout en reconnaissant l'existence d'intersections techniques. Kempf met en garde contre les confusions sémantiques ou technologiques qui pourraient conduire à des fusions hâtives de ces deux champs, et il souligne que leurs usages, leurs contraintes et leurs

[50] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 7.
[51] Olivier Kempf, « Distinguer le cyberespace et l'espace électromagnétique », *Revue Défense Nationale*, 2015/9, n° 784, 2015, p.15-21.

logiques restent fondamentalement distincts. Pour le colonel Samir Ouali-Djerbi, faire la distinction entre les objets est nécessaire et représente un prérequis à toute analyse de l'articulation cyber-GE[52]. Malgré l'apport de ces articles, réussir à distinguer cyber et GE à travers un même article n'est pas chose facile dans la littérature actuelle. Certains travaux sont, eux, davantage tournés vers la complémentarité GE-cyber. Pour ce faire, la plupart évoque le chevauchement technologique, fonctionnel et doctrinal entre cyberespace et GE[53]. Ces points communs permettent d'approfondir leur complémentarité d'un point de vue stratégique, où les capacités de l'un renforcent les effets de l'autre. Ces analyses restent toutefois cantonnées aux seuls aspects technique et abstrait. D'autres reviennent sur l'historique de cette potentielle convergence, et étudient comme la transformation technique des outils militaires a favorisé une interconnexion croissante entre les systèmes d'information et ceux d'armes, rendant ainsi possible une synergie tactique entre le cyber et la GE[54]. Enfin, certains écrits développent des concepts dans lesquelles le cyber et la GE sont compris ensemble. C'est le cas du concept d' « hybridité cyberélectronique » expliqué par Jean-Charles Coste[55], qui montre que certaines opérations combinent à la fois le brouillage, le sabotage de lignes de communication et les cyberattaques dans une logique unifiée, hybride. D'autres auteurs se concentrent également sur les angles tactique et opérationnel de la convergence GE-cyber[56], toujours à une échelle assez théorique et doctrinale. Ce croisement des champs d'action, pensé dans une optique stratégique, ouvre la voie à une relecture contemporaine de la guerre hybride, au centre de laquelle les milieux cyber et électronique prédominent. Enfin, de nombreuses études prospectives émettent des scénarios futurs sur l'utilisation combinée GE-cyber[57], et manquent de fait de cas concrets.

En somme, cet état de l'art est une illustration de l'intérêt d'un sujet de mémoire qui s'intéresse à l'articulation GE-cyber, dans un même travail, et avec des cas d'étude concrets. La littérature scientifique sur le sujet oscille entre deux tendances. La première est qu'elle

[52] Samir Ouali-Djerbi, « Guerre électronique et combat dans le cyber espace : quelle complémentarité ? », *op.cit.*, 2015, p. 83-88.
[53] Matt Thompson, "Blurring the Lines: The Overlap between cyber and electronic warfare", *The Journal of Electromagnetic Dominance*, 2023.
[54] Zsolt Haig, "Electronic warfare in cyberspace", *Security and Defence Quarterly*, vol. 2, n° 7, 2015, p. 22-35.
[55] Jean-Charles Coste, « De la guerre hybride à l'hybridité cyberélectronique », *Revue Défense Nationale*, vol. 2016/3, n° 788, 2016, p.19-23.
[56] Rémy Hémez et Anthony Namor « L'apport des actions cyberélectroniques aux opérations de déception tactiques et opératives », *op. cit.*, 2022, p. 199.
[57] B. Van Niekerk and M. Maharaj, "The Future Roles of Electronic Warfare in the Information Warfare Spectrum", *Journal of Information Warfare*, vol. 8, n° 3, 2009, p. 1–13.

distingue les deux concepts de manière très séparée. Dans ces travaux isolés, GE et cyber ne sont pas compris ensemble, et ils sont soit étudiés de manière technique, avec un point sur leurs caractéristiques propres, soit incorporés à une thématique plus large dont ils ne sont pas le cœur d'analyse. La deuxième tendance montre à l'inverse un effort analytique de s'intéresse à la relation GE-cyber. Cependant, cette dernière se fait uniquement dans une perspective théorique, technique, doctrinale ou future. Dans ce cadre, inutile de préciser que les influences de l'un sur l'autre d'un point de vue historique, évolutif et global, ne sont pas étudiées.

Méthodologie de la recherche

Construction de l'objet

La montée en puissance du cyberespace dans les écrits contemporains de sécurité a donné lieu à une production scientifique foisonnante. Le cyber est, depuis plus d'une décennie, envisagé à travers une variété d'approches — techniques, juridiques, stratégiques, historiques — et il s'insère dans de nombreux cadres d'analyse, souvent en lien avec les mutations de la conflictualité. Cette diversité a contribué à faire du cyber un objet central et transversal dans la recherche sur les transformations militaires. En comparaison, la GE apparaît bien plus en retrait dans les travaux académiques récents. Lorsqu'elle est traitée, c'est souvent à travers des publications à forte technicité, centrées sur les propriétés physiques des ondes, les capacités des équipements ou les performances industrielles. La réflexion stratégique sur la GE, en tant que moyen d'action à part entière dans la guerre, demeure relativement marginale. C'est en croisant ces deux trajectoires que s'est imposée la nécessité de réfléchir à l'impact concret de l'émergence du cyber sur l'évolution de la GE : non pas en termes de substitution, mais d'évolution des usages et des effets, et de compréhension conjointe de ces deux notions.

Les deux objets, bien qu'au cœur des transformations contemporaines de la conflictualité, sont encore rarement pensés de manière croisée et structurée. Ils apparaissent le plus souvent isolément, ou intégrés à des réflexions plus larges, sans articulation directe ni clarification de leurs caractéristiques respectives. Cette absence de traitement conjoint alimente un flou : s'agit-il de domaines séparés, complémentaires, ou en voie de fusion ? Le manque d'analyses combinées rend difficile l'identification des points de convergence, des zones de recoupement ou des évolutions différenciées. Ces éléments sont pourtant essentiels

pour distinguer les deux objets et mieux comprendre leurs actions, voire leurs effets mutuels, notamment lorsqu'ils coexistent dans les conflits actuels. L'intérêt de ce travail est donc de produire une analyse centrée sur l'articulation entre GE et cyber. L'objectif n'est pas de proposer une redéfinition stricte des deux, mais plutôt de retracer leurs trajectoires, d'éclairer leurs fonctions respectives, afin d'examiner les modalités concrètes de leur interaction dans les dynamiques conflictuelles contemporaines.

Question de recherche et hypothèses

Au tournant du XXIe siècle, la GE a vu émerger un nouvel environnement technique et stratégique : le cyberespace. À première vue, ces deux moyens – l'un issu des ondes, l'autre des réseaux – relèveraient de logiques séparées, tant dans leurs origines que dans leurs usages. Pourtant, les évolutions récentes laissent entrevoir une situation plus ambiguë. L'accélération des capacités numériques, la porosité croissante des champs d'opérations, mais aussi certaines configurations tactiques contemporaines tendent à rapprocher ces deux moyens. Dans certains conflits récents, ils semblent agir de manière articulée, dans des temporalités proches, sur des couches techniques parfois communes, avec des effets complémentaires. Dès lors, est-il encore pertinent de les penser séparément ? Cette tension est d'autant plus marquante que la distinction entre la GE et le cyber tend à s'estomper dans les écrits contemporains. Cette confusion, qu'elle soit sémantique, doctrinale ou politique, accentue la nécessité de questionner précisément la nature de leur relation. C'est dans cette dynamique que s'inscrit la problématique de ce mémoire : l'émergence du cyberespace dans les conflits contemporains a-t-elle eu un impact sur le paradigme et l'utilisation de la GE ?

À partir de cette question, plusieurs hypothèses ont été avancées pour orienter le travail de recherche. La première hypothèse est que la mutation des conflits, depuis la Guerre froide, a changé les manières de penser la guerre, mais aussi les priorités des États à investir dans la R&D pour des outils de guerre traditionnels. La GE est ancienne, et l'arrivée du cyber aurait pu être considéré comme un nouvel instrument plus flexible et adaptable aux nouvelles formes asymétriques et hybrides des conflits contemporains. De cette observation découle une deuxième hypothèse : le cyberespace aurait peut-être suscité la concentration des efforts et investissements nationaux, reléguant progressivement la GE au second plan. Enfin, la dernière hypothèse reste prudente sur la potentielle influence du cyber envers la GE. À partir des actions de la Russie en Ukraine depuis 2014, elle rappelle que l'utilisation de la GE dans les conflits reste stratégique et prédominante, et qu'il serait probablement faux de considérer

que le cyber a remplacé la GE. Tout au long de ce travail de recherche, une double interrogation s'est posée : d'une part, sur le devenir de la GE, face à un domaine cyber devenu omniprésent dans les représentations stratégiques ; d'autre part, sur la nature du lien qui se construit entre ces deux moyens dans les conflits actuels.

Éléments méthodologiques

L'approche méthodologique retenue pour ce travail de recherche repose sur deux temps. La première phase a consisté en l'analyse de nombreux travaux scientifiques, sources secondaires, documents institutionnels et doctrines. Concernant la GE, ce sont surtout des ouvrages complets, des chapitres d'ouvrages collectifs et des actes de colloques, parfois un peu datés, qui ont permis d'étoffer le processus de définition et de retracer son évolution. Si la littérature scientifique sur la GE était limitée, les doctrines régissant son utilisation et son développement étaient plus accessibles. Même si l'angle du sujet ne se prêtait pas à l'étude des doctrines militaires en elles-mêmes, elles auront permis de comparer les définitions et les évolutions de la GE, dans le temps et selon plusieurs États. Quant au cyber, la littérature scientifique et les working papers étaient bien plus abondants. Cependant, ces travaux mobilisent souvent le cyber avec un autre concept, ce qui a nécessité un travail d'extraction ciblée des éléments utiles à l'analyse pour ce mémoire. Concernant les sources primaires, les doctrines étatiques sont relativement récentes, et beaucoup d'écrits institutionnels, notamment de l'OTAN, font voir l'évolution de la considération du cyber dans les conflits.

Une seconde phase de la recherche s'est ensuite ouverte : la prise de contact avec plusieurs experts du domaine ou auteurs de travaux particulièrement pertinents. Un premier entretien a eu lieu avec le Colonel Éric Gomez, ancien officier renseignement de l'armée de l'air, ancien linguiste d'écoute, ancien commandant du CNC[58] et actuellement attaché de défense à Bagdad. Fort de son expérience dans le ROEM, la GE et la coordination des actions cyber, il a apporté un éclairage précieux sur l'articulation entre cyber et GE, tout en approfondissant et en réactualisant certains de ses écrits[59]. Un deuxième échange a été mené avec M. Pierre Baratault, ancien de Thomson CSF, aujourd'hui Thalès, et auteur d'un papier

[58] Créé en 2000, ce centre est une unité de la base aérienne 110 composé d'aviateurs et de militaires de l'armée de Terre et de la Marine nationale, aux ordres de l'état-major des armées. Ce centre est directement relié au Centre de Planification et de Conduite des Opérations, qui assure la planification et la conduite des opérations extérieures et intérieures. Le CNC est, de fait, un acteur essentiel des capacités d'intervention militaire de la France.

[59] Éric Gomez, « Focus 2. La guerre électronique », *op. cit.*, p. 79-85.

sur les recherches en GE entre 1960 et 1990[60]. Au croisement des mondes industriels et militaires, ses nombreuses connaissances ont permis de revenir sur l'évolution historique, technique et stratégique du spectre électromagnétique. Un troisième entretien a été conduit avec M. Serge Cholley, directeur Sécurité Défense chez Eutelsat. Anciennement officier général de l'armée de l'air, attaché de défense en Chine, chargé de responsabilités à la DRM, au CPCO, son expertise stratégique dans le renseignement, la spatialisation des conflits et l'articulation cyber-électronique, a été précieuse pour l'analyse du cas d'étude Ka-Sat. Le quatrième entretien, avec M. Yannick Genty-Boudry, a été riche en exemples concrets, et en sources difficiles d'accès. Son expérience très variée – OSINT chez Thalès, officier, enquêteur de terrain, journaliste technique chez Air&Cosmos, conseiller indépendant – a conduit à des angles de réflexion rarement explorés. Enfin, un dernier entretien avec M. Jean-François Grandin, expert en traitement intensif de données, est venu compléter les aspects techniques et clarifier la relation théorique du cyber et de la GE. Ce croisement de perspectives – institutionnelle, industrielle, militaire, technique et journalistique – a contribué à compenser la rareté des travaux scientifiques spécifiquement consacrés à l'articulation GE-cyber, et à enrichir la réflexion d'expériences et de savoirs inédits.

Démarche de réflexivité

La pluralité des sources et la rigueur méthodologique ne saurait toutefois masquer certaines limites inhérentes à ce travail de recherche. D'abord, le sujet traité implique un niveau de technicité élevé, notamment dans le champ de la GE, qui reste largement dominé par des publications techniques, industrielles ou militaires, souvent peu accessibles ou peu vulgarisées. À l'inverse, le champ du cyber fait l'objet d'une surabondance de publications, mais qui tendent à le diluer dans des approches très larges, ce qui rend difficile l'extraction d'éléments propres au sujet traité ici. Ensuite, l'articulation GE-cyber se heurte à deux obstacles majeurs : l'asymétrie temporelle des deux domaines et la faible visibilité de leur zone de recouvrement. Tandis que la GE s'est institutionnalisée dans les doctrines militaires depuis des décennies, le cyber en tant qu'espace de conflictualité est un phénomène bien plus récent – et donc moins stabilisé, tant sur le plan conceptuel qu'opérationnel. Ce décalage historique a parfois été une limite pour les comparaisons et les tentatives de conceptualisation commune. Enfin, ce mémoire a été pensé pour s'éloigner d'une approche

[60] Pierre Baratault, « La recherche en guerre électronique et ses retombées depuis 1960 », in *La Guerre électronique en France au XX*e *siècle*, Paris : Centre d'études d'histoire de la Défense, 2002. Actes du colloque organisé le 20 avril 2000 à l'École militaire, p. 97-116.

strictement technique, en optant pour un positionnement analytique et stratégique. L'objectif n'était pas de documenter les outils et les procédés opératoires propres à chacun des domaines, mais de comprendre comment ces deux espaces d'action militaire s'influencent, se croisent ou se distinguent, dans un contexte de mutation permanente des formes de guerre. Ce positionnement impliquait de fait un certain recul critique vis-à-vis des discours techniques ou doctrinaux, et invitait ainsi à s'interroger sur l'interopérabilité concrète et stratégique entre GE et cyber.

Annonce du plan

Ce travail s'organise en trois temps. Le premier chapitre retrace les origines de la guerre électronique et met en lumière la genèse technique de son articulation avec le cyber. Les continuités et les ruptures identifiées entre les deux objets permettent de nommer leur relation convergence et non fusion. Le deuxième chapitre poursuit l'identification des facteurs de convergence. Pour ce faire, il revient sur la Guerre froide et ses héritages stratégiques, pour analyser comment la transformation de la conflictualité a favorisé un rapprochement progressif entre guerre électronique et cyberespace. Enfin, le troisième chapitre propose une lecture empirique de cette convergence, à travers l'étude de cas concrets à l'Est de l'Europe, en particulier ceux impliquant la Russie.

Chapitre 1. Des origines de la guerre électronique à l'irruption du cyber : genèse d'une articulation technique

L'exploitation des ondes électromagnétiques a ouvert, dès la fin du XIX^{e} siècle, un nouveau champ d'action immatériel, rapidement investi par les forces militaires. À cette époque, l'ordre mondial est marqué d'une forte instabilité qui découle de l'affrontement permanent entre les grandes puissances[61]. L'arrivée des ondes sur le champ de bataille donne aux belligérants la toute nouvelle capacité de capter, perturber ou dissimuler l'information transmise par ce biais. Cet outil apparait vite comme un levier stratégique, au service de la connaissance de l'ennemi et du renforcement de la coordination interne de ses propres forces[62]. Cette maîtrise progressive de l'environnement électromagnétique marque une transformation silencieuse mais profonde de l'art de la guerre, que le général Jean-Paul Siffre résume par la formule « Si vis pacem, para bellum electronicum[63] ». Un siècle plus tard, c'est au tour de l'informatique de se développer. L'essor des réseaux et l'interconnexion progressive des machines, à partir du milieu du XX^{e} siècle, font émerger une nouvelle dimension : celle du cyberespace. Portant l'action au cœur de l'information numérique, il bouleverse les cadres traditionnels de la maîtrise informationnelle, et recompose les champs de la confrontation immatérielle. Dès lors, se pose la question de la place de la GE au sein de cette reconfiguration impulsée par l'outil cyber.

Comprendre comment la conflictualité a façonné la GE, de la fin du XIX^{e} au milieu du XX^{e} siècle (1.1), permettra ensuite de distinguer avec clarté les similitudes et les différences qui rythment son articulation avec le cyberespace (1.2).

[61] Robert Latham, "History, Theory, and International Order: Some Lessons from the Nineteenth Century", *Review of International Studies*, vol. 23, n° 4, 1997, p. 419–443.
[62] Olivier Letertre, Patrick Justel, Romain Lechâble et Stéphane Dossé, « Regards croisés sur la guerre électronique », *IFRI*, Focus stratégique 90, 2019, p. 9.
[63] Jean-Paul Siffre, « La conquête du spectre des fréquences électromagnétiques et son utilisation en guerre électronique », *op. cit.*, p. 13.

1.1. L'instabilité mondiale du XIX^e siècle à 1945 : la guerre électronique comme produit de la conflictualité

L'instabilité du XIX^e siècle et le développement industriel des puissances à l'époque ont été deux sources majeures à l'origine des révolutions technologiques dans la guerre[64]. La première révolution industrielle a donné naissance à la machine à vapeur et a été synonyme de progrès dans les domaines de la métallurgie et de l'outillage. À compter des années 1880, la seconde s'est établie sur une nouvelle vague industrialo-technologique, dominée par la chimie, l'électricité et le moteur à combustion interne. Puis, à la fin du XIX^e siècle et dans les premières années du XX^e siècle, les nouveaux progrès technologiques, notamment en électronique, ont permis la troisième révolution industrielle, aussi appelée révolution de l'information. Ces trois vagues majeures de révolutions ont été analysées par J.F.C Fuller[65]. Ce-dernier attache d'ailleurs de l'importance à les différencier des progrès technologiques qui avaient eu lieu dans les siècles précédents. Aux temps pré-modernes, la technologie revêtait déjà de l'importance, et les innovations technologiques avaient des conséquences sur la manière de faire la guerre. Cependant, les changements étaient lents, à tel point qu'ils laissaient assez de temps pour qu'une sorte d'équilibre s'installe entre chaque étape de développement de ces technologies militaires[66]. À l'inverse, le début de l'ère industrialo-technologique a rompu avec ce rythme. Comme Fuller l'avait prédit, les changements se faisaient désormais si rapidement que : « la meilleure armée de sa génération serait incapable d'affronter en terrain découvert un adversaire bien équipé de la génération suivante[67] ». Dès lors, chaque évolution technologique représentait une nouvelle étape essentielle à franchir pour toute armée qui souhaitait rester dans la compétition. Et c'est dans ce contexte qu'est née la GE.

1.1.1. Les réseaux à la fin du XIX^e siècle : de l'outil stratégique à la nouvelle cible militaire

En 1837, l'invention de la machine télégraphique électrique de Samuel F.B. Morse a donné naissance à la ligne Washington-Baltimore, la première démonstration d'un système

[64] Azar Gat, « VII. Les révolutions technologiques dans la guerre, des débuts de l'âge industriel au XXI^e siècle », in Jean Baechler et Christian Malis, *Guerre et Technique*, Paris : Hermann, 2018, p.107-119.
[65] John F.C. Fuller, *The Foundations of the Science of War*, Londres : Hutchinson & Co., 1926.
[66] Azar Gat, « VII. Les révolutions technologiques dans la guerre, des débuts de l'âge industriel au XXI^e siècle », *op.cit.*, 2018, p.107.
[67] Azar Gat, *ibid*., p. 107.

de communication filaire à courant électrique[68]. En 1850, la première liaison transmanche est installée[69], et en 1858, le premier message transatlantique est échangé entre la reine Victoria et le président américain Buchanan[70]. Sans tarder, le téléphone de Bell voit le jour en 1876[71], suivi de la télégraphie sans fil (TSF) de Marconi en 1896[72]. Ces innovations électriques n'ont cessé de préparer le terrain à la GE. En effet, puisque chaque découverte scientifique est vouée à être exploiter par les autres domaines de la société, ces innovations électriques n'ont pas tardé à être intégrées dans les recherches et les stratégies militaires du monde.

De la guerre de Crimée à la guerre de Sécession, quand le fil devient front

En 1853, la guerre de Crimée incarne la toute première mise en réseau de l'espace de bataille[73]. En trois ans, cette mise en réseau s'étend des corps expéditionnaires à leur capitale. À Paris, le commandement par les forces impériales à travers le réseau marque le premier cas « d'entrisme » d'un état-major à distance dans les opérations en cours[74]. De leurs côtés, les Ottomans et les Britanniques développent les leurs dans la région avec des réseaux tactiques et stratégiques[75]. Quant aux Russes, ils mettent en œuvre une ligne entre Saint-Pétersbourg et Sébastopol. À cette époque, cette mise en réseau n'avait fait l'objet d'aucune action d'ampleur pour contrer sa création[76]. En ce sens, la télégraphie, et plus largement les réseaux, étaient considérés à cette époque comme des moyens, des outils techniques à la pointe de l'innovation, pour commander à distance et instaurer un intermédiaire entre les niveaux stratégique et tactique. Les télécommunications en tant que telles n'étaient pas, ou peu, attaquées par l'adversaire. Elles ne constituaient pas, en soit, une cible.

---

[68] Louis Cahen, « La télégraphie électrique des origines au début du XX[e] siècle », *Revue d'histoire des sciences et de leurs applications*, vol. 1, n° 2, 1947, p. 142.
[69] Bruno Marnot, « Chapitre 8 - Révolution maritime et communications transatlantiques », in *La mondialisation au XIX[e] siècle (1850-1914)*, Paris : Armand Colin, 2012, p. 213.
[70] Paul M. Kennedy, "Imperial cables communications and strategy, 1870-1914", *The English Historical Review*, vol. 86, n° 341, 1971, p. 731.
[71] Randy Alfred, "March 10, 1876: 'Mr. Watson, Come Here ... '", *Wired*, 10 mars 2008 (https://www.wired.com/2008/03/dayintech-0310/).
[72] Jean Cazenobe, « Les origines de la télégraphie sans fil », *Cahiers d'Histoire et de Philosophie des Sciences*, vol. 16, n° 15, 1981, p. 35.
[73] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 69.
[74] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 18.
[75] Yakub Bektas et Michèle Albaret, « La télégraphie au service du sultan ou le messager impérial », *Réseaux*, vol. 12, n° 67, 1994, p. 143-152.
[76] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 19.

Il en va autrement lors de la guerre de Sécession[77], survenue seulement cinq ans après la guerre de Crimée. Au niveau stratégique, le président Lincoln avait nationalisé des lignes privées pour la guerre, tandis qu'au niveau tactique, le télégraphe électrique servait au guidage de tirs d'artillerie. Il permettait ainsi une communication bidirectionnelle en temps quasi réel. Il donnait aux hauts gradés la possibilité d'exercer le commandement et le contrôle tout au long de la guerre. Les dirigeants de l'Union, tout comme ceux de la Confédération[78] pouvaient communiquer avec leurs commandants supérieurs sur les stratégies, les mouvements et les événements sur le terrain. Le président Lincoln passait des heures chaque jour dans son bureau télégraphique militaire à Washington pour recevoir des mises à jour et donner des instructions à ses commandants. Envoyer des messages sur les 24 000 kilomètres de fil tendus pour les opérations télégraphiques pendant la guerre était facile ; et il était également facile de les intercepter[79]. En effet, avec le déclenchement de cette guerre, les lignes télégraphiques sont devenues l'une des cibles les plus importantes. Le trafic télégraphique militaire était détourné vers de mauvaises destinations, de faux ordres étaient transmis aux commandants de l'Union et des lignes étaient coupées pour intercepter des informations destinées aux forces de l'Union[80]. Ces usages peuvent être considérés comme les premières étapes du commandement et du contrôle des communications par les réseaux, ainsi que des exemples précoces de renseignement et de tromperie[81]. Ces premiers combats sur la couche logique[82] des réseaux ont été duals. D'une part, le niveau de commandement opératif déjà existant durant la guerre de Crimée, afin de connecter les niveaux stratégique et tactique, a continué de se développer durant la guerre de Sécession et a donc permis la coordination et le commandement à distance des troupes armées. Il ne s'agit donc pas d'un outil novateur, mais d'une utilisation plus poussée et perfectionnée de ce qui se faisait déjà en Crimée. D'autre part, le fait que les communications aient été détournées en profondeur représente ici une nouvelle utilisation des réseaux, où les télécommunications deviennent des cibles directes d'attaques.

[77] La guerre de Sécession est le nom donné à la guerre civile américaine qui s'est déroulée de 1861 à 1865.
[78] L'Union et la Confédération sont les deux camps de la guerre de Sécession : l'Union représentant les États du Nord abolitionnistes (présidés par Lincoln), et la Confédération ceux du Sud, les États confédérés esclavagistes.
[79] National Security Agency, *Civil War Signals: Ominous music and drum beat*. Maryland : NSA, s.d.
[80] Alfred Price, *The History of US Electronic Warfare*, Alexandria : Association of Old Crows, vol. 1, 1984, p. 41.
[81] J. P. R Browne and Michael T. Thurbon, *Electronic Warfare*, Washington : Brassey's, 1998.
[82] Nous reprenons ici la notion de couche logique du cyberespace afin de désigner la partie de la transmission et de la circulation des informations.

Au-delà d'un combat indirect sur les télécommunications à travers la couche logique, le combat sur les réseaux a aussi été physique. Si le codage a été développé pour tenter de protéger les communications, et donc protéger la couche logique, des patrouilles ont également été déployées par l'Union pour surveiller les lignes sur le terrain, soit, la couche physique. Celles-ci étaient chargées de contrer les attaques confédérées, qui étaient perpétrées par des unités « spécialisées », mises sur pied par la Confédération pour « détruire des câbles ou mener des opérations de déception et d'écoute – innovation de cette guerre –, dans le territoire contrôlé par l'Union[83] ». Ces actions d'agression sur les télécommunications marquent en effet une nouvelle étape. Alors que les conflits précédents montraient l'importance de la télégraphie pour la communication et la coordination des armées, la guerre de Sécession a ouvert la voie à un combat direct sur les réseaux. Tandis que la GE n'en est, à l'époque, qu'à ses prémices, les notions de contre-mesure et de contre-contre-mesure trouvent dans ce cas d'étude leurs ancêtres.

> *La "guerre civile" américaine constitue le prodrome de la guerre industrielle qui sera portée à son paroxysme au siècle suivant. Conceptuellement, la plupart des tactiques de combats sur les réseaux datent de cette période et sont adaptées de formes de combats plus anciennes. Elles ont perduré ensuite avec des techniques différentes et renouvelées, se combinant entre elles et devenant plus complexes au fil du temps[84].*

De 1870 à 1900 : l'avènement des trois domaines de la guerre électronique

La guerre franco-allemande de 1870 aboutit l'avènement des trois grands domaines de la future GE[85] : l'attaque électronique, ou contre-mesures ; la protection des activités électroniques, ou contre-contre-mesures ; et le soutien électronique, ou ROEM. Avec l'analyse précédente sur la guerre de Sécession, il convient de noter que ces deux premiers domaines, attaque et protection, avaient déjà été initié. D'une part, les belligérants protégeaient leurs lignes de communication, que ce soit par du codage pour la couche logique ou par des troupes armées directement près des lignes physiques ; d'autre part, chacun menait des actions d'agression sur les lignes adverses, afin de dévier les communications ou de détériorer les couches physiques des lignes. En 1870, ces constatations sont toujours

[83] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 19.
[84] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p.19.
[85] Entretien avec M. Pierre Baratault.

exactes[86]. À celles-ci s'ajoute toutefois le domaine du renseignement. Il ne s'agit pas du ROEM ou soutien électromagnétique actuel, effectué à travers les ondes du spectre électromagnétique pour obtenir des informations en tout genre, mais plutôt de son inverse, et en quelques sortes, de son ancêtre : le renseignement physique et humain à partir de n'importe quel vecteur, pour obtenir de l'information sur les moyens de transmission adverses. En ce sens, il est incorrect de parler de la naissance du ROEM, car il n'y avait pas d'exploitation des ondes à des fins de renseignement. Toutefois, il est intéressant de noter que le développement des moyens électroniques et la stratégie établie pour les transmissions avaient recours à du renseignement :

> *À partir du 18 septembre [1870], M Steenacker organise avec ses télégraphistes un réseau zonal de renseignement humain au sud-ouest de Paris […]. Les opérateurs recueillent des informations de la population, observent les forces ennemies et les transmettent à Tours, jusque sous le feu de l'ennemi malgré le risque d'être fusillé pour espionnage ou tué dans les combats […]. Certains opérateurs civils se sont même infiltrés au-delà des lignes ennemies soit pour renseigner, soit pour rétablir les communications avec Paris, soit pour les saboter. Il faut citer en exemple les missions de M. Lemercier de Jauvelle, dans l'Essonne en octobre-novembre, au sud de Paris en novembre-décembre et au nord-ouest de Paris en décembre-janvier*[87].

Ce renseignement physique et humain, aussi utile soit-il à l'époque, reste encore extérieur au réseau lui-même : il ne pénètre ni dans ses logiques internes, ni dans ses flux informationnels. À ce stade, la guerre n'exploitait donc pas encore les transmissions ennemies comme vecteur direct d'information ou d'agression. Néanmoins, l'innovation technologique de ce siècle était rapide[88]. Il n'aura fallu attendre que quelques décennies pour que le renseignement franchisse le seuil décisif de l'intrusion dans le système de communication adverse, et non plus seulement son observation ou sa perturbation périphérique, par le biais du renseignement humain. La guerre hispano-américaine de 1898[89], à Cuba et dans les Philippines, répertorie les premiers combats sur les réseaux, au niveau stratégique. L'objectif visé est celui du contrôle de la télégraphie, et les moyens employés pour cela sont la coupure des câbles et le filtrage des communications[90]. Parallèlement, la guerre des Boers constitue un autre exemple, avec la censure britannique

[86] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p.19.
[87] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p.21.
[88] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p.20.
[89] Stéphane Dossé et Joffrey Guerry, "Combat dans le cyberespace : la bataille des câbles au XXIe siècle ?", *Défense et Sécurité Internationale*, n° 74, 2011, p. 54–55.
[90] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 22.

sur les câbles[91]. Entre 1870 et 1880, la TSF, qui utilise le spectre électromagnétique, a fait l'objet de recherches scientifiques et techniques. En 1900, elle devient réellement opérationnelle et ouvre ainsi la possibilité de la GE. « En moins de 7 ans, la GE est passée d'une éventualité académique à un emploi opérationnel efficace[92]. »

Du fil au spectre : 1905 et le premier cas de brouillage à usage opérationnel réel

La guerre russo-japonaise de 1904 à 1905 se déroule dans un contexte de rivalités impérialistes croissantes en Asie orientale, où le Japon cherche à s'imposer face à une Russie tsariste en pleine expansion vers le Pacifique. Dans cette région sous tension, où les alliances stratégiques comme l'Entente anglo-japonaise de 1902 jouent un rôle d'équilibre[93], ce conflit illustre comment l'ordre mondial instable du début du XX^{e} siècle a nécessairement accéléré l'innovation militaire par les technologies. Dans ce conflit, le milieu naval devient un terrain d'expérimentation inédit pour l'usage des ondes électromagnétiques. Dès le 14 avril 1904, le port russe de Port-Arthur, situé au sud de la péninsule chinoise du Liadong, est bombardé par les cuirassés japonais Kasuga et Nisshin[94]. L'usage de la liaison radio pour guider les tirs depuis de plus petits navires témoigne d'une première intégration des technologies électromagnétiques dans la manœuvre. Mais l'innovation majeure vient de la riposte russe : un opérateur capte les échanges nippons et utilise son propre émetteur comme brouilleur. Il parvient ainsi à perturber la manœuvre ennemie. Ce geste improvisé constitue le premier exemple documenté de brouillage à visée opérationnelle[95]. Cet épisode, encore isolé, annonce toutefois l'importance stratégique croissante des communications sans fil sur le théâtre des opérations[96]. À mesure que le conflit progresse, l'emploi du spectre électromagnétique s'intensifie : les Japonais apprennent de leurs erreurs électroniques et sont fournis en matériels d'écoute par les Britanniques[97] ; et les Russes ne cessent de développer leurs capacités. En octobre 1904, les informations transmises par la TSF, codées en morse, ne se distingue pas fondamentalement des telex et télégrammes qui circulent sur les réseaux

[91] Michael T. Thurbon, "The Origins of Electronic Warfare", *The RUSI Journal*, vol. 3, n° 122, 1977, p. 58.
[92] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 22.
[93]Gilbert Bonifas et Martine Faraut, « Les liaisons dangereuses (1902-1914) », in *Pouvoir, classes et nation en Grande-Bretagne au XIX^{e} siècle*, Paris : Elsevier Masson, 1992, p.225.
[94] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 23.
[95] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 23.
[96] Abdul Karim Baram, "Technology in Warfare: the Electronic Dimension", *The Emirates Center for Strategic Studies and Research*, 2008, p. 16.
[97] Pierre-Alain Antoine, « De la nécessité de développer la Guerre Électronique sous toutes ses formes pour l'armée de l'Air et de l'Espace », *Athéna-Défense*, 2023, p. 2.

câblés océaniques. En revanche, la nouveauté est que ces informations peuvent être diffusées depuis des points mobiles, et donc des réseaux éphémères et mouvants[98]. La flotte de la Baltique, russe, envoyée en renfort par l'amiral Rozhestvensky, est équipée de systèmes de télécommunications, notamment de moyens radio, parmi les plus avancés de l'époque. Toutefois, leur utilisation reste mal maîtrisée, et leur efficacité est affaiblie par le manque de coordination et d'expérience du commandement russe[99]. En effet, les transmissions russes, souvent non cryptées ou trop fréquentes, deviennent une mine d'information pour le camp nippon. L'amiral japonais Togo, conscient de cet avantage, met en place un réseau de veille alliant postes d'écoute, réseau de guet visuel et coordination radio. L'absence de silence radio côté russe permet ainsi aux Japonais de localiser avec précision les mouvements adverses et d'anticiper son itinéraire. Cette asymétrie informationnelle culmine lors de la bataille décisive de Tsushima, les 27 et 28 mai 1905. Tandis que la flotte russe approche, l'amiral Togo s'appuie sur la TSF pour coordonner les mouvements de ses escadres, même en cas de brouillard ou de perte de contact visuel. Ces communications mobiles et dynamiques, rendues possibles par la TSF, offrent une flexibilité opérationnelle inédite. À l'inverse, les Russes, désorganisés et mal synchronisés, restent fragmentés et ne parviennent pas à exploiter efficacement leurs propres capacités radio. L'asymétrie dans la maîtrise du spectre électromagnétique devient de fait un facteur déterminant du succès japonais. En juin 1905, un article de la Japan Gazette met en évidence le rôle des communications : « Jamais l'électricité n'a joué un rôle aussi important dans la conduite de la guerre que du côté japonais ». D'ailleurs, l'emploi de la TSF est directement mentionné dans le rapport définitif de l'Amiral Togo sur la bataille dans la mer du Japon : « ... peu après, ayant reçu un ordre télégraphique de rassemblement à l'île Ulleung, les amiraux cessèrent les opérations et firent route au Nord-Est[100] ». La bataille de Tsushima ne se résume donc pas à une victoire navale classique : elle constitue le premier exemple de supériorité tactique fondée sur l'exploitation du spectre électromagnétique, à la fois en écoute, en coordination et en brouillage. Cet usage pionnier de la GE, encore embryonnaire mais déjà décisif, inaugure une nouvelle dimension de la guerre moderne où maîtrise de l'information rime avec spectre électromagnétique.

[98] Jean-Marc Sarale, « La bataille de Tsushima - Discours de presse et déplacements de représentations », in Dany Savelli, *Les Carnets de l'exotisme 5 : Faits et imaginaires de la guerre russo-japonaise*, Sète : Kailash Éditions, 2005, p. 91-109.
[99] Jean-Marc Sarale, *ibid.*, p. 97.
[100] Ces éléments d'archive ont été répertorié dans le minutieux travail de reconstitution de la bataille de Tsushima de M. Jean-Marc Sarale, *ibid.*

Lorsque vous emploierez quelque artifice, ce n'est pas en invoquant les Esprits, ni en prévoyant à peu près ce qui doit ou peut arriver, que vous le ferez réussir ; c'est uniquement en sachant sûrement, par le rapport fidèle de ceux dont vous vous servirez, la disposition des ennemis, eu égard à ce que vous voulez qu'ils fassent[101].

Selon Sun Tzu, le renseignement est la matière la plus importante dans l'art de la guerre, car sans informations sur l'ennemi, un stratège ne peut élaborer de plans de batailles efficaces. Ce principe fait de l'asymétrie d'information un facteur déterminant dans les conflits depuis toujours. En ce sens, le spectre électromagnétique, puisqu'il constitue l'un des vecteurs de l'obtention d'informations en temps de guerre, est lui-aussi, dès sa première utilisation, devenu un outil indispensable de la guerre. Le précédent majeur engendré par la bataille Tsushima ouvre ainsi la voie à l'intégration croissante des moyens électromagnétiques dans les stratégies de combat modernes.

1.1.2. La Première Guerre mondiale : laboratoire improvisé de la guerre électronique

En 1914, les transmissions radio ne sont encore perçues que comme un moyen parmi d'autres de communication militaire, et aucune armée ne dispose alors d'une doctrine ou d'un projet structuré visant à exploiter, contrôler ou perturber l'environnement électromagnétique. Comme le rappelle Louis Ribadeau-Dumas, il s'agit à cette époque d'une logique de renseignement encore fragmentaire : « Avant 1914, aucun des futurs belligérants n'avait de projet de GE. Seuls étaient envisagés les écoutes, l'interception des messages et leur décryptage[102]. » Pourtant, dès les premières semaines du conflit, des usages improvisés se multiplient, et esquissent les contours d'une pratique qui préfigure la GE. Dès le début de la guerre, la Tour Eiffel est réquisitionnée comme station TSF principale et devient rapidement un poste d'écoute majeur[103]. Son rôle n'est pas prévu par une doctrine particulière, mais il s'impose par nécessité et par opportunité. Sa puissance et sa hauteur permettent de capter une grande quantité de communications ennemies. Les premières interceptions révèlent des radiogrammes allemands envoyés en clair, ou chiffrés de manière

[101] Sun Tzu, « Article XIII : Le Renseignement », in *L'art de la guerre*, Paris : Milles et une nuits, 1996, n° 122, p. 100.
[102] Louis Ribadeau-Dumas, « La guerre électronique en 1914-1918 : deux faits marquants », in *La Guerre électronique en France au XX*e *siècle*, Paris : Centre d'études d'histoire de la Défense, 2002. Actes du colloque organisé le 20 avril 2000 à l'École militaire, p. 15-17.
[103] Jean-Marc Degoulange, « La tour Eiffel : premier système de guerre électronique », *Revue Historique des Armées*, 2017/3, n° 288, 2017, p.112.

rudimentaire, et créent ainsi des ruptures de sécurité majeures côté allemand[104]. L'impact tactique de ces écoutes se manifeste rapidement lors de la Bataille de la Marne[105]. En août 1914, les stations françaises parviennent à renseigner le GQG[106] sur les positions de la IIe armée allemande, détournée vers Maubeuge. Le général Joffre modifie alors ses plans et change le cours de la bataille[107]. C'est la première fois qu'un ROEM a un effet direct sur la conduite d'une bataille d'envergure. La détection des raids aériens allemands par les Alliés renforce cette dynamique.

> *Les écoutes permirent de relever les caractéristiques propres à ces raids : d'abord, avant leur départ, les Zeppelin essayaient leurs postes de TSF, dont la note particulière donnait l'éveil et permettait d'alerter les moyens de protection, "saucisses" et chasse. Ensuite, les Zeppelin se dirigeaient au moyen de relevés goniométriques : aussi bien en France qu'en Angleterre, ces liaisons furent brouillées avec succès. Certains disent même qu'ayant remonté le système de chiffrement correspondant, on put envoyer de faux messages pour les égarer*[108].

Rapidement, les opérateurs français remarquent que certaines stations reçoivent les signaux allemands plus fortement que d'autres. Cette différence s'explique par le mode de propagation des ondes longues utilisées à l'époque, qui voyagent au ras du sol et dont l'intensité diminue avec la distance. En comparant les niveaux de réception enregistrés dans différentes stations, il devient possible d'estimer la position des émetteurs ennemis. Ce procédé rudimentaire[109], mais efficace, permet de suivre la progression des postes de commandement allemands sur le front. Autrement dit, les caractéristiques physiques mêmes des ondes radio, jusqu'alors négligées, se transforment en véritable outil de renseignement opérationnel. Après ces épisodes, l'adversaire prend conscience de la vulnérabilité de ses communications radios. En conséquence, le trafic se réduit et les communications tactiques passent au téléphonique filaire. Mais cette adaptation comporte une nouvelle vulnérabilité :

---

[104] Nova, "5 Little-Known Facts About the Eiffel Tower", *NOVA Tech + Engineering*, 15 juillet 2024 (https://www.pbs.org/wgbh/nova/article/5-little-known-facts-about-the-eiffel-tower/).
[105] AGEAT, « Le suivi de la Bataille de la Marne par les écoutes secrètes françaises - journée du 8 septembre 1914 », *Association de la guerre électronique de l'armée de terre*, 8 septembre 2013 (https://www.ageat.asso.fr/spip.php?article130).
[106] Le GQG, Grand Quartier Général, est la structure de commandement française utilisée lors de la Première Guerre mondiale. Il assure le commandement de l'ensemble du corps de bataille français, de 1914 à 1919. Le général Joseph Joffre y est nommé commandant en chef des armées.
[107] Jean-Marc Degoulange, « La tour Eiffel : premier système de guerre électronique », *op.cit.*, 2017, p.114.
[108] Louis Ribadeau-Dumas, « La guerre électronique en 1914-1918 : deux faits marquants », *op.cit.*, 2002, p. 16-17.
[109] Il est possible de rapprocher ce mode opératoire d'une radiogoniométrie par intensité. La radiogoniométrie classique utilise l'angle d'arrivée d'un signal pour localiser un émetteur. Celle par intensité repose sur la comparaison de l'intensité du signal reçu par plusieurs stations fixes.

le phénomène de diaphonie[110]. Cette vulnérabilité technique est détournée à des fins de renseignement par le sous-lieutenant Delavie, En mars 1915, il met au point un dispositif d'écoute téléphonique à quelques dizaines de mètres des lignes ennemies, qui permet d'intercepter les conversations allemandes. En mai, ce poste d'écoute permet de détecter une attaque imminente, immédiatement contrée par l'artillerie. Le procédé est validé et étendu à la 1ère armée, puis à l'ensemble du front. Il est nécessaire de constater qu'à partir de ces évènements, la GE ne se limite plus à capter des signaux : elle consiste à les exploiter, les localiser, les décrypter, et à en tirer des décisions opératoires. C'est ce que confirme le cas de Verdun[111], en février 1916. Les postes d'écoute téléphonique installés autour de la ville interceptent des ordres qui prévoient une attaque allemande le 13 février. Grâce à cette alerte, les défenses françaises sont renforcées et l'attaque est annulée. Le sursis obtenu permet de réorganiser le secteur. Là encore, un renseignement d'origine électromagnétique détermine une manœuvre militaire concrète, dans un cadre désormais défensif. Les trois domaines de la GE – soutien ou ROEM, attaque ou contre-mesure, et protection ou contre-contre-mesure – apparaissent.

Après Verdun, la GE française se structure. La Tour Eiffel n'est plus seulement un poste d'écoute : elle devient un centre de coordination. Elle capte les transmissions diplomatiques et militaires, mais aussi les émissions vers les sous-marins allemands, les Zeppelins[112], et les communications économiques entre l'Allemagne et ses alliés. Elle participe au brouillage actif des stations ennemies, notamment Norddeich et Nauen, en émettant des signaux parasites sur les mêmes longueurs d'onde. Lors du raid des Zeppelin le 19 octobre 1917, la coupure volontaire de la station Eiffel — que les dirigeables allemands utilisaient comme repère — entraîne la désorientation de plusieurs appareils, dont l'un s'écrase près de Sisteron. En 1918, avec les dernières offensives allemandes, le système atteint sa pleine maturité, et le message intercepté le 1er juin devient le « radiogramme de la Victoire[113] ». Les postes d'écoute s'intègrent au réseau de la DCA, de l'aviation, et des communications interalliées. La Tour Eiffel participe à des opérations de guidage radio des avions alliés en territoire ennemi, par émissions coordonnées avec d'autres stations. Des

[110] À l'époque, les lignes téléphoniques n'utilisent qu'un seul fil pour transporter le signal. Le courant revient par le sol (la terre) pour former un circuit électrique complet. Mais quand plusieurs lignes passent près les unes des autres, le courant de l'une peut introduire un signal dans l'autre. C'est le phénomène de diaphonie.
[111] Jean-Marc Degoulange, « Verdun sur écoute », *Inflexions*, 2021/2, n° 47, 2021, p.57-61.
[112] Vincent Arbaretier, « Les écoutes de la Victoire, Général (2S) Jean-Marc Degoulange, Éditions Pierre de Taillac, 2019, 255 pages », *Revue Historique des Armées*, 2019/4, n° 297, 2019, p.139-140.
[113] Jérôme Poirot, « Tour Eiffel », in Hugues Moutout et Jérôme Poirot, *Dictionnaire du renseignement*, Paris : Perrin, 2018, p.774-776.

tentatives de camouflage, de brouillage, ou de désinformation sont également expérimentées. La GE s'étend au champ diplomatique, avec l'écoute des communications entre les puissances centrales et les pays neutres comme l'Espagne ou la Turquie.

> *La Première Guerre mondiale donna lieu à la première exploitation militaire importante du spectre électromagnétique avec l'utilisation de réseaux radio militaires, l'écoute et la localisation de ces émissions. La guerre électronique prit alors une importance de premier ordre pour les états-majors et les opérations, permettant d'obtenir du renseignement de niveau stratégique et tactique*[114].

Les exemples mentionnés dans cette démonstration relatent surtout des cas liés à la France, mais le combat sur les réseaux a été la préoccupation de toutes les parties prenantes à la guerre. Dans leur ouvrage, Aymeric Bonnemaison et Stéphane Dossé répertorient les utilisations électroniques de plusieurs pays[115], à leurs débuts : une maîtrise technique allemande défaillante aux conséquences lourdes ; l'excellence opérative et la performance tactique française ; les avancées britanniques positives en mer mais médiocres sur terre ; la maîtrise des Autrichiens ; les États-Unis en devenir de la GE.

1.1.3. De l'outil auxiliaire à la manœuvre stratégique : la guerre électronique dans la Seconde guerre mondiale

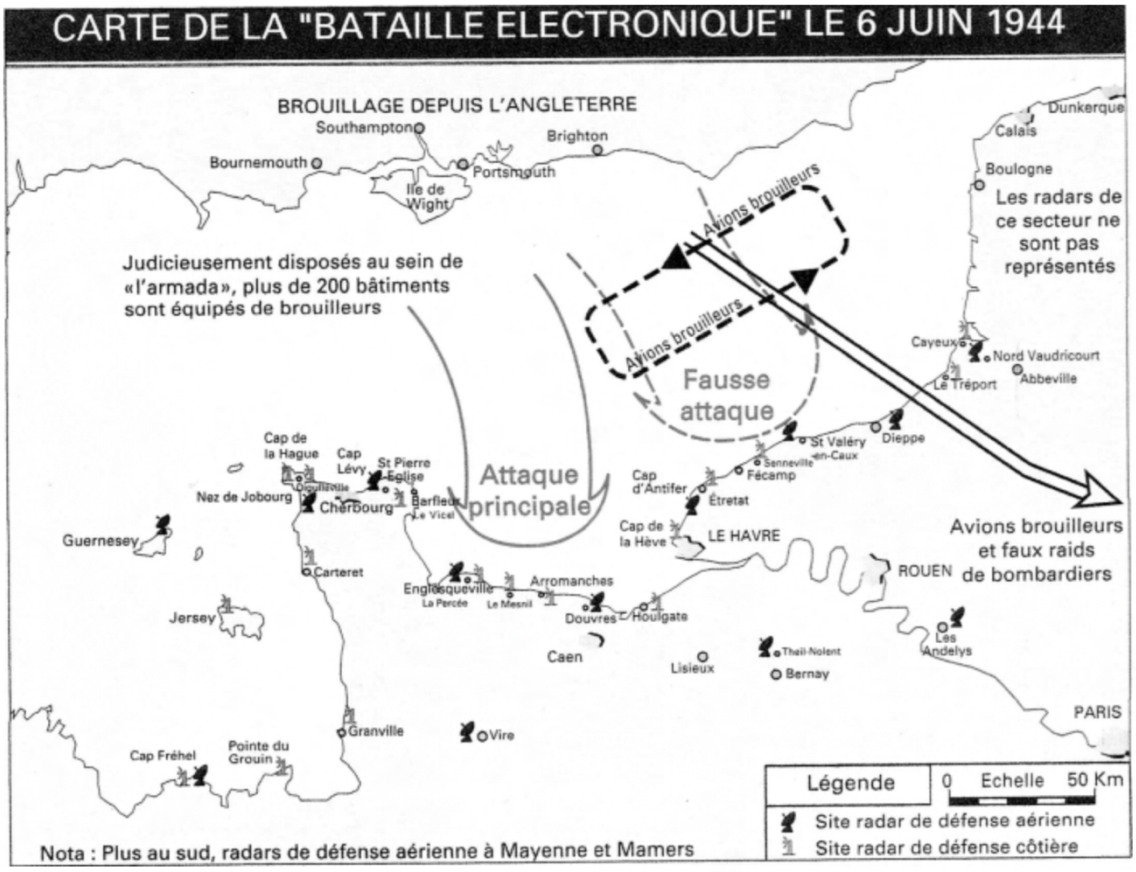
En 1930, la radiogoniométrie[116] à usage civile pour la navigation aérienne et maritime, puis la technologie radar apparaissent. À peine une décennie plus tard, la Seconde guerre mondiale confirme cette accélération technologique spectaculaire, ainsi que la vision stratégique qui est faite de la GE sur le champ de bataille. Les improvisations du conflit précédent laissent place à une exploitation systématisée, intégrée et technologiquement avancée de l'environnement électromagnétique. La radiogoniométrie, encore balbutiante en 1914-1918, atteint sa pleine efficacité en 1939. Du côté allemand, les stratégies de GE fusent dès les premières semaines du conflit. La Luftwaffe utilise la radionavigation pour diriger ses bombardiers sur des objectifs ponctuels en cas de mauvais temps ou en pleine nuit. Cette capacité reposait sur le système Knickebein : des stations terrestres sur le continent émettait

[114] Éric Gomez, « Focus 2. La guerre électronique », *op. cit.*, p.80.
[115] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 24-31. Les adjectifs utilisés dans ce court récapitulatif, pour résumer la maîtrise de la GE par les autres États, sont ceux donnés par les auteurs, dans des titres de passages consacrés à la GE chez les autres puissances.
[116] D'après la définition de Éric Gomez : la radiogoniométrie est utilisée dans le cadre de la navigation aérienne ou maritime. Elle s'appuie sur des procédés permettant de déterminer la localisation d'un émetteur d'ondes radioélectriques.

un faisceau radio, et lorsque celui-ci était croisé par un autre, la cible se trouvait en dessous[117]. Mais la riposte britannique se révèle encore plus performante : c'est l'épisode de la bataille des faisceaux[118]. Employée contre les U-Boot[119] allemands dans l'Atlantique[120], la radiogoniométrie britannique permet de localiser les transmissions ennemies et de guider les opérations de chasse sous-marine. Le brouillage ciblé des systèmes de radionavigation allemands limite également la précision de leurs raids aériens et maritimes. Les outils de GE restent des cibles à part entière. En 1942, lors du raid de Bruneval[121], des parachutistes britanniques s'emparent des éléments critiques d'un radar allemand, et permettent aux Alliés d'analyser son fonctionnement. Dès lors, les contre-mesures se multiplient. Des dispositifs de brouillage comme Moonshine simulent de fausses formations aériennes pour détourner les chasseurs allemands. Quant aux bombardiers alliés, ils utilisent des bandelettes métalliques pour saturer les radars adverses – Windows – d'échos parasites et ainsi rendre impossible leur localisation[122]. En 1943, des opérateurs britanniques germanophones transmettent de fausses instructions aux chasseurs allemands, et parviennent à perturber leurs opérations et semer le doute sur la fiabilité de leur chaîne de commandement. Les opérations de déception par les ondes se développent rapidement, encouragée par l'émulation du contexte de guerre. Avant l'opération Overlord en Normandie en 1944[123], ces techniques de saturation et de déception électronique sont utilisées au cours de l'opération Fortitude[124], d'avril 1944, pour masquer, en amont, le véritable point d'assaut du débarquement.

---

[117] David MacIsaac, "Through World War II: Air warfare", *The Editors of Encyclopaedia Britannica* (https://www.britannica.com/topic/air-warfare).
[118] Tom Whipple, *The Battle of the Beams: The secret science of radar that turned the tide of the Second World War*, New York : Bantam, 2023, p. 19.
[119] Sous-marins allemands, dont le but est de couler les navires ennemis. Pour leur coordination tactique, ils échangent de nombreux messages radios, cryptés à l'aide de la machine Enigma.
[120] Éric Gomez, « Focus 2. La guerre électronique », *op. cit.*, p.81.
[121] Tom Whipple, *The Battle of the Beams: The secret science of radar that turned the tide of the Second World War*, *op.cit.*, 2023, p. 224.
[122] Alfred Price, *Instruments of Darkness: The History of Electronic Warfare, 1939-1945*, Annapolis : Naval Institute Press, 2017, p. 48-51.
[123] Jean-Paul Siffre, « La Guerre électronique pendant le débarquement », *11ème escadre de chasse*, 5 septembre 2024 (https://www.pilote-chasse-11ec.com/la-guerre-electronique-pendant-le-debarquement/).
[124] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 45.



Source : Jean-Paul Siffre, « La Guerre électronique pendant le débarquement », *11ème escadre de chasse*, 2024.

Enfin, la cryptographie, encore rudimentaire lors de la Grande Guerre, franchit un seuil décisif[125]. L'interception et le décryptage des communications deviennent des priorités absolues. Le cas emblématique est celui de l'opération contre l'amiral Yamamoto : un message japonais, intercepté et déchiffré par les Américains, permet de localiser et d'abattre l'avion transportant le stratège de Pearl Harbor[126]. Dans ce domaine, les Alliés centralisent leurs efforts en regroupant les meilleurs spécialistes, notamment à Bletchley Park, où des percées majeures sont réalisées grâce à des figures comme Alan Turing[127]. En moins d'une génération, la GE est passée d'un ensemble d'initiatives fragmentaires à une arme systématique, intégrée à toutes les dimensions du combat. Son rôle dans la planification, la conduite et le succès des campagnes alliées est devenu incontournable.

[125] Bruno Berthet, « La guerre électronique en ébullition », *Le Magazine des ingénieurs de l'Armement CAIA*, n° 132, 16 juin 2024 (https://www.caia.net/revue-auteurs-rubriques-numeros/article/la-guerre-electronique-en-e-bullition/1407).

[126] Loïc Salmon, « La guerre électronique : nouvel art de la guerre », *Association nationale des croix de guerre et de la valeur militaire*, 13 février 2013 (https://croixdeguerre-valeurmilitaire.fr/la-guerre-electronique-nouvel-art-de-la-guerre/).

[127] Jean-Paul Gillyboeuf, « Guerre de l'information », in *La Guerre électronique en France au XXe siècle*, Paris : Centre d'études d'histoire de la Défense, 2002. Actes du colloque organisé le 20 avril 2000 à l'École militaire, p. 153-154.

De la fin du XIX[e] siècle jusqu'au milieu du XX[e], la GE a cessé d'être une simple possibilité technique pour devenir une nécessité stratégique. Conçue sur le terrain, perfectionnée par la rivalité technologique et intégrée dans les structures opérationnelles au fil des guerres, elle a progressivement imposé la maîtrise du spectre comme condition sine qua non de l'efficacité militaire. De l'instrument de soutien au levier décisif des opérations, son évolution témoigne de l'intégration irréversible de l'électromagnétique au cœur des conflits.

1.2. L'arrivée du cyber : prolongement sans effacement de la guerre électronique

La dynamique de pression exercée par la conflictualité sur l'innovation technologique peut aussi s'appliquer aux débuts de l'histoire des ordinateurs, et par analogie, du cyber. En 1938, Alan Turing[128], logicien et mathématicien, est enrôlé par l'armée anglaise. Au début de la Seconde guerre mondiale, l'une des clés de la victoire allemande est la machine à coder électromécanique Enigma[129]. Le rôle de Turing au sein du service britannique du chiffre, le Government Code and Cypher School, est alors de décrypter ces messages radio[130]. La mise au point de machines de décryptage inspirées de la « Bombe » polonaise permet d'exploiter les failles des communications allemandes, notamment dans la bataille de l'Atlantique. Malgré l'apparition en 1942 d'une nouvelle version d'Enigma[131], les Alliés retrouvent en 1943, avec l'aide des États-Unis et la saisie de documents ennemis, leur capacité d'interception. En 1944, l'invention du Colossus, premier ordinateur de l'histoire, donne aux cryptanalystes Alliés une puissance de calcul décisive. De fait, les ordinateurs, dont les ancêtres sont créés dans les années 1930, se développent davantage dans les années 1940 de la nécessité de décrypter rapidement les messages ennemis. Toutefois, après la guerre, il faut attendre les années 1960 pour avancer dans le milieu informatique. C'est à cette période,

[128] Concepteur d'une machine universelle qui formalise la notion d'algorithme ; précurseur des ordinateurs modernes.
[129] « Histoire de la machine Enigma », Cryptographie et codes secrets, *Bibmath*, (https://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/enigmaguerre).
[130] Michel Bezut, « Turing, Alan », in Hugues Moutouh et Jérôme Poirot, *Dictionnaire du renseignement*, Paris : Perrin, 2018, p. 795-798.
[131] David Kahn, *Seizing the Enigma: the race to break the German U-Boat cades, 1939-1943*, Barnsley : Frontline Books, 2012, p. 31-48.

sous l'impulsion de Joseph Licklider[132], qu'émerge l'idée d'interconnecter les ordinateurs pour faciliter l'accès et la circulation de l'information. En 1969, l'interconnexion à longue distance devient réalité : le socle technique d'Internet est posé, et avec lui, une nouvelle opportunité de communiquer. D'un point de vue militaire, l'intégration du cyber rime avec la notion d'Information Warfare, qui se traduit en concept opérationnel qu'à partir de 1996, avec le premier Field Manual[133] traitant de manière globale des opérations d'information. L'Information Warfare décrit le fait de « recueillir, fournir et nier des informations afin de faciliter la prise de décision tout en influençant négativement celle de l'ennemi[134] », grâce à divers moyens. Ce regroupement des moyens et vecteurs d'attaque annonçait la compréhension conjointe de toutes les actions visant à perturber la chaîne de commandement, les communications ou les perceptions adverses. Le fait que la GE et les cyberattaques visaient toutes deux l'information et utilisaient des supports immatériels a contribué à les penser ensemble, parfois jusqu'à les confondre ou à considérer que le combat cyber, plus récent, a supplanté la GE.

> *Pourquoi a-t-on été amené à confondre les deux objets […] ? C'est bien qu'ils présentent de nombreux points communs qu'on ne saurait nier. Au contraire, les relever est utile car cela permet de cartographier les zones d'intersections (où donc des mutualisations et des modes d'action communs sont possibles) qui révéleront, par contraste, les spécificités propres de chacun des espaces étudiés[135].*

1.2.1. Des intersections communes aux deux moyens : point commun ou point de rencontre

Un vivier de naissance hors de la sphère militaire

Une première similitude peut être celle de leur berceau de naissance. À la fin du XIX^e^ siècle, à la suite du TSF de Marconi, les milieux économiques intègrent rapidement ces nouvelles technologies de l'information dans leurs modes de fonctionnement. Ils comprennent l'intérêt d'écouter leurs concurrents et de les brouiller par les ondes. Les

[132] Joseph C. R. Licklider, "Man-Computer Symbiosis," in *IRE Transactions on Human Factors in Electronics*, vol. HFE-1, n° 1, 1960, p. 4-11.
[133] Les Field Manuals sont des manuels officiels publiés par l'armée américaine, destinés à définir des doctrines, procédures et pratiques opérationnelles sur un sujet donné.
[134] The United States Army War College, *A Return to Information Warfare*, U.S. Army Heritage and Eduction center, p. 2-3.
[135] Olivier Kempf, « Distinguer le cyberespace et l'espace électromagnétique », *op.cit.*, 2015, p.15.

agences de presse, entre autres, s'adonnent dès lors à une concurrence déloyale[136] et donnent de fait naissance, dans les années 1890, à l'ancêtre de la GE. Concernant l'informatique moderne, elle est datée à 1936 avec l'invention d'un modèle de fonctionnement des appareils mécaniques de calcul, par Alan Turing. Le développement des microprocesseurs et l'essor des télécommunications dans les années 1970 permettent de parfaire la naissance l'ordinateur moderne et favoriser l'expansion de l'informatique. Ce n'est qu'en 1968 que la sphère militaire, américaine, lance un appel d'offres pour construire un réseau qui puisse relier l'institut de recherche de Stanford, l'université de Los Angeles et l'université d'Utah. Fin 1969, les deux premières lettres du mot « login » parviennent à Stanford en provenance d'UCLA, et le réseau Arpanet est alors lancé[137]. La mise en place de ce réseau est encouragée par la DARPA, qui est chargée de développer de nouvelles technologies à usage militaire. D'autres réseaux sont créés en parallèle[138], comme le premier Bulletin Board System[139], en 1978, par Ward Christensen et Randy Suess. L'évolution de l'informatique devient rapide, de nouvelles opportunités de communication se créent, et avec elles, de nouvelles vulnérabilités apparaissent : les cyberattaques. De 1980 à la fin des années 1990, les génies de l'informatique et ceux qui pensent à des emplois différents de l'ordinateur ne sont pas les militaires, ni les entreprises, mais des individus dotés de compétences de *hacking* qui leur permettent d'utiliser ce nouvel outil comme ils l'entendent.

> *Les premières décennies sont celles de la démonstration technologique et parfois du désir de nuire des premiers hacktivistes […]. Avec l'entrée dans les années 1990, la donne change. […] Le "hacker astucieux" va céder en partie la place à des individus aux motivations plus inquiétantes utilisant leurs compétences dans des logiques négatives*[140].

De Kevin Mitnick[141] à Fry Guy, en passant par Fred Cohen, Morris Worm, Nahshon Even-Chaim ou encore Ehud Tenenbaum[142], les motivations sont souvent personnelles et techniques, avec des attaques perçues comme un jeu, un défi intellectuel. Peu à peu, l'appât du gain entre en scène et alors le profit est mis à l'honneur. La fin des années 1990 est rythmée par les virus. Il faudra attendre la moitié des années 2000 pour voir apparaitre des

[136] Éric Gomez, « Focus 2. La guerre électronique », *op. cit.*, p.80.
[137] Gérôme Billois, *Cyberattaques : les dessous d'une menace mondiale*, Paris : Hachette, 2022, p. 19.
[138] Gérôme Billlois, *ibid.*, p. 19.
[139] Les BBS sont, en quelque sorte, les ancêtres des réseaux sociaux.
[140] Gérôme Billlois, *ibid.*, p. 20.
[141] Tsutomu Shimomura, "Catching Kevin", *Wired*, 1er février 1996 (https://www.wired.com/1996/02/catching/).
[142] Bruce Middleton, *A history of Cyber security attacks: 1980 to present*, Abingdon-on-Thames : Taylor & Francis Group, s.d., p. 25-64.

cyberattaques d'ampleur, et l'implication étatique tant dans les motivations que dans les origines des attaques[143]. Ainsi, tant pour le spectre électromagnétique que pour le cyberespace, les toutes premières utilisations – parfois malveillantes – de ces nouveaux outils technologiques se font, respectivement, au sein des sphères commerciales ou individuelles. Il s'agit bien sûr de moyens d'attaque précoces qui feront par la suite l'objet d'une réappropriation, amplification, sophistication et utilisation massive par les États, et les armées. Cette caractéristique originelle des deux objets constitue un point commun : avant d'être utilisés sur le champ de bataille pour perturber l'adversaire, ils ont permis d'attaquer des cibles de niveau individuel, privé ou commercial. Ce point commun concerne un aspect de la naissance des objets, du vivier dans lequel ils ont été développés initialement. Cependant, il n'aborde pas les éventuelles similitudes qui pourraient être relevées à propos du fonctionnement technique.

L'utilisation de l'autre objet pour ses propres actions : des zones de chevauchement techniques

La GE et le monde informatique se recoupent aussi sur des aspects plus techniques, notamment leurs actions et effets sur le champ de bataille. Au niveau des objectifs militaires, les deux visent à perturber les opérations cinétiques, en empêchant, en altérant, ou en détruisant les informations ou communications ennemies[144]. Aymeric Bonnemaison et Stéphane Dossé considèrent que les actions électroniques, ainsi que celles cyber, peuvent être regroupées en trois grandes familles – sans compter les actions de défense bien connues : renseigner, agresser et tromper[145]. Olivier Kempf est parvenu à étudier les similitudes de ces deux objets en remarquant que, d'une part, « le cyberespace utilise en grande partie l'espace électromagnétique », et d'autre part, « l'espace électromagnétique s'est beaucoup cybernétisé[146] ». En effet, l'évolution technologique a renforcé l'interdépendance entre ces deux. Pour justifier que le cyberespace repose largement sur l'utilisation de l'espace électromagnétique, Olivier Kempf met en avant le fait que les signaux numériques, produits par l'encodage binaire 0/1 des informations, circulent non seulement à travers des infrastructures matérielles – comme les câbles de cuivre, les fibres optiques ou les circuits

[143] Gérôme Billois, *Cyberattaques : les dessous d'une menace mondiale*, *op.cit.*, 2022, p. 22-23.
[144] Matt Thompson, "Blurring the Lines: The Overlap between cyber and electronic warfare", *op.cit.*, 2023.
[145] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 14.
[146] Olivier Kempf, « Distinguer le cyberespace et l'espace électromagnétique », *op.cit.*, 2015, p. 15-16.

électroniques imprimés – mais aussi via les ondes électromagnétiques. Ces dernières sont notamment utilisées pour toutes les communications sans fil, telles que le Wifi, les réseaux mobiles 3G/4G/5G, ainsi que les satellites. Quant à l'espace électromagnétique, les recherches de Olivier Kempf montrent qu'il a été profondément transformé par la révolution numérique. Depuis les années 1990, la plupart des transmissions – radio, télévision, téléphonie mobile – sont passées d'une modulation analogique classique à une modulation numérique. En d'autres termes, les transmissions ne reposent plus sur des variations continues du signal – modulation analogique – mais sur un codage informatique des signaux, en série de 0 à 1, plus simple à traiter, à exploiter et à sécuriser – modulation numérique. Cette numérisation massive a permis d'intégrer directement dans des dispositifs cyber une grande partie des communications transitant par l'espace électromagnétique[147]. Cela a permis que des senseurs électromagnétiques, autrement dit des capteurs capables de capter et d'analyser les ondes radios et les signaux numériques présents dans l'environnement, puissent intercepter directement des données issues des réseaux civils et militaires, sans passer par les infrastructures filaires. Cette convergence s'incarne notamment dans des programmes militaires comme l'EC-130H Compass Call[148] ou Suter[149], de l'armée américaine, qui combinent interception des signaux et capacités d'action cyber. L'espace électromagnétique, au-delà d'être un vecteur de transmission, est donc aussi devenu un environnement numérisé. En ce sens, le cyberespace et le spectre électronique comportent des zones de chevauchement, où l'un permet la transmission des informations de l'autre, et inverse[150]. En l'occurrence, il ne serait pas exact de nommer cette intersection technique de « point commun » entre les deux espaces. En effet, il ne s'agit pas d'une caractéristique commune aux deux espaces, mais plutôt d'un moment dans l'action où l'un des objets utilise l'autre pour parvenir à son objectif. Il est donc plus juste de désigner cette intersection des moyens comme un point de rencontre ou zone de convergence. D'ailleurs, l'analyse des modes d'action de ces deux espaces révèlent des caractéristiques fondamentalement différentes, qui confirment la notion de convergence.

[147] Olivier Kempf, *ibid.*, p. 16.
[148] Laurent Lagneau, « L'US Air Force envoie un avion de guerre électronique EC-130H "Compass Call" en Pologne », *Opex360.com*, 9 juin 2019 (https://www.opex360.com/2019/06/09/lus-air-force-envoie-un-avion-de-guerre-electronique-ec-130h-compass-call-en-pologne/).
[149] Airforce Technology, "The Israeli 'E-tack' on Syria – Part I", *Airforce Technology*, 9 mars 2008 (https://www.airforce-technology.com/features/feature1625/).
[150] Zsolt Haig, "Electronic warfare in cyberspace", *op.cit.*, 2015, p. 30.

1.2.2. Des spécificités fondamentalement distinctes, vecteur de convergence plutôt que de fusion ou substitution

Dans un numéro de l'armée de l'air, le travail de recherche de Samir Ouali-Djerbi se propose d'étudier la complémentarité du cyberespace et de l'espace électromagnétique. Même si l'étude se concentre sur la convergence de ces deux moyens dans les opérations aériennes, les différences relevées entre les deux espaces afin de mieux cerner leur articulation restent valables pour cette étude.

> *Le caractère englobant du cyberespace […] relie aujourd'hui des mondes identifiés jusque-là comme irrémédiablement distincts. L'interpénétration et l'interconnexion entre les systèmes d'information et les systèmes d'armes est devenue un multiplicateur d'efficacité dans la planification, dans la conduite et dans l'exécution des opérations aériennes. Créant une synergie à une échelle jusque-là inégalée, le cyberespace a peu à peu émergé en tant que milieu propre qui dépasse le milieu physique sur lequel il repose. De facto, ce caractère englobant rendrait la dichotomie actuelle entre guerre électronique et combat dans le cyberespace aussi artificiel qu'obsolète*[151].

En ce sens, il s'accorde à dire qu'il est pertinent d'étudier ces deux objets ensemble. Toutefois, les étudier ensemble ne revient pas pour autant à les confondre ou à les fusionner. D'ailleurs, Samir Ouali-Djerbi pose la même interrogation que notre question de départ pour ce mémoire : « La guerre électronique serait-elle ainsi vouée à se dissoudre au sein de ce nouveau venu et à disparaître en tant que telle selon un schéma à l'allure darwinienne ?[152] » Sa recherche se cantonne à l'aspect technique des modes d'actions cyber et électroniques, et la réponse qu'il formule directement après sa question est : « Ayant chacun la capacité de produire des effets sur des systèmes d'arme, la GE et le combat dans le cyberespace constituent des manœuvres complémentaires qui n'ont pas vocation à fusionner mais à mieux collaborer[153]. » Avant de pouvoir relever des cas concrets de convergence cyber-électronique, il est nécessaire de cerner les points sur lesquels les deux se distinguent pour ensuite être en mesure de reconnaitre les actions de l'un ou de l'autre dans une attaque, et ainsi en déduire ou non des convergences.

[151] Samir Ouali-Djerbi, « Guerre électronique et combat dans le cyber espace : quelle complémentarité ? », *op.cit.*, 2015, p. 83.
[152] Samir Ouali-Djerbi, *ibid.*, p. 83.
[153] Samir Ouali-Djerbi, *ibid.*, p. 84.

Des espaces distincts dans leur nature physique

Malgré les interconnexions fréquentes entre opérations cyber et actions sur le spectre électromagnétique, les deux domaines reposent sur des espaces de nature fondamentalement différente[154]. L'espace électromagnétique est un milieu naturel, régi par des propriétés physiques objectives : il est constitué de l'ensemble des ondes électromagnétiques, des ondes radio jusqu'aux rayons gamma, qui se propagent selon des lois de la physique. Il est un continuum naturel, un champ, où les ondes émises par tous se propagent librement[155]. En cela, il est transversal aux milieux classiques – terre, mer, air, espace – qu'il peut traverser. À l'inverse, le cyberespace est un espace artificiel, créé par l'homme. Il existe par l'interconnexion de machines et par l'organisation numérique de l'information : sa couche physique, constituée d'ordinateurs, de câbles, de serveurs, n'est qu'une base. Elle doit nécessairement être complétée par une couche logique, qui assure la circulation des données par des logiciels, des protocoles de communication ; et une couche sémantique, qui porte le sens et l'interprétation des informations échangées. En effet, le cyber « ne devient un espace à part entière que par agrégation à cette première dimension, d'une dimension logique et d'une dimension sociale[156]. » Il est constitué d'îlots discontinus qui relèvent chacun de la souveraineté ou du contrôle de ses protagonistes. L'un est un milieu préexistant, l'autre est un construit humain reposant sur des technologies codifiées. Cette distinction initiale conditionne de fait des usages et des contraintes profondément différents.

Deux espaces apparentés mais non superposables

Si cyberespace et espace électromagnétique sont souvent utilisés conjointement, ils ne se confondent pas pour autant. Le cyberespace utilise parfois l'espace électromagnétique comme support physique, mais il le dépasse en structurant l'information dans un système codé et manipulable[157]. Ainsi, par exemple, un signal radar n'entre dans le cyberespace qu'au moment où son écho est capté, numérisé, puis traité en tant qu'information. Tant que l'onde n'est pas transformée en donnée, elle appartient strictement à l'espace électromagnétique.

[154] Olivier Kempf, « Distinguer le cyberespace et l'espace électromagnétique », *op.cit.*, 2015, p. 17-18.
[155] Mohinder Singh, *Electronic Warfare*, New Delhi : Popular Science & Technology Series (DESIDOC), 1988, p. 11-13.
[156] Samir Ouali-Djerbi, « Guerre électronique et combat dans le cyber espace : quelle complémentarité ? », *op.cit.*, 2015, p. 84.
[157] Jacob Cox et al., "The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence", *op.cit.*, 2019, p. 84.

C’est ce glissement, du physique au numérique, qui marque la séparation entre actions de GE et opérations cyber[158]. Les premières altèrent le signal brut tandis que les deuxièmes agissent sur l'information transformée. Cette frontière explique pourquoi les deux espaces exigent des approches techniques distinctes.

Des options opérationnelles différentes

Les options offertes par l’espace électromagnétique et par le cyberespace diffèrent dans leur nature et leurs effets[159]. La GE vise principalement à intercepter, perturber ou tromper les communications adverses en agissant directement sur les signaux émis : brouillage, interception radio, détection radar, et contre-mesures actives. Elle opère dans un environnement unifié, où les ondes se propagent librement, bien qu’avec des contraintes physiques. En revanche, le combat cyber s'exerce dans un environnement constitué d'espaces fragmentés et discontinus. Contrairement au spectre électromagnétique, qui forme un milieu unique traversable sans véritable frontière physique, le cyberespace est composé d’une multitude de réseaux distincts : chaque acteur, qu'il s'agisse des États, entreprises, organisations, individus, etc., contrôle son propre environnement numérique. Cet environnement numérique est lui-même protégé par des dispositifs de sécurité, des cloisonnements techniques avec les pares-feux ou la segmentation réseau, et des protocoles de défense. Il n’existe pas de continuité naturelle entre ces réseaux : il faut donc franchir des barrières pour passer d’un espace à un autre. De ce fait, les opérations cyber offensives ne peuvent pas s’appuyer sur une libre circulation : elles nécessitent d’infiltrer spécifiquement les systèmes adverses, par des moyens discrets et souvent complexes, pour mener des actions d’intrusion, d’espionnage, de sabotage ou de manipulation de données. Cette dynamique d’enfermement et de protection rend la manœuvre cyber beaucoup plus difficile que l'interception d'un signal dans l'espace électromagnétique ouvert. En d'autres termes, là où l'espace électromagnétique favorise une certaine liberté de mouvement dans l'interception ou la perturbation, le cyberespace impose souvent de franchir des barrières logicielles complexes avant d'atteindre une cible. Une fois cette distinction comprise, le titre donné par Samir Ouali-Djerbi à l’un de ses passages devient évident : « un espace électromagnétique,

[158] Samir Ouali-Djerbi, « Guerre électronique et combat dans le cyber espace : quelle complémentarité ? », *op.cit.*, 2015, p. 85.
[159] Olivier Kempf, « Distinguer le cyberespace et l’espace électromagnétique », *op.cit.*., 2015, p. 18-21.

des cyberespaces[160] ». Du fait de cette différence de structure du milieu électronique ou cyber, les opérations, même si elles visent un même objectif de déstabilisation de l'adversaire, sont par nature différentes. Dans une situation de conflit, mener une opération cyber nécessite de pénétrer l'espace numérique de l'adversaire, et cette manœuvre apparait bien plus délicate que l'exploitation du spectre électromagnétique ouvert. Cette discontinuité cyber limite la liberté d'action, complique la surveillance et exige une approche beaucoup plus ciblée et discrète pour éviter la détection par les adversaires. De fait, tandis que la GE peut viser des effets larges et simultanés sur tout un théâtre, le combat cyber impose des interventions plus chirurgicales.

1.2.3. L'outil cyber ou le prolongement de la guerre électronique

Contrairement à l'une des questions de départ de cette recherche, qui consistait à savoir si le cyber pourrait englober la GE, dans le sens de le substituer, les éléments démontrés plus hauts prouvent que ce n'est pas le cas. Si l'aspect empirique n'a pas encore été étudié, les actions et modes opératoires de ces deux espaces proposent une complémentarité dans leur utilisation et leurs effets, et non un remplacement du mode ancien – électronique – par le plus récent, le cyber. Le cyberespace a ouvert la voie à de nouvelles possibilités, à de nouveaux vecteurs d'attaques dans la guerre, mais il ne remplace pas les capacités de GE. Dans un conflit, la GE agit sur l'émission ou la réception des signaux électromagnétiques : elle intercepte, brouille ou trompe l'adversaire à travers la manipulation physique du spectre. Le cyberespace, lui, ne peut intervenir qu'après la capture et le traitement du signal sous forme numérique : il agit sur l'information stockée ou en cours d'exploitation, et non sur le signal brut, comme le fait la GE. Par exemple, dans une attaque contre un radar, la GE perturbera la détection en brouillant l'onde ou en créant de fausses cibles ; le combat cyber, lui, aura pour but d'altérer la base de données du radar ou le système qui analyse les échos, et ainsi fausser les décisions qui sont prises à partir de cette information[161]. Le cyber ne remplace donc pas l'action immédiate sur le spectre électromagnétique, mais il prolonge son effet en s'insérant dans la phase suivante, celle du traitement et de l'exploitation des données. La complémentarité est nette : la GE ouvre la brèche au niveau du signal, le cyber exploite cette brèche au niveau de l'information. Ensemble, ils permettent d'enchaîner perturbation

[160] Samir Ouali-Djerbi, « Guerre électronique et combat dans le cyber espace : quelle complémentarité ? », *op.cit.*, 2015, p. 85.
[161] Samir Ouali-Djerbi, *ibid.*, p. 87.

physique et désorganisation cognitive de l'adversaire, selon une logique de continuité opérationnelle. L'enjeu de distinction entre complémentarité et fusion de la GE et du cyber est également visible sur la page GE du site l'OTAN. L'un des points s'attache à définir la GE en la distinguant du cyber :

> *Il ne faut pas confondre guerre électromagnétique avec guerre et capacités cyber. Au sens large, les opérations cyber regroupent diverses techniques de piratage visant à infiltrer et perturber les systèmes informatiques d'une cible afin d'obtenir des renseignements ou de dégrader ses capacités. La guerre électromagnétique utilise l'énergie dirigée pour couper l'accès au spectre électromagnétique, bloquant ainsi des signaux entre des technologies qui deviennent de ce fait inopérantes. Bien sûr, en interférant avec l'infrastructure informatique, la guerre électromagnétique peut affecter les opérations dans le milieu cyber*[162].

Alors que la découverte du spectre électromagnétique résulte d'une dynamique scientifique, la GE a, elle, été façonnée par la conflictualité de la fin du XIX^{e} et du début du XX^{e} siècle, qui l'a fait devenir un instrument stratégique du champ de bataille. L'instabilité incessante de l'époque a précipité son appropriation militaire et son développement exponentiel. Si la GE a su s'imposer au cœur des opérations, l'irruption du cyberespace au tournant du XXI^{e} siècle a questionné son avenir. Néanmoins, l'étude croisée de leur nature intrinsèque montre que le cyberespace n'a pas supplanté le spectre électromagnétique. Le cyberespace a plutôt été synonyme d'un nouveau champ, aux caractéristiques propres, qui s'est ajouté à celui de la GE. Ce sont bien deux moyens complémentaires, dont l'interaction ne procède ni d'une fusion, ni d'une substitution. De fait, la compréhension de leurs trajectoires spécifiques permet de mieux saisir leur articulation contemporaine. Toutefois, elle ne saurait occulter un autre moteur fondamental de convergence : la mutation de la conflictualité. L'évolution de l'ordre international depuis la fin de la Guerre froide représente en effet pour cette étude une source importante de facteurs explicatifs de cette convergence. C'est à cette dynamique plus profonde qu'est consacrée ce deuxième chapitre.

[162] NATO website, « Electromagnetic Warfare », 2023 (https://www.nato.int/cps/fr/natohq/topics_80906.htm?selectedLocale=en).

Chapitre 2. La Guerre froide et la mutation de la conflictualité : autres origines de la convergence cyber-électronique

Si la complémentarité entre GE et cyberespace trouve une part de son origine dans leurs caractéristiques techniques distinctes, elle ne saurait être comprise pleinement sans les dynamiques liées au contexte historique. Après 1945, la bipolarité du nouvel ordre mondial remodèle les priorités stratégiques des puissances[163]. Les tensions qui pèsent sur l'équilibre géopolitique sont désormais d'une nature différente de la guerre traditionnelle qui a sévit la première moitié du XX^{e} siècle. D'une part, la conflictualité physique persiste, comme avec les guerres de décolonisation[164], mais celle-ci revêt une forme distincte, asymétrique et hybride, qui se cantonne souvent à l'ampleur régionale[165]. D'autre part, les rivalités entre les deux blocs ne se traduisent pas en affrontement direct, mais elles restent redoutables. En 1962, le monde frôle une troisième guerre mondiale avec la crise de Cuba[166], et les tensions sont rendues visibles. Pourtant, depuis 1945, elles rythmaient les relations internationales. Dans cette confrontation indirecte, invisible mais puissante, le spectre électromagnétique s'impose comme un outil stratégique fondamental pour les États. Son importance réside dans le fait qu'il est l'un des vecteurs qui rend possible l'espionnage[167]. Quelques décennies plus tard, au tournant des années 1990, la fin de la guerre froide et l'émergence d'un nouvel ordre international conduisent à la restructuration des armées, après que l'illusion d'une pacification mondiale ait été adoptée par les États. C'est dans ce contexte que le cyberespace fait progressivement son entrée dans les sphères militaires. Ces évolutions fonctionnelle et structurelle, ajoutées à la continuité technologique discutée précédemment, contribuent à retracer les trajectoires du rapprochement des deux objets cyber et électronique. Ce chapitre propose ainsi d'analyser deux autres facteurs de convergence, plus implicites : l'évolution des usages et fonctions de la GE avec la mutation des conflits (2.1.), et les réorganisations structurelles des armées du monde impulsées par la fin de la guerre froide (2.2.).

---

[163] Kenneth N. Waltz, "The New World Order", *Journal of International Studies*, vol. 22, n° 2, 1993, p. 189.
[164] Robert J. McMahon, "Decolonization and the Cold War: The Superpowers and the Anti-Colonial Insurgencies in Indonesia and Vietnam", *Journal of Global Strategic Studies*, vol. 3, n° 2, 2023, p. 3-19.
[165] Muzaffer Ercan Yilmaz, "Intra-state conflicts in the post-cold war era", *International Journal on World Peace*, vol. 24, n° 4, 2007, p. 11-33.
[166] Jay Elwes, "How the third world war was narrowly averted ", *The Spectator*, 8 mai 2021 (https://www.spectator.co.uk/article/how-the-third-world-war-was-narrowly-averted/).
[167] Alex Bruns, "The redundant spy", in Morgan Jones, Stuart Glover, Amy Barker, Chad Parkhill, et al., *A Most Provoking Thing: new writing from QUT*, Brisbane : Creative Industries, DOTLIT and Queensland University Technology, 2004, p. 123-130.

2.1. L'évolution de la guerre électronique face aux nouveaux conflits asymétriques : vers une proximité des finalités avec le cyber

Comme démontré dans le Chapitre 1, la GE a été façonnée par la conflictualité et les nécessités d'innovation pour contrôler davantage le pan informationnel des combats. À partir de 1945, l'ère de la Guerre froide s'ouvre et avec elle, des formes de conflits différentes auxquelles le spectre électromagnétique doit s'adapter. Jusqu'à la fin de la Guerre froide, les recherches dans ce domaine battent leur plein : des nouveaux équipements technologiques à l'espionnage en passant par quelques retours aux usages classiques, la GE incarne l'arme invisible de la Guerre froide. Avec l'intensité des recherches dans le domaine, le perfectionnement des usages, et la recherche d'effets toujours plus optimaux du combat sur le spectre, les objectifs électroniques atteints à la fin de la Guerre froide convergent sur certains points vers ceux cyber.

2.1.1. Un repositionnement doctrinal vers le renseignement

Alors que dans les précédents conflits le spectre électromagnétique incarnait l'appui tactique par excellence, la fin de la Seconde guerre mondiale marque pour lui un virage absolu vers l'acquisition de supériorité informationnelle. Déjà dans les décennies précédentes, la domination informationnelle était partie intégrante de ses objectifs. Mais avec la Guerre froide et l'évolution de la conflictualité, cet objectif devient priorité, ce qui s'explique notamment par le fait que le spectre des autres milieux est réduit, ou non exploitable. En cas de conflit physique, il est clair que les milieux traditionnels restent exploitables et continuent de présenter des opportunités stratégiques hors du spectre électromagnétique. Néanmoins, durant la Guerre froide, ce type de conflit conventionnel laisse rapidement place à des tensions qui se traduisent en affrontement indirect. Dès lors, il n'est plus possible pour un État d'obtenir un avantage sur les milieux classiques, sous peine d'être accusé de violer la souveraineté géographique des autres États ou de provoquer des incidents à l'escalade dangereuse. Il apparait ici évident que cette option n'était pas la plus judicieuse dans ce contexte où la moindre erreur pouvait signer le début d'une troisième guerre mondiale. En ce sens, la domination informationnelle, déjà indispensable aux belligérants avant 1945, devient désormais l'un des rares moyens de s'assurer un avantage stratégique sans déclencher d'affrontement direct, et le spectre électromagnétique, l'un des vecteurs les plus efficaces d'obtenir de l'information.

Les guerres de décolonisation, entre usage classique et inflexions opératoires

Parmi les conflits physiques de la Guerre froide, beaucoup concernent les guerres de décolonisation[168]. En effet, la Guerre froide ne signe pas la fin des conflits cinétiques traditionnels : elle marque un virage vers des formes de guerre plus hybrides, mais ne supprime pas instantanément celles dites classiques. Dans ces conflits cinétiques, le spectre électromagnétique a bien sûr continué d'être indispensable, sans pour autant stagner dans ses usages. « Ponctuellement, des engagements militaires nécessitent de recouvrer l'ensemble des capacités de combats sur les réseaux qui prend le nom de GE dans les années 1960[169]. » Dans ce contexte, les cas de la France et de la Grande-Bretagne[170], décrits de manière historique par Aymeric Bonnemaison et Stéphane Dossé[171], permettront d'étayer la place de la GE et surtout, son adaptation quelques années après la fin du second conflit mondial.

En Algérie, la France déploie à partir de 1954 un dispositif d'interception et de radiogoniométrie d'une ampleur inédite. Il est le fruit d'une coordination interservices poussée entre les armées, le SDECE, la DST et le STR[172]. Si ce dispositif s'appuie techniquement sur des compétences développées pendant la Seconde Guerre mondiale, il innove sur le plan organisationnel : c'est la première fois qu'un réseau de GE intègre aussi systématiquement les structures civiles et militaires, et assure une continuité fluide entre interception, traitement et exploitation des données. Cette structuration reflète aussi une nouvelle manière de conduire les opérations dans un contexte de guerre asymétrique et de dissymétrie technologique. En effet, le théâtre algérien oppose une armée française régulière, qui dispose d'un appareil industriel et technologique avancé, à une guérilla mobile et déterritorialisée, qui opère avec grande maîtrise dans des zones montagneuses ou désertiques à faible densité. Dans ce contexte, le spectre électromagnétique devient un outil indispensable de localisation, de cartographie et de ciblage. Étant donné que le rapport de force direct n'est pas toujours exploitable, avec des risques d'accusations d'exactions, de

[168] George F. Kennan, "Cold War and Decolonization, 1945-1961", in Michael D. Richards and Paul R. Waibel, *Twentieth Century Europe: A Brief History, 1900 to the Present*, Oxford : Wiley Blackwell, 2014, p.207-229.
[169] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 49.
[170] Michael Graham Fry, "Decolonization", in *The International Politics of Eurasia: The End of Empire? Comparative perspectives on the Soviet Collapse*, Londres : Routledge, 1997, p. 34.
[171] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 49-52.
[172] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 50.

pertes civiles ou d'échecs opérationnels coûteux, l'interception des communications et la géolocalisation des émetteurs deviennent des vecteurs privilégiés d'engagement. L'enjeu n'est plus uniquement de détruire, mais de préciser où frapper et quand. Ce processus de structuration connaît un tournant décisif en 1956, avec une montée en puissance significative des moyens militaires[173]. Jusque-là, les capacités techniques, bien que coordonnées, restaient encore limitées en volume et en répartition territoriale. À partir de cette date, l'armée de Terre implante deux sections de GE en Oranie, le STR élargit son réseau de stations d'interception, et l'armée de l'Air se dote de moyens aéroportés dédiés. Cette structuration systémique des capacités d'écoute traduit une prise de conscience stratégique à l'époque : dans une guerre où la mobilité ennemie empêche les frappes conventionnelles, la maîtrise du spectre permet une surveillance constante, adaptable et difficilement détectable. Ce basculement marque de fait l'entrée dans une logique de ROEM réactif, pleinement intégré à la manœuvre contre-insurrectionnelle. L'un des exemples les plus révélateurs de cette intégration est l'initiative du général Challe en 1959[174], qui ordonne la cartographie des émetteurs hautes fréquences des différentes wilayas[175] de l'Armée de libération nationale afin de planifier leur neutralisation. Ce travail de renseignement électromagnétique permet de visualiser les réseaux de commandement de la guérilla algérienne, en reliant les transmissions à leurs localisations physiques, et donc à des cibles humaines et logistiques. La GE incarne alors un outil pré-opérationnel, qui agit en amont des frappes, à la fois dans le ciblage et dans le renseignement stratégique. Elle permet, en d'autres termes, de transformer l'invisible en visible.

> *Il ressort de la guerre d'Algérie que les opérations de guerre électronique les plus réussies sont celles qui combinent, en interarmées et avec les services de renseignement, les moyens d'écoute et de localisation, en appui de la manœuvre aéroterrestre (Plan Challe). En terrain désertique ou montagneux, faiblement denses en population, ces moyens se sont révélés redoutables pour les cibles ennemies à haute valeur ajoutée comme les chefs de Wilayas[176].*

Ce rôle central du ROEM dans les conflits cinétiques de la guerre froide se retrouve également dans la guerre des Malouines. Ici aussi, l'appui électronique britannique s'inscrit

[173] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 50.
[174] Maurice Faivre, *Le plan Challe*, Paris : Revue Historique des Armées, n° 238, 2005, p. 108-117.
[175] Les « wilayas » sont les divisions politico-militaires de l'Armée de libération nationale (ALN) durant la guerre d'Algérie. Le territoire algérien était structuré en six wilayas principales, chacune correspondant à une zone géographique et disposant de sa propre organisation militaire.
[176] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 51.

dans une logique interarmées. En avril 1982, l'Argentine déclenche l'opération Azul[177], une invasion éclair de l'archipel britannique des Falklands, les Malouines. Mal préparés à une telle agression, les Britanniques sont initialement pris de court. Le GCHQ, service de renseignement électronique du Royaume-Uni, ne détecte la préparation de l'opération que tardivement, par l'interception d'échanges radio entre les navires argentins, comme ceux du Santa Fe ou du Santísima Trinidad. Cette relative surprise stratégique met en avant une faiblesse d'anticipation dans le spectre global, mais aussi un sous-investissement britannique dans le renseignement sur la zone Amérique du Sud, confiée principalement aux États-Unis dans le cadre de l'accord UKUSA[178]. Si l'absence d'anticipation stratégique a initialement désavantagé Londres, le déclenchement de l'offensive le 2 avril marque un tournant, dans lequel la GE sert d'appui tactique décisif pour regagner l'avantage sur le terrain. Une unité spécialisée est embarquée sur le HMS[179] Intrepid afin d'assurer un appui électronique tactique permanent. Cette unité parvient à intercepter des messages sur les mouvements logistiques argentins, les rotations d'hélicoptères, et surtout les transmissions entre les unités terrestres. L'analyse de ces signaux permet d'identifier l'ordre de bataille adverse, de localiser les défenses installées autour de Port Stanley, et d'adapter la manœuvre amphibie en conséquence. Dans un environnement insulaire, éloigné de tout soutien terrestre, cette capacité d'écoute embarquée permet aux Britanniques de restaurer leur supériorité décisionnelle et d'agir avec une précision largement supérieure à celle de l'adversaire[180]. Au-delà de ses performances techniques, la GE dans les Malouines illustre une autre forme de transformation : elle s'intègre non seulement à la manœuvre interarmées, mais devient condition de possibilité d'une opération expéditionnaire dans un théâtre mal couvert par les services de renseignement traditionnels. Autrement dit, c'est la GE qui compense le déficit initial de connaissance stratégique, et qui permet, par l'interception en temps réel, de reconstruire un cadre décisionnel dans un contexte dégradé. Selon les auteurs de *Attention : Cyber !*, « Dans cette campagne l'appui électronique au contact, encore une fois, montre tout son apport à la manœuvre interarmées[181]. »

---

[177] Stephen Badsey, *An overview of the Falklands War: politics, strategy and operations*, Tokyo : National Institute of Defense Studies (NIDS), 2011, p. 161.
[178] Archive de la NSA, *Amendment no. 4 to the Appendices to the UKUSA Agreement (third edition)*, Maryland : National Security Agency, 1955.Certaines archives concernant l'accord UKUSA sont disponibles sur le site de la NSA, dans le fichier UKUSA Agreement Release (https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/UKUSA/smdpage14704/4/)
[179] HMS, *Her/His Majesty's Ship*, est le préfixe de navire utilisé dans la Royal Navy britannique.
[180] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 52.
[181] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 52.

L'étude de ces conflits de décolonisation confirme la persistance de la GE comme outil tactique intégré aux opérations cinétiques. Son usage y demeure central pour perturber, désorganiser ou masquer, et confirme une continuité dans sa fonction de soutien aux forces conventionnelles. Ces conflits révèlent aussi un changement de nature plus subtil mais fondamental : l'objectif ne se limite plus à neutraliser les communications ennemies ou à protéger les siennes, il s'étend désormais à la captation et l'analyse active des émissions adverses. Cette évolution introduit une nouvelle logique : celle d'une exploitation du spectre électromagnétique non seulement comme champ d'action tactique, mais aussi comme espace de collecte structurée et permanente de données. Si les écoutes étaient déjà pratiquées durant les grands conflits mondiaux, elles sont ici plus systématiques, et surtout, orientées vers une exploitation stratégique à long terme. Autrement dit, le brouillage ne se contente plus d'appuyer la manœuvre, mais il s'articule à une captation, un archivage et un traitement des signaux, qui incarnent en quelques sortes les prémices d'un travail de renseignement à grande échelle. Ce glissement annonce l'intensification, mais surtout, l'institutionnalisation du ROEM comme champ autonome, avec ses méthodes, ses technologies, et ses propres institutions.

Bipolarité et contournement de l'affrontement réel : l'institutionnalisation de l'interception

Dans ce contexte de bipolarité internationale, entre bloc communiste et bloc libéral, les conflits cinétiques persistent mais ne sont plus les seules sources de tensions réelles. Par des actions indirectes, des jeux d'alliances et des oppositions, y compris dans d'autres domaines que le militaire, les deux blocs font valoir leur puissance par une rivalité devenue plus hybride, non-conventionnelle. Cette ère de la conflictualité globale et non-traditionnelle voit naturellement émerger de nouveaux vecteurs pour l'obtention d'avantages stratégiques, notamment par le spectre électromagnétique.

> *Après la Seconde Guerre mondiale, les vainqueurs réorganisent leurs services dans l'optique de la guerre froide […]. La multiplication des conflits et le développement des télécommunications impliquent une explosion des besoins en renseignement d'origine électromagnétique et en écoutes internationales*[182].

[182] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 48.

Le spectre électromagnétique véhicule une course à la domination informationnelle, dans laquelle les États-Unis et l'URSS, entre autres, innovent à vitesse grand V. La création de la NSA américaine en 1952, et du KGB soviétique en 1954, ne sont pas de simples réorganisations bureaucratiques : elles incarnent l'entrée dans une ère où le renseignement devient hautement prioritaire, et doté de moyens techniques, humains et juridiques sans précédent. Mais cette dynamique ne concerne pas uniquement les deux superpuissances.

> *La plupart des pays ayant des visées géostratégiques développent des capacités d'interception : les États-Unis, bien sûr, avec le service longtemps le plus secret et aujourd'hui le plus cité, la NSA, et le Royaume-Uni, avec le GCHQ, qui figurent parmi les plus célèbres. Mais comptent aussi parmi les plus actifs et performants les services dédiés en Russie, en Chine avec les 3e et 4e départements de l'état-major général de l'Armée populaire de libération, ou encore Israël avec l'unité 8200*[183].

Ce mouvement d'institutionnalisation du ROEM est accompagné d'un usage de plus en plus systématique des principes issus de la pensée cybernétique, au sens que lui donne Norbert Wiener[184] dans les années 1940 : une science des systèmes autorégulés fondée sur les boucles de rétroaction, la transmission de l'information et le contrôle à distance. Sans être encore « cyber » au sens contemporain, ces premières architectures de surveillance s'ancrent dans une logique de traitement, de décodage et de circulation de l'information qui préfigure l'infrastructure cognitive de la GE moderne. Dans le domaine militaire, ces principes se traduisent par l'idée que l'efficacité d'un système, par exemple un poste de commandement ou un réseau de défense aérienne, dépend de sa capacité à capter des signaux, à les interpréter rapidement, et à ajuster son action en fonction de ces retours. L'interception électromagnétique devient ainsi un élément crucial non seulement pour obtenir de l'information, mais aussi pour comprendre et perturber les boucles de décision adverses. C'est le cas du dispositif mis en place par la NSA pour surveiller les communications soviétiques à partir des stations d'écoute de Menwith Hill, au Royaume-Uni, ou de Bad Aibling, en République Fédérale d'Allemagne par exemple[185]. Ces réseaux américains de surveillance et d'interception des communications, y compris civiles, étaient nommés ECHELON[186], et désignaient l'ensemble des installations liées au ROEM

[183] Olivier Brun, « ROEM », in Hugues Moutouh et Jérôme Poirot, *Dictionnaire du renseignement*, Paris : Perrin, 2018, p. 658-661.
[184] Jacques Ellul, « Wiener (Norbert) - Cybernétique et société. Traduit de l'anglais », *Revue française de science politique*, n°1, 1955, p. 171-172.
[185] Jean-Yves Duval, « La NSA et le réseau ÉCHELON », *Diplomatie*, n° 5, 2003, p. 51-54.
[186] Steve Wright, *An Appraisal of Technologies of Political Control: Interim Study,* Luxembourg : European Parliament, 1998. Scientific and technological options assessment, p. 19-20.

exploitées par les États-Unis et les États membres du traité UKUSA. En interceptant les échanges entre postes de commandement soviétiques ou les télégrammes diplomatiques chiffrés, la NSA collectait de l'information brute, et alimentait dans le même temps un système d'analyse en temps quasi réel, destiné à anticiper les mouvements de l'adversaire, ajuster les contre-mesures, voire brouiller la chaîne décisionnelle ennemie.

> *De nombreuses stations d'écoutes furent ainsi installées par les protagonistes en des lieux jugés stratégiques, tels que l'Allemagne ou le Canada, tandis que des plateformes aéronautiques et maritimes furent équipées de systèmes d'écoutes, de localisation ou de brouillage*[187].

À cette époque, les institutions de renseignement s'insèrent dans une géopolitique du contrôle informationnel. Loin d'être de simples instruments défensifs, elles participent à une logique offensive de quadrillage du spectre électromagnétique. L'image d'un traité de Tordesillas informationnel, suggéré par Aymeric Bonnemaison et Stéphane Dossé[188], dans lequel les grandes puissances tenteraient de se partager l'invisible, est très éclairante. Alors que le traité de Tordesillas divisait le monde entre l'Espagne et le Portugal en 1494, l'accord UKUSA[189] de 1946 divise lui les zones d'interception globale du spectre électromagnétique. Cet accord témoigne d'une volonté de délimiter des zones d'écoute, d'assigner des priorités cibles et de cartographier les canaux de communication adverses. Cette cartographie invisible redouble, dans le spectre, les frontières mouvantes de l'influence géopolitique. Il s'agit d'un pouvoir de surveillance généralisé avec l'écoute des communications diplomatiques, mais aussi celle des transmissions économiques ou scientifiques. Dans les années 1970, « les opérateurs de l'agence américaine de renseignements techniques affichaient ce mot d'ordre : "En Dieu nous croyons, tous les autres nous écoutons"[190] ». De son côté, l'URSS avait mis en place une « doctrine cybernétique[191] », toujours dans le sens de la théorie du contrôle et de la communication dans les systèmes de Weiner. L'appellation « doctrine cybernétique » faisait ainsi référence non pas au « cyber » au sens de cybersécurité ou d'attaque informatique, mais plutôt à une doctrine d'optimisation du système soviétique par le traitement de l'information et l'automatisation.

---

[187] Éric Gomez, « Focus 2. La guerre électronique », *op. cit.*, p.81.
[188] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 53.
[189] Archive de la NSA, "Amendment no. 4 to the Appendices to the UKUSA Agreement (third edition)", *op.cit.*, 1995.
[190] Olivier Terrien, *Les 36 stratagèmes de la guerre électronique*, Paris : JePublie, 2012, p. 72.
[191] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 54.

Les premières décennies de la Guerre froide sont donc synonymes d'un renseignement à partir du spectre électromagnétique, plus abouti que lors des conflits mondiaux. Toutefois, les années 1970 marquent une inflexion décisive dans cette trajectoire. L'informatisation progressive des outils d'interception transforme en profondeur les pratiques du renseignement. La NSA, tout en conservant son ancrage dans le spectre électromagnétique, entre dans l'ère du traitement massif des données. Ce basculement s'opère dans un contexte de compétition technologique qui engendre des disparités entre les puissances : tandis que les États-Unis investissent massivement dans les supercalculateurs, comme CRAY, les communications numériques, notamment avec les recherches autour du réseau d'Arpanet, et bientôt les ordinateurs personnels, l'URSS peine à suivre, piégée dans ce que certains contemporains désignent comme un « computer gap[192] ». À cette date, il ne s'agit pas encore du « cyberespace » au sens actuel du terme, mais il est toutefois possible de constater l'émergence de formes primitives de guerre informationnelle : capacité à stocker, croiser, corréler, automatiser des masses de données interceptées.

2.1.2. Le virage de la guerre électronique vers le traitement intensif de l'information : convergence des objectifs avec le cyber

À l'instar des efforts menés pendant les conflits mondiaux, la recherche en GE continue de battre son plein lors de la Guerre froide. Pierre Baratault, ancien de chez Thomson-CSF, l'actuel Thalès, et expert de la GE, écrit :

> *Bien entendu, dans les exemples cités, la guerre électronique n'a pas été le seul moteur conduisant au progrès. Mais elle a été le plus souvent le fer de lance dans ces domaines et l'on peut, sans exagération, lui attribuer une bonne partie des retombées des actions qui y ont été conduites[193].*

L'importance revêtue par le spectre électromagnétique dans le cadre du renseignement est une raison évidente de la quantité de recherche menée ces années. Mais les efforts ne se sont pas concentrés uniquement sur les manières de collecter le renseignement à partir des services secrets, discutés précédemment. Ces recherches ont continué de développer les technologies embarquées :

[192] Aymeric Bonnemaison et Stéphane Dossé, *ibid.*, p. 51.
[193] Pierre Baratault, « La recherche en guerre électronique et ses retombées depuis 1960 », *op.cit.*, 2002, p. 110.

De nouvelles technologies furent également développées dans ce sens, comme l'illustrent l'utilisation de la réflexion électromagnétique sur la Lune pour détecter les radars soviétiques, les vols d'avions U2 au-dessus du territoire soviétique dans les années 1950 ou le développement de satellites de communication et d'écoutes électromagnétiques à partir des années 1960[194].

Ces années de recherches, impulsées par la pression d'un contexte international de méfiance entre les deux blocs, n'ont cessé de démultiplier le spectre des effets pouvant être produits par la GE. À tel point que, dans les années 1970, ces nouvelles technologies présentent une spécificité inédite dans la combinaison des moyens qu'elles regroupent, notamment pour répondre au besoin urgent de traitement massif et rapide des données collectées, afin de les exploiter[195]. À cet égard, l'entretien conduit avec Pierre Baratault a permis d'illustrer ce point avec le cas de l'avion de renseignement électronique français Douglas DC-8 Sarigue.

Dans les airs, et encore plus dans l'espace, on capte un très très grand nombre de signaux, qui forme des flux de données tout à fait impressionnants. Il faut savoir reconnaitre dans ces signaux ceux qui peuvent être intéressants, à la fois pour bien connaître les caractéristiques techniques des radars d'un adversaire, mais aussi pour les localiser, savoir où ils se situent et comment ils se déplacent, communiquent entre eux. Pour cela, jusque dans les années 1970, c'étaient surtout des opérateurs qui, sur un oscilloscope, examinaient les signaux, faisaient du tri. […] La goniométrie […] suppose tout un traitement de données qui, quand on a un radar tout seul, n'est pas très compliqué, mais quand on a un certain nombre de radars avec des caractéristiques voisines qui se mélangent, devient un bon casse-tête[196].

Ce programme a constitué un tournant : le DC-8 Sarigue comptait de nombreux récepteurs et une équipe d'une quinzaine d'opérateurs chargés de capter en vol un large éventail de signaux radar. Sa mission principale était le SIGINT[197], ou *signal intelligence*, la traduction anglaise du ROEM, qui regroupe deux branches. L'ELINT, ou *Electronic intelligence*, consiste en du renseignement technique d'origine électromagnétique, à partir des émissions non communicantes. Elle permet de caractériser avec précision ce qui est physiquement émis par un émetteur, et peut donc servir à localiser un radar par exemple. La deuxième branche, COMINT, ou *Communication Intelligence*, analyse, elle, les contenus des renseignements issus de l'interception de télécommunications. Les opérateurs à bord

[194] Éric Gomez, « Focus 2. La guerre électronique », *op. cit.*, p.81.
[195] Victor Bréhat Chapuis, « Aéronautique – L'informatique dans l'Armée de l'air – Coupes et congrès dans l'aéronautique militaire – Le Xe Salon de Hanovre », *Revue Défense Nationale*, n° 335, 1974, p. 162-168.
[196] Entretien avec M. Pierre Baratault.
[197] AviationsMilitaires.net, « Douglas DC-8 SARIGuE » (https://aviationsmilitaires.net/v3/kb/aircraft/show/12508/douglas-dc-8-sarigue).

sont divisés en deux équipes, l'une chargée de l'ELINT et l'autre du COMINT[198]. Contrairement aux générations précédentes, cet aéronef, étant donné qu'il est doté d'un système d'enregistrement numérique, permettait une capitalisation et un traitement différé des signaux interceptés. Ce changement méthodologique est fondamental : jusque dans les années 1970, c'étaient les opérateurs qui, face à des oscilloscopes, examinaient et triaient manuellement les signaux jugés pertinents[199]. L'arrivée de l'informatique à bord a permis non seulement d'enregistrer numériquement l'ensemble des signaux captés, mais aussi d'assister les opérateurs dans le traitement de ces données. Avec le Sarigue, l'objectif n'était plus seulement de collecter, mais aussi de hiérarchiser, recouper et localiser les sources d'émission à partir de calculs goniométriques automatisés.

> *L'informatique grâce à sa puissance de calcul a permis d'obtenir ce résultat [exploiter rapidement les informations]. Patricia [...], comprend un nombre élevé de capteurs de divers types à bord de l'avion qui, de la caméra aux radars, permettent à l'appareil volant à basse altitude de couvrir une zone allant jusqu'à 6 x 30 kilomètres autour de sa trajectoire. Au sol, des consoles reliées à l'ordinateur permettent l'examen comparatif des informations accumulées pendant le vol, une sélection plus rapide des résultats et la constitution des dossiers d'objectifs. Dans le cadre de la guerre électronique, le système Sarigue [...] fonctionnera suivant un principe analogue*[200].

Dès lors, la GE ne peut plus être pensée sans une composante d'analyse de l'information, ce qui ouvre la voie à une hybridation progressive avec les logiques computationnelles. L'intérêt de cet exemple réside dans sa portée méthodologique : le Sarigue réunit, à bord d'une même plateforme, la capacité de capter et celle de traiter de manière numérique des signaux issus de l'environnement électromagnétique. Cela préfigure, en quelques sortes, une forme de convergence fonctionnelle entre GE et pratiques informatiques. Loin d'être fusionnés à cette époque, les deux domaines restent distincts : la GE relève encore d'une logique majoritairement militaire et technique, tandis que l'informatique, puis le cyber, s'imposent, plus tard, comme une sphère à part entière, avec ses propres doctrines et outils. Cependant, la montée en puissance du traitement automatique des signaux, à travers des dispositifs comme le DC-8 Sarigue, pose les jalons d'un futur rapprochement. La capacité à exploiter l'information en temps court, à la filtrer, la localiser et la modéliser, devient un enjeu aussi central que sa collecte. Par la suite, à mesure que les

[198] Entretien avec M. Pierre Baratault.
[199] Entretien avec M. Pierre Baratault.
[200] Victor Bréhat Chapuis, « Aéronautique – L'informatique dans l'Armée de l'air – Coupes et congrès dans l'aéronautique militaire – Le Xe Salon de Hanovre », *op.cit.*, 1974, p. 164.

technologies ont évolué, les logiques d'optimisation du traitement et de la circulation de l'information, qui sont en soi les caractéristiques du cyber, ont commencé à rencontrer celles de la GE, sans que les frontières ne soient pour autant immédiatement supprimées.

Après des décennies de recherches continues dans le domaine électronique, les efforts spécifiquement centrés sur la GE ont connu un certain essoufflement dans les années 1990[201]. Il est intéressant de noter que cette période coïncide avec l'émergence des travaux sur les « Révolutions dans les affaires militaires » (RAM), notamment dans les milieux stratégiques américains. Ces réflexions sont nourries par la montée en puissance des technologies de l'information et des systèmes interconnectés[202]. Dès le début des années 1990, des auteurs comme Andrew Marshall, alors directeur du très influent Office of Net Assessment[203], encouragent une lecture transformationnelle des conflits, en insistant sur l'impact des technologies de l'information sur la structure et la dynamique des forces armées[204]. En l'occurrence, ces auteurs s'interrogent sur l'impact que pourrait avoir la combinaison de l'informatique et des réseaux de télécommunication. L'idée centrale qui traverse ces travaux est que l'accumulation de changements technologiques peut provoquer un basculement profond dans la manière de concevoir et conduire la guerre, soit, une *Revolution in Military Affairs*[205]. Des concepts comme celui de « network-centric warfare[206] », structurent cette pensée : la guerre devient une affaire de flux informationnels, de capteurs distribués et d'effets synchronisés à distance. Cette grille d'analyse fait entrée, de manière diffuse, le cyber dans la pensée stratégique. Sans être encore pleinement théorisé comme un domaine autonome, il apparaît en creux dans les travaux. L'une des révolutions mises en avant dans les RAM est bien celle de l'informatisation croissante de l'appareil militaire, et donc, en filigrane, du rôle stratégique de l'espace numérique. Le chevauchement chronologique entre le ralentissement des recherches en GE et la montée en puissance des travaux sur les RAM, en particulier ceux intégrant les dimensions liées aux technologies de l'information, peut susciter l'hypothèse d'un déplacement de l'intérêt stratégique. En effet,

[201] Pierre Baratault, « La recherche en guerre électronique et ses retombées depuis 1960 », *op.cit.*, 2002, p. 115.
[202] Barry D. Watts, "The maturing Revolution in Military Affairs", *Center for Strategic and Budgetary Assessments*, 2011, p.2.
[203] Ancien office fédéral américain au sein du département de la Défense, servant de laboratoire d'idées interne pour planifier des stratégies à long terme. Projection de 20 à 30 ans dans le futur, d'un point de vue militaire.
[204] Andrew W. Marshall, "Some thoughts on Military Revolutions – Second version", *Office of the Net assessment*, Memorandum for the record, 1993, p. 3.
[205] Williamson Murray, "Thinking About Revolutions in Military Affairs", *Joint Forces Quarterly*, n° 16, 1997, p. 69-76.
[206] Arthur K. Cebrowski and John H. Garstka, "Network-Centric Warfare: Its Origin and Future", *US Naval Institute Proceedings*, 1998.

à mesure que les réflexions se structurent autour de concepts comme la guerre réseau-centrée, il peut sembler que les priorités militaires se tournent vers les réseaux et le traitement numérique de l'information, donc vers le cyberespace, délaissant progressivement les approches plus classiques du spectre électromagnétique. Toutefois, ce constat repose sur une comparaison déséquilibrée. Les travaux sur les RAM proviennent pour une grande majorité du champ académique, alors que les recherches sur la GE, tout comme celles sur le cyber appliqué au champ militaire, relèvent d'un tout autre espace : celui de la sphère technico-opérationnelle, militaire, plus cloisonnée, mais où les dynamiques de recherche ne se sont en réalité jamais interrompues[207]. Autrement dit, si l'on se limite à une lecture académique des priorités stratégiques, l'hypothèse d'un « remplacement progressif » de la GE par le cyber peut apparaître fondée : dans les années 1990, les travaux concernent de plus en plus les thématiques cyber et leur avenir, et la GE devient moins prisée. Mais replacée dans la logique propre au monde militaire, cette hypothèse perd de sa pertinence. Les entretiens menés avec M. Pierre Baratault et Jean-François Grandin ont précisément permis d'infirmer cette lecture : le ralentissement relatif de la visibilité de la GE ne découle pas de l'essor du cyber, et encore moins d'un effet de substitution. À la question portant sur l'effet du cyber sur le ralentissement des recherches en GE, M. Pierre Baratault répond avec certitude : « Non, je crois que c'était complètement disjoint à cette époque-là. On ne parlait que très peu de cyber à ce moment-là[208]. » Aymeric Bonnemaison et Stéphane Dossé semblent d'ailleurs accordés avec ce refus d'attribuer au cyber une influence démesurée sur la GE : « L'émergence des télécommunications [par le spectre électromagnétique] a représenté une révolution dans l'art de la guerre, le cyber actuel ne constituant qu'une évolution[209]. »

En somme, la GE a évolué sous l'effet conjugué de la mutation de la conflictualité et des avancées technologiques. Des conflits cinétiques de décolonisation aux affrontements plus diffus de la guerre froide, elle s'est adaptée à des contextes de plus en plus complexes, glissant progressivement vers ses fonctions plus discrètes, le renseignement. Parallèlement, le développement de capacités de collecte et de traitement automatisé des données a amorcé une convergence fonctionnelle avec certaines logiques issues du cyber. À ce stade, une forme de glissement analogique a pu se dessiner : les objectifs se rapprochent, les outils se croisent, les domaines dialoguent. Mais cette convergence, encore partielle, ne saurait être interprétée

[207] Entretien avec M. Pierre Baratault.
[208] Entretien avec M. Pierre Baratault.
[209] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 69.

comme une substitution du cyber à la GE, ou une absorption de la GE par le cyber. Pour comprendre l'ensemble de la dynamique à l'œuvre, et les raisons du ralentissement des recherches en GE à partir des années 1990, il faut désormais explorer d'autres facteurs.

2.2. Une guerre électronique post-guerre froide en sourdine : recompositions budgétaires et institutionnelles

Les mutations des formes de conflictualité et les évolutions technologiques ont largement participé à redéfinir les usages de la GE dans les dernières décennies du XX^{e} siècle. Néanmoins, elles ne suffisent pas à rendre compte du ralentissement observé dans les recherches à partir des années 1990. Les entretiens menés avec plusieurs praticiens du domaine invitent à déplacer l'analyse, et à identifier deux dynamiques post-guerre froide, plus structurelles : d'une part, l'effet concret des coupes budgétaires sur la recherche et le développement dans la sphère miliaire ; d'autre part, les réorganisations institutionnelles qui, sous contrainte, ont favorisé un rapprochement pragmatique entre les dispositifs de GE et les capacités cyber, encore émergentes à l'époque. Ces deux dimensions, largement sous-explorées dans la littérature, permettent de rétablir leurs véritables trajectoires pour remonter aux racines de la convergence et de l'articulation entre GE et cyber.

2.2.1. Les « dividendes de la paix » : la contrainte budgétaire comme principal frein à la recherche en guerre électronique

À la fin des années 1980, l'émergence de l'outil cyber et la multiplication des recherches faites sur ses usages en temps de guerre ont créé une dynamique d'intérêt cyber. Dans le même temps, le développement de la GE a semblé s'essouffler. La GE faisait pourtant l'objet d'innovations techniques, matérielles, industrielles, régulières et convoitées par la sphère militaire. De fait, la déduction selon laquelle le cyber aurait pris le pas sur la GE pouvait être plausible. Toutefois, les échanges menés avec les praticiens ont permis d'obtenir une explication moins évidente et plus pragmatique. À la question : « le cyber a-t-il eu un impact sur la diminution des recherches en GE dans les années 1990 ? », la réponse de Pierre Baratault a été très claire.

Non, je crois que c'était complètement disjoint à cette époque-là. On ne parlait que très peu de cyber à ce moment-là. Et la raison, elle était budgétaire. […] Une fois que la guerre froide s'est arrêtée, ça a été l'expression fameuse des "dividendes de la paix". Sur la question des investissements, on a considéré qu'il n'y avait plus de risque du côté soviétique. Donc ça ne valait plus la peine de mettre beaucoup d'argent pour recueillir du renseignement, ni pour mieux connaître les dispositifs d'un adversaire, puisque l'adversaire, on ne l'avait plus[210].

L'un des principaux facteurs de la fin de l'élan des recherches en GE est donc lié aux dividendes de la paix[211]. Cette expression, qui recouvre la période des années 1990, désigne la sorte de parenthèse budgétaire inédite dans l'histoire récente des politiques de défense, jusqu'au début des années 2000. L'effondrement du bloc soviétique, entre 1989 et 1991, entraîne la disparition soudaine du communisme et d'une menace militaire clairement identifiée par les démocraties libérales, qui avaient jusqu'alors justifié un haut niveau de dépenses. Dans un contexte de déficits publics croissants, les gouvernements occidentaux, mais surtout européens, saisissent cette occasion pour réévaluer certaines priorités budgétaires[212]. La défense apparaît alors comme un poste de dépense sur lequel des économies peuvent être réalisées sans coût politique immédiat. Selon Charles Million, ministre français de la Défense sous Jacques Chirac de 1995 à 1997, les gouvernements ont fait des budgets de la défense de véritables « variables d'ajustement du point de vue budgétaire[213]. » Cette dynamique s'accompagne d'une reconfiguration doctrinale : la probabilité d'un conflit conventionnel de haute intensité semble s'éloigner, et avec elle, le besoin de maintenir certains dispositifs hérités de la logique de bipolarité[214]. Les forces armées sont donc amenées à se transformer, à opérer dans des environnements perçus comme plus diffus, moins massifs, moins symétriques. Les dividendes de la paix sont portés par la croyance en la fin de l'histoire[215], la paix durable, la stabilisation du système international,

[210] Entretien avec M. Pierre Baratault.
[211] Malcolm Knight, Norman Loayza and Delano Villanueva, "The Peace Dividend: Military Spending Cuts and Economic Growth", *IMF Economic Review*, vol. 43, 1996, p. 1-37.
[212] Jean-Marc Daniel, « Finances publiques : les dividendes de la paix ? », *Observations et diagnostiques économiques (Observatoire français des conjonctures économiques)*, n° 47, 1993, p. 91.
[213] Jean-Baptiste Noé, « Qui va toucher les dividendes de la paix ? Entretien Charles Million », *Revue Conflits*, 2 mai 2023 (https://www.revueconflits.com/qui-va-toucher-les-dividendes-de-la-paix-entretien-charles-millon/).
[214] Julien Malizard, « Le financement des armées au sortir de la guerre du Golfe et de la guerre froide », *Revue Défense Nationale*, n° 843, 2021, p. 26.
[215] La « fin de l'histoire » est théorisée par F. Fukuyama en 1992 : à la succession de la crainte d'une guerre mondiale succède l'euphorie de la victoire des démocraties libérales sur toutes les autres formes de régimes politiques ou d'idéologies. C'est la « fin de l'histoire » des autres formes de régimes politiques.

et en ce sens, ils justifient la baisse des budgets militaires. Dans un entretien pour la revue Conflits, Charles Millon explique :

> *Les années 1990 ont été marquées par la fin de la guerre froide ainsi que par la montée de l'illusion pacifiste. Cette pensée pacifiste a permis à Laurent Fabius de parler de ces fameux "dividendes de la paix" dont devraient bénéficier les pays occidentaux, et qui ont justifié la chute dramatique des budgets de la défense qui rappelons ont baissé de 25% en 30 ans*[216].

Cette chute des budgets a de fait entraîné une redéfinition des priorités capacitaires, une rétraction des programmes de recherche associés à certains domaines, au premier rang desquels, la GE. En effet, la recherche d'un développement durable et d'une stabilité internationale supposait plusieurs contrôles et restrictions sur la production des armes, la recherche et le développement militaire, et les produits à utilisations duales, civiles et militaires[217]. Ce désarmement budgétaire, fondé avant tout sur la réduction immédiate des crédits de défense, a donc eu pour effet un ralentissement significatif de l'activité scientifique et technique dans les secteurs militaires. Il ne s'agissait pas d'un désengagement idéologique ou d'une réorientation doctrinale assumée, mais bien d'une logique de gestion pragmatique des finances publiques, qui a conduit les pouvoirs publics à établir des priorités strictement budgétaires[218]. Les domaines perçus comme moins urgents, ou dont la valeur opérationnelle ne se manifestait pas directement dans les engagements en cours, ont été les premiers à faire les frais de cette rétraction. La R&D militaire, en particulier dans les secteurs à cycle long et à forte intensité technologique comme la GE, a été directement touchée[219]. Les données du SIPRI confirment d'ailleurs ce recul. Le tableau ci-dessous témoigne de la baisse significative des dépenses allouées à la R&D militaires de 1986 à 1997.

TABLEAU 3 – LES DEPENSES MILITAIRES DE R&D DE 1986 A1997 (EN MILLIONS DE DOLLARS, EN PRIX ET TAUX DE CHANGE FIXE 1995) ET LA PART DES DEPENSES DE R&D MILITAIRES (RDM) DANS LES DEPENSES PUBLIQUES TOTALES CORRESPONDANTES (RDP).

Pays	1986	1989	1992	1995	1997
USA	51 000	51 000	44 000	37 000	38 000
RDM/RDP	0,69	0,65	0,59	0,54	0,54
France	6 200	7 100	6 800	5 200	4 600
RDM/RDP	0,33	0,39	0,34	0,30	0,29
Royaume-Uni	5 400	4 100	3 500	3 300	3 300
RDM/RDP	0,55	0,46	0,44	0,36	0,35
Allemagne	2 300	3 100	2 400	2 000	2 100
RDM/RDP	0,016	0,005	0,002	0,0034	-
Japon	800	1 100	1 400	1 600	1 800
RDM/RDP	-	0,52	0,59	0,62	-
Italie	540	750	600	560	-
RDM/RDP	0,085	0,068	0,07	0,09	-

Source : SIPRI, 1999.

[216] Jean-Baptiste Noé, « Qui va toucher les dividendes de la paix ? Entretien Charles Million », *op.cit*., 2023.
[217] Jacques Fontanel et Sylvie Matelly, « Le coût des dividendes de la paix », *Mondes en Développement*, vol. 28, n° 112, 2000, p. 2.
[218] Jacques Fontanel et Sylvie Matelly, *ibid.*, p. 2.
[219] Jacques Fontanel et Sylvie Matelly, *ibid.*, p. 7.

De nombreux programmes ont été ajournés, réduits, voire abandonnés[220]. Les crédits alloués aux technologies duales, telles que la surveillance, les communications, ou encore le traitement de données, ont été revus à la baisse, freinant ainsi les dynamiques d'innovation qui avaient pourtant connu une forte impulsion durant la guerre froide[221]. La GE, bien qu'elle ait conservé une certaine utilité opérationnelle, a ainsi naturellement perdu de sa centralité stratégique. Non pas parce qu'elle était devenue obsolète, ou parce qu'elle avait été remplacée par l'outil cyber, mais bien parce que, en tant que moyen militaire, elle n'était plus perçue comme prioritaire dans un contexte d'engagements extérieurs limités et de menaces diffuses[222]. Ce déclassement relatif ne résulte donc pas d'un changement de doctrine, d'une remise en cause de son utilité, ou d'un remplacement par le cyberespace, mais d'un ajustement conjoncturel des moyens, guidé par des considérations d'efficacité budgétaire. Cette période des dividendes de la paix aura produit des effets durables[223], en ralentissant l'innovation, en fragmentant les savoir-faire, et en supprimant des dispositifs patiemment construits durant la guerre froide, sans stratégie de remplacement immédiate.

> *Avec la chute du mur de Berlin, il y a eu une espèce d'angélisme qui s'est mise en place. Et là, on a cassé un outil de renseignement électronique qui était extrêmement puissant, mais très tourné vers l'Est, parce qu'on a démantelé progressivement tout un tas d'emprises d'écoute, de radar. Non seulement on les a démantelées, mais en plus, on ne les a pas réorientées ailleurs, ou très peu*[224].

Si les coupes budgétaires ont d'abord affecté le contenu même de la GE, par ses dynamiques internes de recherche et d'innovation, elles ont également eu des répercussions structurelles plus larges. En tant que domaine capacitaire, la GE a été progressivement réorganisée, parfois replacée dans des structures de recherche plus vastes. Ce processus, davantage exogène, relève moins d'une évolution doctrinale que d'une logique de rationalisation institutionnelle.

[220] Christophe David, « Histoire des Lois de programmation militaire (LPM) », *Les Cahiers de la Revue Défense Nationale*, Au(x) défis de la puissance – Regards du CHEM, 72e session, 2023, p. 198.
[221] Pierre Baratault, « La recherche en guerre électronique et ses retombées depuis 1960 », *op.cit.*, 2002, p. 102-115.
[222] Michel Rogalski, « Dépenses militaires et dividendes de la paix », *Revue Défense Nationale*, n° 532, p. 126.
[223] Entretien avec le colonel Éric Gomez.
[224] Entretien avec le colonel Éric Gomez.

2.2.2. Réorganisation institutionnelles et convergence fonctionnelle : quand le cyber croise la guerre électronique

Un certain nombre de travaux académiques s'est intéressé aux restructurations liées à la défense[225], et aux enjeux de transformation[226] qui y sont liés. La réorganisation des armées au lendemain de la Guerre froide est un fait avéré qui a concerné la majorité des États. Toutefois, les études qui abordent ce phénomène se concentrent surtout sur l'aspect économique, et donc sur la réorientation de certaines industries vers des secteurs civils par exemple. L'objectif de ces travaux est plutôt d'étudier les conséquences de ces réorganisations d'un point de vue humain, ou stratégique sur le long terme. Or, la convergence GE -cyber que nous souhaitons analyser est bien plus restreinte, et de fait bien moins discutée. Dans le cas de la France et des États-Unis, les éléments fournis par le colonel Éric Gomez permettent de compenser le manque de ressources sur ce point. Il évoque tout d'abord la notion de « vivier » pour expliquer le facteur structurel de cette convergence, puis il donne l'exemple de l'IMSI-Catcher, entre autres, comme illustration concrète de la continuité cyber-électronique.

Une convergence structurelle portée par un vivier issu de la guerre électronique

À propos des raisons de la convergence entre GE et cyber, le colonel Éric Gomez évoque une raison institutionnelle, avec la notion de vivier. Il utilise cette notion au sens d'un réservoir de compétences et de profils humains déjà présents dans le milieu militaire, pour expliquer la genèse et le développement du cyber militaire en France.

> *Cette structure [cyber], elle n'a pas pu se constituer à partir de rien. Il fallait prendre des gens qui avaient quand même un savoir-faire proche. À l'époque, l'écosystème universitaire était quand même très limité sur le sujet, on avait très peu de fonctionnaires, de militaires, ou même d'ingénieurs compétents dans le domaine. Donc, naturellement, on a puisé dans un vivier le plus proche possible. Et parmi ces viviers, la guerre électronique en faisait grandement partie : il y a des compétences d'ingénieurs, des compréhensions de comment fonctionnent les signaux, les programmations, les appareils, etc. Et donc, même si ce n'est pas similaire, ça s'en rapproche quand même pas mal*[227].

[225] Jean-Pierre Aubert, Frédéric Bruggeman et Jean-Pierre Carli, « Les Restuctuations de défense : Un modèle pour l'industrie ? », *Le Journal de l'École de Paris du management*, vol. 3, n° 65, 2007, p.30-36.
[226] Romain Guillet, « S'adapter sans improviser : les enjeux de transformation organisationnelle », *Revue Défense Nationale*, Hors-série n° 15, 2024, p. 253-267.
[227] Entretien avec le colonel Éric Gomez.

À défaut de spécialistes déjà formés au cyber, l'État a naturellement cherché les profils les plus proches. Or, ceux qui savaient travailler sur les ondes, les signaux, les dispositifs d'écoute, de brouillage, ou de protection des communications, étaient directement issus du domaine de la GE. À titre d'exemple, le colonel Éric Gomez évoque notamment le parcours du général Patrick Justel, mais aussi ceux de Stéphane Dossé et du général Aymeric Bonnemaison, avec qui il a eu l'occasion de travailler. Le premier point commun de ces trois hommes est qu'ils ont été chefs de corps du 54ème régiment de transmission, qui est l'un des régiments de GE de l'armée de terre. Leur deuxième point commun est que lorsque l'armée de terre a intégré le cyber dans ses stratégies, ces spécialistes de la GE se sont retrouvés à occuper des postes haut-placés du domaine cyber[228]. Aujourd'hui, le général Aymeric Bonnemaison exerce des fonctions au sein du ComCyber. Le colonel Éric Gomez évoque une « réalité vraiment sociologique derrière tout ça ». En effet, la proximité technique entre GE et cyber a entraîné une continuité humaine et institutionnelle. Parce que les compétences de la GE étaient les plus proches de ce qu'exigeait le développement du cyber, ce sont les spécialistes de ce domaine qui ont été choisis. Ce choix a créé un noyau d'acteurs familiers aux deux domaines, ce qui a sans doute facilité, par la suite, une compréhension croisée et une articulation plus fluide entre GE et cyber, tant sur le plan opérationnel que stratégique. De fait, les facteurs majeurs de la convergence ont aussi été sociologique et institutionnel. D'ailleurs, le Plan « Armées 2000 », même s'il se concentre principalement sur la redistribution des compétences et la réorganisation territoriale des armées, a aussi pour objectif de « développer la coopération interarmées dans les domaines du soutien, des inspections et de l'enseignement supérieur[229] ». Ce plan, dont la mise en œuvre était prévue entre 1990 et 1991, visait à renforcer la cohérence et la transversalité entre les différentes armées. En favorisant une culture de coopération et la circulation des compétences entre milieux opérationnels, il a contribué à créer un cadre propice aux rapprochements entre les spécialités techniques[230]. C'est dans ce contexte que des dynamiques de convergence comme celle entre GE et cyber ont pu se créer, en s'appuyant sur des profils hybrides et une logique interarmées déjà encouragée à l'échelle structurelle.

[228] Entretien avec le colonel Éric Gomez.
[229] Conseil des ministres 1989, « Plan "Armées 2000" », *Vie publique*, 26 juillet 1989 (https://www.vie-publique.fr/discours/154657-conseil-des-ministres-du-26-juillet-1989-le-plan-armees-2000).
[230] Maurice Faivre, « Défense en France – Le Plan "Armées 2000" », *Revue Défense Nationale*, n° 502, 1989, p. 177-179.

Ce cas concerne, certes, la situation de la France. Toutefois, il est possible d'illustrer la convergence institutionnelle GE-cyber également par le cas des autres puissances de la fin du XX^{e} siècle. Dans le cas des États-Unis, le service qui dirige le cyber n'est rien d'autre que celui chargé des écoutes et de la GE : la NSA[231].

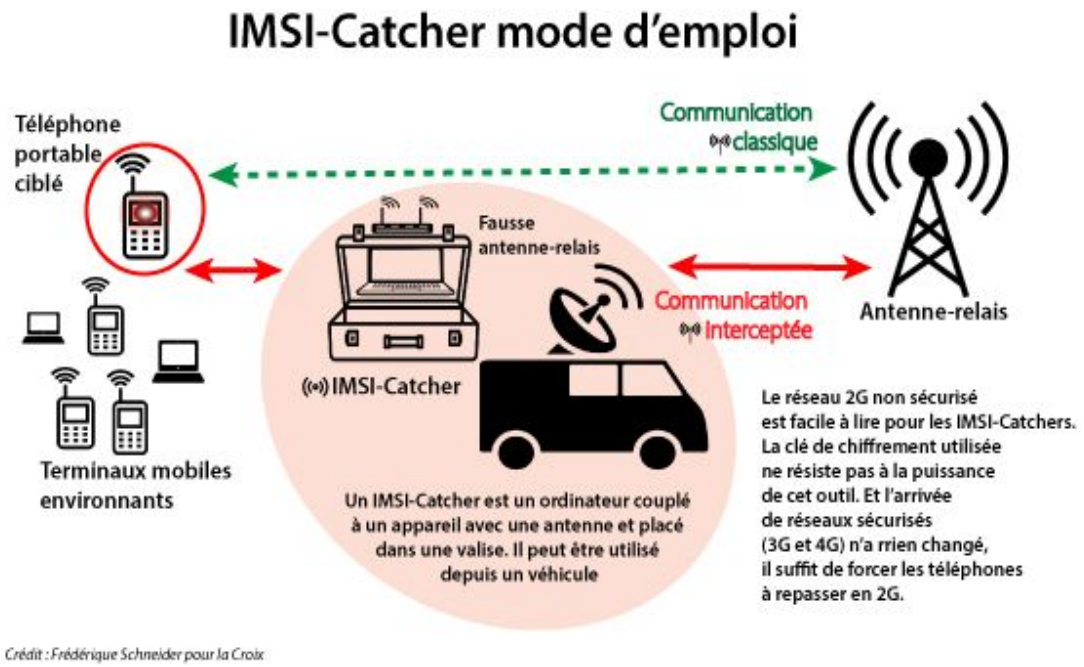
> *Il y a une filiation qui s'est créée dans plusieurs pays. Peut-être aussi parce qu'il y a un peu de mimétisme. On [les autres États] a vu qu'aux États-Unis, ça se constituait par ce canal de la NSA ; et bien souvent, les agences, pour monter une capacité [cyber] comme ça, doivent coopérer au départ. La plupart du temps, une agence, quelle qu'elle soit, n'est pas en mesure de monter cette capacité seule*[232].

Aux débuts du cyber, les agences des différents États ont dû mettre en place un dialogue. Les États-Unis ont monté la capacité cyber via la NSA. De fait, le dialogue qui s'est mis en place ensuite avec les autres agences du monde a concerné les services de renseignement technique des autres États, et donc les services de GE. Ceux-ci ont dû échanger directement avec la NSA, parce qu'ils en avaient les compétences. Ainsi, à l'échelle plus large aussi, le constat du vivier technique et sociologique se confirme. Dans plusieurs pays, la construction des capacités cyber s'est appuyée sur les structures, les compétences et les acteurs issus de la GE. La convergence s'est aussi renforcée par la nécessité de coopérations entre services comparables.

<u>L'apparition du cyber dans des outils de guerre électronique : vers une complémentarité opérationnelle</u>

Après l'intégration du cyber dans les services, la continuité cyber-électronique a commencé à être visible, notamment dans les outils opérationnels. Cette démonstration s'appuie uniquement sur le cas du IMSI-Catcher, et est donc bien sûr loin d'être exhaustive.

[231] Entretien avec le colonel Éric Gomez.
[232] Entretien avec le colonel Éric Gomez.



Source : Frédérique Schneider, « IMSI-Catcher, ou comment les téléphones portables sont écoutés », *La Croix*, 2016.

L'IMSI-Catcher constitue un exemple particulièrement parlant de la manière dont un même dispositif peut produire des effets relevant à la fois de la GE et du champ cyber[233]. Ce dispositif, capable de se faire passer pour une antenne de téléphonie mobile, a pour but de limiter le fonctionnement d'une (vraie) antenne-relais de téléphonie mobile. Le ralentissement du fonctionnement de la vraie antenne, provoqué par l'IMSI-Catcher, pousse donc les téléphones situés à proximité à se connecter à lui[234]. De fait, cette capacité repose sur des techniques de manipulation du spectre électromagnétique, et son usage relève donc de la GE. Initialement, sa fonction était celle de radiogoniométrie, à savoir, la localisation précise des terminaux à partir des émetteurs. Cependant, comme l'explique le colonel Éric Gomez, les usages de l'IMSI-Catcher se sont rapidement étendus. Une deuxième fonction a permis que, une fois connecté à l'appareil ciblé, le boîtier soit une voie d'accès à des informations techniques telles que l'identifiant du terminal, le numéro de carte SIM ou l'historique des connexions[235]. Ces données sont exploitées dans une logique de renseignement technique, et donc à la croisée des fonctions électroniques et numériques. Ensuite, l'outil a permis de servir de vecteur pour des actions offensives de type cyber, par exemple en exploitant cette connexion pour injecter du code malveillant, accéder aux

[233] Entretien avec le colonel Éric Gomez.
[234] Martin Untersinger, « Que sont les IMSI-catchers, ces valises qui espionnent les téléphones portables ? », *Le Monde*, 31 mars 2015 (https://www.lemonde.fr/pixels/article/2015/03/31/que-sont-les-imsi-catchers-ces-valises-qui-espionnent-les-telephones-portables_4605827_4408996.html).
[235] Entretien avec le colonel Éric Gomez.

données internes du téléphone, activer à distance les capteurs tels que le micro, la caméra, voire dans des cas extrêmes, provoquer une dégradation physique de l'appareil[236]. Ainsi, ce cas montre que le spectre électromagnétique peut constituer un point d'entrée vers des effets cyber, sans changement de dispositif technique, en l'occurrence l'IMSI-Catcher, ni discontinuité dans l'action. En effet, l'IMSI-Catcher en lui-même ne change pas de nature, sa structure reste la même, mais le champ d'action qu'il a permis au fil des années s'est élargi, passant d'un usage de GE à des effets cyber complémentaires à ce premier usage. Il illustre ainsi une convergence opératoire : non pas une substitution d'un domaine à l'autre, mais une continuité dans les moyens, qui permet un élargissement du spectre des effets produits.

L'analyse menée dans ce deuxième chapitre confirme que la convergence entre GE et cyberespace ne doit pas être interprétée comme une fusion des deux domaines, ni comme le remplacement de la GE par le cyber. Cette convergence s'est plutôt construite de manière progressive, en réponse à des dynamiques extérieures : mutation de la conflictualité, évolution technologique, contraintes budgétaires post-guerre froide, et réorganisations institutionnelles. C'est moins une convergence doctrinale qu'une convergence de fait : dans un contexte de désescalade militaire, elle a été façonnée par la rationalisation des forces armées à la fin des années 1990, la mutualisation des ressources, la proximité des savoir-faire, et l'illusionnisme d'un ordre international apaisé. Cette convergence, dans un premier temps, a donc été fonctionnelle et structurelle. À mesure qu'elle s'est matérialisée, elle a également trouvé une résonance nouvelle dans certaines pratiques opérationnelles contemporaines. Parmi elles, le développement continu, coordonné et assumé des capacités cyber et de GE par la Russie a montré que certains États avait fait de cette convergence une priorité doctrinale, intégrée aux schémas de pensée opérationnels, aux manœuvres et aux stratégies de puissance. Les épisodes d'agressions russes depuis la fin des années 2000 ont révélé la portée stratégique de cette articulation, qu'il convient désormais d'étudier de manière concrète et empirique dans le dernier chapitre.

[236] Entretien avec le colonel Éric Gomez.

Chapitre 3. La convergence cyber-électronique : observations empiriques à l'Est de l'Europe

L'articulation du spectre électromagnétique et du cyberespace, étudiée précédemment sous des prismes historiques, fonctionnels et organisationnels, n'est pas qu'une observation abstraite et académique. Elle se matérialise aussi et avant tout de façon tangible dans les conflits contemporains. Les effets croisés de ces deux dimensions sont recherchés, coordonnés et intégrés dans les manœuvres militaires. Parmi les puissances ayant fait de cette articulation un levier stratégique, la Russie occupe une place singulière. Depuis la fin des années 2000, l'État russe a progressivement redéfini les modalités de projection de sa puissance, dans un contexte international marqué par l'élargissement de l'OTAN[237], la perte d'influence dans son étranger proche[238] et la volonté de restaurer la grandeur de la Russie[239]. Cette dynamique s'est traduite par une approche renouvelée de la conflictualité, où l'effort ne porte plus uniquement sur les capacités conventionnelles, mais aussi, et surtout, sur l'intégration de moyens indirects au service d'objectifs politico-militaires[240]. Cette orientation repose sur une conception fluide et anticipatrice de la guerre, où la coordination entre les capacités cyber et électronique participe d'un continuum stratégique qui mêle temps de paix, compétition, et affrontement ouvert. Dans cette perspective russe, les champs d'action se superposent, les seuils d'escalade s'émoussent, et l'usage combiné des technologies pour déstabiliser devient un levier central de projection de puissance. Le spectre électromagnétique et le cyberespace, loin d'évoluer en silos, sont pensés comme des instruments complémentaires au service d'une même logique : obtenir de l'information, désorganiser, déstabiliser, voire neutraliser l'adversaire par des moyens non cinétiques, plus invisibles, et redoutablement efficaces. Au-delà de l'emploi systématique de ces deux objets de manière combinée, l'intérêt du cas d'étude russe réside aussi sur la possibilité d'étudier cette convergence dans différents types de conflits. D'un côté, dans le contexte de guerre hybride, où la GE et le cyber sont employés à bas bruit dans des stratégies de déstabilisation

[237] Michel Guénec, « La Russie face à l'extension de l'OTAN en Europe », *Hérodote*, 2008/2, n° 129, 2008, p. 221-246.
[238] Mikhail Suslov, "'Russian World' Concept: Post-Soviet Geopolitical Ideology and the Logic of 'Spheres of Influence'", *Geopolitics*, vol. 23, n° 2, 2018, p. 330–353.
[239] Julie Philippe, « Poutine, l'homme qui veut ressusciter l'URSS, à tout prix », *Public Sénat*, 15 décembre 2016 (https://www.publicsenat.fr/actualites/non-classe/poutine-l-homme-qui-veut-ressusciter-l-urss-a-tout-prix-51713)
[240] Alain Bauer, « La doctrine militaire russe et les leçons à en tirer pour l'Occident », *Les Cahiers de la Revue Défense Nationale*, 24 février-24 août : 6 mois de guerre en Ukraine, 2022, p. 52-61.

(3.1.). De l'autre, dans un contexte de conflit conventionnel, où ces outils sont également utilisés au sein des opérations classiques (3.2.). L'objectif de ce chapitre n'est pas de livrer une étude exhaustive des doctrines russes ou de l'emploi de cette convergence, ni un panorama technique des outils engagés, mais d'observer, à travers des cas précis, comment cette convergence se manifeste dans les faits, et quels en sont les effets sur les dynamiques de conflit.

3.1. Des manœuvres en zone grise : de l'ajustement des techniques hybrides à la convergence cyber-électronique

La relecture de la conflictualité par les élites militaires russes à partir des années 1990 est, entre autres, marquée par la volonté de pallier l'asymétrie face à l'OTAN. L'une des alternatives qui apparait pour contourner le désavantage matériel est l'utilisation de moyens indirects et d'opérations sous le seuil de la guerre déclarée, capables de produire des effets sans confrontation militaire directe[241]. Cette réflexion s'accélère avec les années 2000. L'arrivée au pouvoir de V. Poutine et les interventions occidentales, notamment au Kosovo et en Irak, nourrissent une vision selon laquelle les futures guerres se gagneront par la maîtrise des perceptions et la désorganisation des systèmes adverses. C'est dans ce cadre que la Russie a progressivement formulé une conception propre de la guerre hybride, souvent qualifiée de « guerre non linéaire[242] », qui conjugue l'usage de moyens civils et militaires, les outils technologiques, les acteurs étatiques et non étatiques, en contexte de paix apparente. Elle repose sur une anticipation des conflits où la ligne entre paix et guerre est volontairement brouillée, et où les capacités de désorganisation priment sur la supériorité militaire conventionnelle. L'articulation cyber-électronique devient alors une ressource privilégiée de cette approche, capable d'affaiblir un adversaire sans recours à la force armée ouverte[243]. Les opérations hybrides du début des années 2000 ont mis en avant certaines limites de l'usage des vecteurs technologiques, mais la réactivité russe quant à ces stratégies a progressivement pallié ces faiblesses pour atteindre l'efficacité, y compris cyber-électronique.

[241] Alain Bauer, « La doctrine militaire russe et les leçons à en tirer pour l'Occident », *op.cit.,* 2022, p. 52-54.
[242] Étienne Tremblay, « La guerre "non-linéaire" russe appliquée en Ukraine analysée à travers la guerre « hors limites » chinoise" », *Canadian Forces College*, Exercise Solo Flight, 2016.
[243] Harun Aras and Kahraman Süvari, "Unveiling Russia's secret weapon: cyber-electronic operations in hybrid warfare", *Journal of Military and Strategic Studies*, vol. 25, n° 1, 2024, p. 1-16.

3.1.1. Le cas estonien en 2007 : cyberattaque déstabilisatrice

En avril 2007, l'Estonie devient le théâtre de ce que de nombreux experts considèrent comme la première cyberattaque de grande ampleur dirigée contre un État souverain[244]. Cet épisode s'inscrit dans un contexte de tensions croissantes entre Tallinn et Moscou, sur fond de mémoire historique conflictuelle. Au cœur de la crise : la décision du gouvernement estonien de déplacer le monument soviétique, le « Soldat de bronze », situé au centre de la capitale, vers un cimetière militaire en périphérie. Si dans le récit russe ce soldat symbolise l'Armée rouge et la libération de l'Estonie en 1944, il est perçu, en Estonie, comme le rappel de l'occupation soviétique. Sa relocalisation avait ainsi provoqué une vive réaction de la communauté russophone locale[245], des émeutes dans les rues de Tallinn, et surtout, une condamnation ouverte de Moscou. Le ministre des Affaires étrangères russe, Sergueï Lavrov, avait qualifié cette décision de « blasphème » et avait menacé de « prendre des mesures sérieuses[246] », sans pour autant en préciser la nature. Quelques jours plus tard, le 27 avril 2007, une série coordonnée d'attaques informatiques frappe l'Estonie avec une intensité inédite. Pendant plus de trois semaines, les infrastructures numériques de l'ensemble du pays sont ciblées par des vagues massives d'attaques cyber. Les serveurs du gouvernement, du Parlement, des ministères, des grandes banques, des opérateurs télécoms et de plusieurs médias sont surchargés par des flux continus de requêtes malveillantes – ou déni de service[247] – qui provoquent le dysfonctionnement de nombreux services. L'ampleur des dégâts est d'autant plus importante que l'Estonie avait fait d'Internet la colonne vertébrale de son administration et de son économie[248]. En effet, pour compenser la faible densité de population (1,3 million d'habitants) et les ressources limitées du pays, l'Estonie s'est érigée, depuis les années 1990, comme un e-State : en 2007, 95% des opérations bancaires s'effectuaient en ligne et 98% du territoire était couvert par l'accès à Internet[249]. En 2007, le pic de cyberattaques a été relevé le 9 mai, soit, le jour de célébration de la victoire de 1945

[244] Thomas Armistead and Leigh Armistead, *A new Frontier in war: Cyber Warfare in Estonia*, Kruger National Park : NATO CCDCOE, 2015. 10th International Conference on Cyber Warfare and Security, p. 10.
[245] Peter Finn, "Statue's Removal sparks violent protests in Estonia", *Washington Post Foreign Service*, 2007.
[246] Eneken Tikk, Kadri Kaska and Liis Vihul, *International cyber incidents: Legal Considerations. Estonia 2007*, Tallin : NATO CCDCOE, 2010, p. 14.
[247] Ce procédé d'attaque consiste à prendre la main à distance sur des réseaux d'ordinateurs compromis au préalable (dits *botnets*) et de s'en servir pour relayer des messages qui viendront saturer les systèmes officiels jusqu'alors très peu protégés en Estonie. (Aymeric Bonnemaison et Stéphane Dossé, p. 62).
[248] Joshua Davis, "Hackers take down the most wired country in Europe", *Wired*, 21 août 2007 (https://www.wired.com/2007/08/ff-estonia/).
[249] Eneken Tikk, Kadri Kaska and Liis Vihul, *International cyber incidents: Legal Considerations. Estonia 2007*, *op.cit.*, 2010, p. 16-18.

par la Russie. Le lendemain, Hansapank, la première banque d'Estonie, était contrainte de fermer son service en ligne. Une semaine plus tard, ce fut tour de la deuxième banque du pays, SEB Pank, d'en faire autant[250]. La paralysie provoquée par cette vague de cyberattaques a rendu inaccessible les institutions publiques, et le pays a été contraint de bloquer les connexions extérieures, et donc de se couper temporairement du reste du monde numérique. Officiellement, l'attaque n'est pas attribuée à l'État russe. Aucun lien formel n'a pu être établi entre les assaillants et le Kremlin, bien que les adresses IP publiées par les autorités estoniennes pointent majoritairement vers la Russie[251]. Le gouvernement russe nie toute implication, mais la nature hautement coordonnée de l'opération, son ampleur[252], et le contexte géopolitique dans lequel elle intervient, renforcent les soupçons d'un acte sanctionnateur, orchestré ou au moins encouragé en arrière-plan par la Russie. Cette offensive illustre la capacité d'un seul moyen numérique à infliger des perturbations majeures à un État hautement numérisé, sans franchir le seuil de la guerre conventionnelle. Cet épisode marque un tournant dans la compréhension des logiques hybrides russes. Sans recourir à la force armée, Moscou, ou ceux agissant en son nom, a réussi à exercer une pression stratégique directe sur un État membre de l'Union européenne et de l'OTAN. Au-delà de l'impasse estonienne, cette cyberattaque a agi comme un électrochoc pour de nombreux États occidentaux[253], en soulignant à la fois la vulnérabilité des sociétés numérisées et le flou doctrinal concernant la réponse à ce type d'agression. En réaction, l'OTAN a créé dès 2008, à Tallinn, le CCDCOE, chargé d'améliorer l'expertise stratégique en matière de cyberdéfense[254]. Son implantation en Estonie n'est pas anodine : elle consacre l'événement de 2007 comme un moment fondateur dans la prise de conscience collective des nouvelles formes de conflictualité.

L'attaque contre l'Estonie a permis à Moscou de mesurer l'efficacité des opérations cyber et de s'assurer de la pertinence de ce moyen pour atteindre ses objectifs stratégiques à l'avenir. Elle inaugure l'emploi des capacités cyber comme instrument de sanction, d'intimidation et de désorganisation, parfaitement adapté aux stratégies russes de

[250] Gérôme Billois, *Cyberattaques : les dessous d'une menace mondiale*, *ibid.*, p. 90.
[251] Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Tallin : NATO CCDCOE, 2018, p. 2-4.
[252] Iain Thomson, "Russia 'hired botnets' for Estonia cyber-war", *ITnews*, 1er juin 2007 (https://www.itnews.com.au/news/russia-hired-botnets-for-estonia-cyber-war-82600).
[253] Mark Landler and John Markoff, "Digital fears emerge after data siege in Estonia", *The New York Times*, 29 mai 2007 (https://www.nytimes.com/2007/05/29/technology/29estonia.html).
[254] Michael R. Grimaila, "The Genesis of the NATO Cooperative Cyber Defense Centre of Excellence", *Information Systems Security Association Journal*, vol. 16, n° 8, 2018, p. 21.

déstabilisation en temps de paix. Dans ce cas, bien que la GE n'ait pas été explicitement utilisée, elle n'a pas été écartée de la doctrine russe pour autant. Après l'effondrement de l'URSS, les capacités de brouillage, d'interception et de désinformation avaient déjà été expérimentées dans divers contextes hybrides, notamment en Tchétchénie[255]. La déclaration de l'amiral Sergueï Gorchkov pendant la guerre froide – « celui qui maîtrise la totalité du spectre électromagnétique dominera le monde » – restait exacte en 2007[256]. Et c'est précisément parce que ses effets étaient déjà connus et maîtrisés que Moscou n'a pas eu recours au spectre électromagnétique, et que la capitale a pu privilégier l'expérimentation du cyberespace. Cette dissociation n'aura été que temporaire : dès l'année suivante, en Géorgie, la Russie amorce une première convergence entre capacités cyber et GE.

3.1.2. Le conflit russo-géorgien : mise en application limitée de la convergence cyber-électronique et réajustements

Le conflit russo-géorgien d'août 2008 constitue une étape majeure de l'utilisation des moyens cyber-électroniques dans un conflit. Contrairement à l'attaque contre l'Estonie un an plus tôt, qui reposait exclusivement sur des moyens cybers offensifs dans un contexte non militaire, la guerre contre la Géorgie inaugure l'emploi simultané de capacités cyber et de GE en appui à une opération militaire cinétique. Malgré l'intervention physique de troupes russes, ce conflit reste qualifié d'hybride car il a mobilisé de nombreux autres moyens en parallèle ; l'intervention cinétique ne constituant qu'une brève étape. L'épisode de 2008 se déroule dans un contexte de tension croissante entre Tbilissi et Moscou[257]. Sous l'impulsion de Mikheil Saakachvili, élu en 2004 après la Révolution des Roses, la Géorgie a opéré un rapprochement stratégique avec les États-Unis et l'OTAN. En parallèle, le pays intensifie ses efforts pour reprendre le contrôle des régions séparatistes d'Abkhazie et d'Ossétie du Sud[258], soutenues par la Russie depuis les années 1990. Le 7 août 2008, le conflit se matérialise : l'armée géorgienne lance une offensive contre l'Ossétie du Sud. En réaction, Moscou prétexte la défense de ses « compatriotes » et de ses forces de maintien de la paix dans la

[255] John Arquilla and Theodore Karasik, "Chechnya: A Glimpse of Future Conflict?", *Studies in Conflict & Terrorism*, vol. 22, n° 3, 1999, p. 207–229.
[256] Olivier Dujardin, « Guerre électronique : la guerre qu'il ne faut (surtout) pas perdre ! », *Centre français de Recherche sur le Renseignement*, note n° 35, 2021, p. 8.
[257] Natia Seskuria, "Russia's 'Hybrid Aggression' against Georgia: The Use of Local and External Tools", *Center for Strategic and International Studies*, 2021, p. 2-4.
[258] Julien Thorez, « Géorgie-Ossétie-Russie. Une guerre à toutes les échelles », *EchoGéo*, 2009.

région, et déploie des troupes, des blindés et des forces aériennes et navales[259]. Le conflit, bref mais intense, s'achève le 12 août 2008, après cinq jours d'hostilités, et laisse la Géorgie affaiblie. Cette campagne marque un tournant stratégique dans l'approche russe. Pour la première fois, des opérations cybernétiques sont intégrées à une offensive militaire pour perturber l'information, semer la confusion et désorganiser l'appareil décisionnel adverse. Selon Arnaud Garigues, les affrontements russo-géorgiens de 2008 « offrent […] un visage bien plus probable – que l'exemple estonien – de ce que pourrait être une utilisation militaire des capacités de perturbation offertes par Internet[260]. » Dès le mois de juillet 2008, bien avant le déclenchement des hostilités le 7 août, les premières cyberattaques sévissent[261]. Elles visent les centres de pouvoir géorgiens, notamment le ministère géorgien de la Défense et celui des Affaires étrangères, les sites des grandes chaînes d'information comme Rustavi 2, mais également les banques, et la population[262]. Elles amorcent une phase préparatoire du conflit. Durant la semaine du 7 au 12 août, les cyberattaques sont coordonnées dans le temps avec les opérations cinétiques sur le terrain : elles précèdent les frappes russes et visent à ralentir la capacité de réaction de l'État géorgien. Elles sont toutefois loin de semer un chaos incontrôlé. Tout d'abord parce que, en 2008, seuls 7% des Géorgiens accèdent à Internet, et donc les cyberattaques ne les paralysent pas eux directement[263]. Ensuite parce que les forces russes, dans ce contexte de guerre hybride et non de conflit traditionnel, cherchent avant tout à désorganiser l'adversaire, à affaiblir sa capacité de communication et à démontrer une supériorité informationnelle en amont et en parallèle des offensives. Cette approche graduée et ciblée révèle une stratégie de déstabilisation encore maladroite, du fait d'une mauvaise compréhension de la faible dépendance estonienne à Internet. Toutefois, l'intégration du vecteur cyber à l'ensemble des opérations incarne les prémices d'une convergence plus large. Elle ne conduit pas à un anéantissement total de la Géorgie, mais permet de véhiculer une démonstration de force et d'efficacité sur un terrain observé de près par l'OTAN et les autres puissances[264]. De nombreux experts considèrent ces cyberattaques comme les

[259] Serge Sur, « Analyse, interprétation et conséquences des évènements militaires en Géorgie », *Centre Thucydide*, Cahier Thucydide n° 9, 2010, p. 18-21.
[260] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 63.
[261] Aaron Mannes and James Hendler, "The First Modern Cyberwarfare?", *The Guardian*, 22 août 2008 (https://www.theguardian.com/commentisfree/2008/aug/22/russia.georgia1).
[262] Serge Sur, « Analyse, interprétation et conséquences des évènements militaires en Géorgie », *op.cit.*, 2010, p. 44-46.
[263] Eneken Tikk, Kadri Kaska and Liis Vihul, *International cyber incidents: Legal Considerations. Estonia 2007*, *op.cit.*, 2010, p. 68.
[264] Aymeric Bonnemaison et Stéphane Dossé, *Attention : Cyber ! : Vers le combat cyber-électronique*, *op.cit.*, 2014, p. 64.

premiers exemples de « cyber-couverture[265] » d'une manœuvre militaire classique. En ce sens, l'outil cyber confirme son efficacité opérationnelle et perfectionne l'usage qui en avait été fait en Estonie. Du côté de la GE, les capacités sont déployées sur le théâtre d'opération pour perturber les communications tactiques de l'armée géorgienne[266]. De fait, l'expérience géorgienne a permis de tester, en conditions réelles, la combinaison d'outils cyber et de GE. Toutefois, cette campagne, malgré son efficacité en termes de résultat final, a aussi mis en évidence des faiblesses structurelles dans le dispositif russe relatif à cette convergence.

> *L'attaque cybernétique et cinétique combinée de la Russie contre la Géorgie en 2008 a été le premier test pratique de cette doctrine. Même si cette opération n'a pas été pleinement couronnée de succès, nous devons supposer que l'armée russe a retenu les leçons, tout comme elle l'a fait pour tous les autres aspects de sa mauvaise performance contre la Géorgie[267].*

> *Lors de la guerre en Géorgie, les forces russes se montrèrent incapables de neutraliser efficacement les défenses antiaériennes adverses en raison de l'obsolescence de leur matériel de guerre électronique. Moscou payait là son désintérêt pour la discipline depuis 1979[268].*

Il convient de nuancer la notion de « désintérêt », car la Russie, tout comme les États-Unis, n'a jamais abandonné le développement de l'outil électronique[269]. Même si la fin de la Guerre froide a imposé une baisse des investissements dans le secteur militaire, la GE a continué d'occuper les esprits militaires russes même après la chute de l'Union soviétique[270]. Cet intérêt avait d'ailleurs été renforcé à la suite de l'utilisation de la GE par les Américains lors de la première guerre du Golfe, faisant de ce sujet « un thème récurrent » dans les études des officiers d'état-major russes[271]. Mais cet intérêt n'a pas suffi pour atteindre l'efficacité électronique sur le champ de bataille. D'une part, les capacités de brouillage utilisées reposaient pour la plupart sur des systèmes hérités de l'ère soviétique. De fait, ces dispositifs étaient peu adaptés aux standards numériques contemporains et à la guerre réseau-centrée. Leur portée, leur précision et leur résilience étaient insuffisantes face à des systèmes

---

[265] David Hollis, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, 1er juin 2011 (https://smallwarsjournal.com/2011/01/06/cyberwar-case-study-georgia-2008/).
[266] Patrick Smith," Russian Electronic Warfare: A growing threat to U.S. Battlefield Supremacy", *American Security Project*, 2020, p. 3-5.
[267] David J. Smith, "Russian Cyber Strategy and the War Against Georgia", *Focus Quarterly NATO*, 2014.
[268] Yannick Genty-Boudry, « Guerre électronique. Le multiplicateur de force russe », *Défense et Sécurité Internationale*, n° 143, 2019, p. 98.
[269] Entretien avec M. Pierre Baratault ; entretien avec le colonel Éric Gomez ; entretien avec M. Yannick Genty-Boudry.
[270] Patrick Smith," Russian Electronic Warfare: A growing threat to U.S. Battlefield Supremacy", *op.cit.*, 2020, p. 3.
[271] Patrick Smith, *ibid*., p. 2.

modernes de communication. D'autre part, c'est au niveau de la coordination interarmées entre les unités de GE et les forces conventionnelles que la méthode russe s'est révélée défaillante. Les capacités de GE n'étaient ni systématisées ni intégrées dans la planification opérationnelle. Elles ont échoué à neutraliser les défenses aériennes géorgiennes plus modernes, à couvrir les forces en progression et à créer des zones de brouillage. Leur impact réel sur le champ de bataille est donc resté limité : elles ont gêné ponctuellement les transmissions géorgiennes mais sans produire d'effets stratégiques durables. Enfin, la guerre a aussi montré l'absence d'un commandement centralisé du domaine informationnel. Et c'est précisément ce que la Russie s'est efforcée de corriger dès l'après-conflit, en repensant l'articulation entre les différents services de la sphère militaire. Ces relatifs échecs ont constitué une nouvelle relance de la vision combinée des moyens. À l'issue du conflit, les autorités russes prennent acte de ces lacunes : le ministère de la Défense, sous l'impulsion d'Anatoli Serdioukov puis de Sergueï Choïgou, engage une vaste réforme de modernisation militaire dès 2009[272]. Un effort particulier est consacré à la mise à jour des outils de GE. Le taux de modernisation de ces équipements passe de 10% à 70% entre 2010 et 2020[273]. Sur le plan doctrinal, les leçons de la Géorgie donnent de la matière pour redéfinir la guerre dite « non linéaire », dans laquelle l'usage coordonné des vecteurs informationnels devient central. La création, en 2012, de l'unité d'opérations informationnelles, "Information Troops", au sein des forces armées russes, témoigne de cette volonté de mieux intégrer le champ cyber avec les milieux électronique et cognitif[274]. Cette modernisation de l'armée post-conflit a priorisé les domaines où la Russie pouvait obtenir un avantage asymétrique sur ses potentiels adversaires. Parmi eux, la GE, et plus généralement, les outils informationnels, sont ressortis comme les vainqueurs de cette ambitieuse réforme. À tel point que les efforts entrepris dans le domaine électronique ont surpassé les capacités américaines : « Aujourd'hui, de nombreux observateurs et responsables de la défense affirment que la capacité de la Russie à s'engager dans la GE est supérieure à celle des États-Unis[275]. » Cette hybridation balbutiante post-Géorgie renforce les bases d'une future coordination cyber-électronique opérationnelle, au-delà de la simple convergence.

[272] Aleksei Ramm, "The Russian Army: Organization and Modernization", *CAN National Security Analysis*, 2019, p. 8.
[273] Yannick Genty-Boudry, « Guerre électronique. Le multiplicateur de force russe », *op.cit.*, 2019, p. 98.
[274] Keir Giles, *"Information Troops" – a Russian Cyber Command?* Tallin : NATO CCDCOE, 2011. 3rd International Conference on Cyber Conflict.
[275] Patrick Smith," Russian Electronic Warfare: A growing threat to U.S. Battlefield Supremacy", *op.cit.*, 2020, p. 4.

3.1.3. L'Ukraine de 2014 à 2022 ou la démonstration d'une stratégie intégrée et plus aboutie

Par rapport à l'Estonie en 2007 ou la Géorgie en 2008, l'intervention russe en Ukraine en 2014 révèle une inflexion stratégique plus aboutie : l'intégration coordonnée, à une échelle inédite, des moyens militaires, cybernétiques, et électromagnétiques. Cet épisode reflète l'évolution de la compréhension russe quant aux nouvelles formes de conflictualité, notamment après la publication d'un article du chef d'état-major russe Valeri Guerassimov en février 2013[276]. En analysant les interventions occidentales en Irak, dans les printemps arabes et les révolutions de couleur, il constate deux éléments : un brouillage croissant entre guerre et paix ; la montée en puissance des moyens non militaires et le fait que « l'influence à distance, sans contact avec l'adversaire, devient le principal moyen d'atteindre ses objectifs de combat et d'opération[277] ». Dès lors apparait la nécessité de répondre à ces menaces par une combinaison de moyens conventionnels et non linéaires. Ce texte, interprété abusivement comme une doctrine par l'Occident, est en réalité un constat, qui pose les bases d'une pensée stratégique russe centrée sur la désorganisation systémique de l'adversaire avant même l'engagement armé[278]. Dans cette optique, la désactivation technologique, le brouillage informationnel et la désorientation cognitive ne sont plus des outils périphériques : ils deviennent les conditions préalables à toute intervention efficace, comme le montre le cas ukrainien dès 2014.

L'intervention débute dans les jours qui suivent la révocation par le Parlement ukrainien du Président pro-russe Viktor Ianoukovitch. En novembre 2013, celui-ci rompt brutalement les négociations de l'Ukraine avec l'Union européenne, et déclenche une vague de protestations populaires, connues sous le nom d'Euromaidan[279], qui dégénèrent en affrontements violents. Dans ce contexte de crise institutionnelle, la Rada, le Parlement ukrainien, décide de libérer l'opposante emblématique Ioulia Timochenko, d'organiser une élection présidentielle anticipée en mai 2014, et acte ainsi la perte de légitimité de

[276] Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Industrial Kurier*, 2013.
[277] Céline Marangé, « Le nucléaire russe : un instrument de dissuasion et d'intimidation », *Revue Défense Nationale*, n° 802, 2017.
[278] Émile Vaizand, « Comprendre l'impénétrable modèle de la doctrine militaire russe », *Slate*, 14 mars 2024 (https://www.slate.fr/story/266136/guerre-hybride-russie-poutine-guerassimov-doctrine-strategie-militaire-renseignement-armee-ukraine-occident).
[279] Taras Kuzio, "Euromaidan Revolution, Crimea and Russia–Ukraine War: Why It Is Time for a Review of Ukrainian–Russian Studies", *Eurasian Geography and Economics*, vol. 59, n° 3, 2018, p. 529–553.

Ianoukovitch, qui fuit le pays[280]. Profitant de ce désordre politique à Kiev, la Russie engage une opération multidimensionnelle. Il ne lui aura fallu que deux semaines pour prendre le contrôle complet de la péninsule de Crimée sans engager de bataille conventionnelle majeure. Cette opération, rapide et efficace, témoigne d'une haute planification et d'une fine synchronisation entre les moyens militaires de faible intensité, et les vecteurs numériques et informationnels[281]. Dès le 27 février, des hommes armés, vêtus d'uniformes militaires verts, équipés de matériels russes, et sans éléments d'identification, prennent le contrôle du parlement régional de Crimée à Simferopol. Ils hissent le drapeau russe et instaurent un gouvernement local favorable à Moscou. Ceux que l'on a nommé les « petits hommes verts » sont en réalité des forces spéciales russes, les Spetsnaz du GRU, et des troupes aéroportées, VDV, qui ont été débarquées à Sébastopol, officiellement pour « protéger les intérêts russes[282] ». Leur présence est à l'époque déniée publiquement par Moscou. Parallèlement, une série de cyberattaques ciblées et d'actions de GE est lancée. Fin février 2014, les téléphones des parlementaires ukrainiens sont paralysés par une attaque TDoS (Telephony Denial of Service[283]), au moment précis des votes décisifs à Kiev pour la transition du pouvoir[284]. Dans le même temps, un câble de communication est physiquement sectionné en Crimée : les autorités ukrainiennes locales sont alors isolées des structures nationales. Selon Ukrtelecom, cette coupure physique du câble est combinée à des brouillages d'ondes radio orchestrés depuis des navires russes en mer Noire et des installations mobiles au sol, ce qui bloque dans le même temps les communications militaires et civiles dans la péninsule[285]. Les opérations de GE se concentrent sur le brouillage des transmissions militaires ukrainiennes, ainsi que des fréquences civiles. Il contribue de fait à créer un brouillard informationnel total en Crimée. Ces outils, déjà éprouvés en Géorgie en 2008, sont ici utilisés avec une précision tactique accrue. Cette opération multi frontale est conduite avec une précision chirurgicale : cyber, GE, sabotage physique, désinformation et forces spéciales

[280] Le Monde avec AP, AFP et Reuters, « Le président destitué, Timochenko libérée : l'Ukraine bascule », *Le Monde*, 22 février 2014 (https://www.lemonde.fr/europe/article/2014/02/22/proche-de-ianoukovitch-le-president-du-parlement-ukrainien-demissionne_4371588_3214.html).
[281] Matthieu Douillet, « Opérer en environnement multi-milieux/multi-champs : de la théorie à la formation : Complexité et innovation dans les opérations militaires », *Revue Défense Nationale*, vol. 8, n° 863, 2023, p.74.
[282] Michel Goya, « Comment neutraliser un pays sans le dire », *Défense et Sécurité Internationale*, n° 144, 2019, p. 68-71.
[283] Technique qui consiste à saturer les lignes téléphoniques par des appels automatisés massifs, rendant toute communication impossible.
[284] Anthony Namor, « Le combat cyberélectronique russe en Ukraine », *Le Rubicon*, 8 juillet 2022 (https://lerubicon.org/le-combat-cyberelectronique-russe-en-ukraine/).
[285] Margarita Jaitner and Peter A. Mattson, *Russian Information Warfare of 2014*, Tallin : NATO CCDCOE, 2015. 7th International Conference on Cyber Conflict, p. 45.

convergent dans un temps resserré[286]. Les objectifs sont atteints en 13 jours : le 11 mars 2014, le Parlement Criméen et Sébastopol adoptent supposément une déclaration d'indépendance vis-à-vis de l'Ukraine, et le 16 mars, elle est soi-disant validée à 95% avec un taux de participation de 80%[287]. Ce référendum est boycotté par les opposants et dénoncé par le gouvernement ukrainien ainsi que la quasi-totalité des pays étrangers. Le lendemain, le Parlement déclare officiellement son indépendance ainsi que son accession à la Russie. Ces mesures sont jugées illégales par la communauté internationale[288].

À partir du printemps 2014, la Russie étend son action hybride au Donbass, dans les régions de Donetsk et de Louhansk. Contrairement à la Crimée, l'occupation se heurte ici à une résistance ukrainienne plus structurée, ce qui conduit à un conflit de moyenne à haute intensité. Les moyens employés évoluent, mais la coordination cyber-électronique reste présente dans la phase initiale. En mai 2014, à la veille de l'élection présidentielle ukrainienne, les services de cybersécurité découvrent un malware infiltré dans le système de vote électronique, conçu pour falsifier les résultats en supprimant des bulletins[289]. L'attaque est neutralisée à temps, mais témoigne de l'intention russe de perturber la légitimité du scrutin au plus haut niveau. Sur le terrain, les forces séparatistes prorusses bénéficient d'un soutien direct en renseignement électronique. Le système de GE Leer-3[290], par exemple, est déployé dès 2015 et permet d'intercepter les communications GSM, de localiser les positions via les signaux téléphoniques, voire de diffuser des faux messages de reddition ou de panique aux troupes ukrainiennes. Ces dispositifs agissent de concert avec les capacités cyber russes, opérées par des unités issues du FSB, du GRU, notamment l'unité 26165, et d'un réseau de cybercriminels affiliés. Ce n'est qu'après 2015 que la synchronisation entre actions cinétiques et cyber commence à décliner, avec l'absence de corrélation temporelle forte entre frappes physiques et attaques informatiques[291]. Une nouvelle mutation s'opère alors : les vecteurs cyber deviennent des instruments autonomes d'attrition politique ou de sabotage stratégique. En effet, dans les années qui suivent, les opérations russes en Ukraine évoluent

[286] Tim Maurer and Scott Janz, "The Russia-Ukraine Conflict; Cyber and Information Warfare in a Regional Context", *International relations and Security Networks ETH Zurich*, 2014, p. 33.
[287] Perspective Monde, "Tenue d'un référendum en Crimée », *Perspective Monde*, 2014.
[288] Anne Peters, "The Crimean vote of March 2014 as an abuse of the institution of the territorial referendum", *Max Planck Institute for Comparative Public Law and International Law*, 2014, p. 256.
[289] Anthony Namor, « Les opérations numériques dans les conflits contemporains », in Stéphane Taillat, Amaël Cattaruzza et Didier Danet, *La Cyberdéfense : Politique de l'espace numérique*, 2e éd., Paris : Armand Colin, 2023, p. 233-243.
[290] Yannick Genty-Boudry, « Guerre électronique. Le multiplicateur de force russe », *op.cit.*, 2019, p. 100.
[291] Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefields Events?", *Journal of Conflict Resolution*, vol. 63, n° 1, 2017, p. 317-347.

vers une conflictualité indirecte, non localisée et non cinétique. En décembre 2015, la cyberattaque Black Energy, attribuée au groupe Sandworm, supposément lié au GRU, provoque une coupure de courant et affecte environ 230 000 personnes dans l'ouest de l'Ukraine[292]. C'est la première fois qu'une cyberattaque entraîne une panne d'électricité à grande échelle. Cette opération illustre l'intégration croissante des capacités cyber dans les objectifs stratégiques russes, en ciblant directement les infrastructures critiques. D'autres attaques suivent, comme NotPetya en 2017. Lancée à partir d'un logiciel comptable très utilisé en Ukraine, M.E.Doc, elle paralyse instantanément des infrastructures clés des secteurs bancaires, énergétiques, gouvernementaux[293]. Au-delà de ces déstabilisations régulières, la Russie renforce le contrôle de l'espace informationnel. Dès 2014, la pose de câbles sous-marins entre la Crimée et la Russie continentale sécurise les flux numériques et exclut le réseau ukrainien. Ce contrôle permet ensuite d'y déployer un Internet filtré par le FSB et de restreindre l'accès aux médias non alignés, tout en orchestrant des campagnes massives de désinformation, par exemple sur la « légitimité » du référendum ou sur les prétendues persécutions des russophones[294]. En somme, le succès de la déstabilisation invisible russe 2014 à 2022 a reposé sur une logique de préparation informationnelle du champ de bataille : brouillage, désorganisation cognitive, saturation de la décision politique, tout était mis en œuvre pour rendre la résistance inopérante. Dans ce cas précis, l'utilisation complémentaire du cyberespace et du spectre électromagnétique a été fondamentale. Alors que la plupart des auteurs occidentaux utilisaient la notion de « guerre hybride » pour désigner le rôle des acteurs non-étatiques dans les conflits, le cas ukrainien ajoute une nouvelle couche de définition à ce concept complexe : celle de la combinaison des moyens conventionnels et non-conventionnels, et leur hybridité[295].

Depuis la fin des années 2000, la Russie a pris un virage assumé vers le domaine informationnel, devenu un levier efficace discret, parfaitement adapté à ses stratégies de déstabilisation hybrides. L'approche russe en matière de guerre hybride illustre une résilience rapide, notamment dans les moyens cyber et électroniques. Moscou en a fait un outil central, non seulement pour affirmer son influence dans son voisinage, mais aussi pour

[292] Tamara Maliarchuk, Yuriy Danyk and Chad Briggs, "Hybrid Warfare and Cyber Effects in Energy Infrastructure", *Connections: The Quarterly Journal*, vol.18, n° 2, 2019, p. 97.
[293] Andy Greenberg, "The Untold Story of NotPetya, the most devastating cyberattack in history", *Wired*, 22 août 2018 (https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/).
[294] Anthony Namor, « Les opérations numériques dans les conflits contemporains », *op.cit.*, 2023, p. 239.
[295] Gjorgji Veljovski, Nenad Taneski and Metodija Dojchinovski, "The Danger of 'Hybrid Warfare' from a Sophisticated Adversary: The Russian 'Hybridity' in the Ukrainian Conflict", *Defense & Security Analysis*, vol. 33, n° 4, 2017, p. 292-307.

démontrer ses capacités informationnelles face à l'OTAN. Consciente de ses limites conventionnelles, la Russie mise sur ces vecteurs, utilisés en temps de paix comme en temps de guerre, pour conserver un avantage stratégique et opérationnel constant. Et cette logique ne s'arrête pas à la guerre hybride.

3.2. De l'ombre au champ de bataille : la convergence cyber-électronique dans le conflit russo-ukrainien

Au vu des opérations cyber-électronique menées dans des conflits de courte durée ou dans des épisodes de guerre hybride, la coordination cyber-électronique ne peut qu'être réutilisée dans des conflits de haute intensité. Cette logique d'hybridation des moyens informationnels n'a cessé de structurer la montée en puissance des capacités militaires russe depuis 2007. Même si la fréquence des pics de tensions ouvertes s'est temporairement atténuée après l'annexion de la Crimée, la Russie a continué de perfectionner ses outils, et en particulier la coordination entre GE et capacités cyber. L'intervention en Syrie en 2015[296] ou l'exercice militaire Zapad en 2017[297], ont été, entre autres, des indices probants de la volonté persistante russe d'articuler capacités cyber et électroniques. Le conflit en Ukraine depuis 2022 ne marque pas une rupture, mais plutôt le prolongement naturel du processus de maturation de cette convergence cyber-électronique. Dans cet affrontement de haute intensité, l'intégration cyber-électronique est devenue un appui régulier et non-négligeable des campagnes militaires russes, notamment dans les offensives où la désorganisation des réseaux ennemis provoque un effet de levier pour les moyens conventionnels.

3.2.1. L'attaque Ka-Sat ou la neutralisation du C2 par la convergence cyber-électronique

En temps de guerre, l'intérêt d'utiliser les vecteurs cyber et électronique réside dans la capacité de démultiplier les fronts, et donc les chances d'obtenir un avantage sur l'adversaire. En l'occurrence, pour les actions cyber et la GE, l'un des buts peut être de se concentrer là où la force militaire n'opère pas, pour jouer sur l'effet de surprise et ainsi provoquer une plus

[296] Austen Givens, "Putin's Cyber Strategy in Syria: Are Electronic Attacks Next?", *The Cyber Defense Review*, 2015.
[297] Jonas Kjellén, "Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces", *Swedish Defence Research Agency*, 2018, p. 51.

grande déstabilisation. En ce sens, le concept d'attaque parallèle des cinq cercles de John Warden[298] est éclairant. Cette théorie explique que dans un conflit de haute intensité, l'attention se focalise majoritairement sur les forces conventionnelles. De fait, infliger le maximum de dégâts exige de contourner cette attention adverse. Le but est alors le suivant : frapper au plus près du centre de commandement, par d'autres vecteurs et avec d'autres cibles. Ainsi, les centres névralgiques d'un État deviennent des cibles privilégiées : centrales énergétiques, réseaux de communication, réseaux routiers ou de distribution, etc. Ces atteintes permettent de désarticuler l'adversaire de manière stratégique, par exemple avant un affrontement, et peuvent toucher durablement l'économie d'un État et sa population[299]. Les capacités cyber et électroniques qui ont servi aux Russes lors de l'entrée en guerre s'inscrivent dans cette logique. L'attaque sur le réseau Ka-Sat[300] est un cas d'école sans précédent. Dans la nuit du 23 au 24 février 2022, quelques heures avant l'entrée des chars russes en Ukraine, la première attaque avait été lancée : elle était cyber-électronique. La nature de l'attaque sur le réseau satellitaire Ka-Sat est inédite dans l'histoire des conflits interétatiques : elle combine, dans le même temps, des actions cinétiques, électroniques et cyber. L'entretien conduit avec M. Serge Cholley, directeur Sécurité Défense chez Eutelsat au moment de l'attaque, a été une précieuse opportunité pour recueillir des éléments inédits.

Dans n'importe quelle guerre, « tout planificateur qui se respecte commence par casser les canaux qui permettent à un chef de donner des ordres et recevoir des comptes rendus[301] ». En ce sens, l'objectif affiché par cette attaque de casser la chaîne de commandement et de contrôle (C2) adverse n'est pas nouveau dans la guerre. Traditionnellement, les guerres ont toujours débuté par la destruction des capacités C2 adverses : attaques physiques par missiles, par obus, par roquettes, pour casser les pylônes, antennes, tours de transmission, radars. Il faut casser le système nerveux d'un adversaire pour l'empêcher de s'organiser et d'être efficace, c'est-à-dire, son système de télécommunication. De fait, il n'est pas surprenant de constater que, dans la nuit du 23 au 24 février 2022, les Russes ont cassé avec des bombes toutes les antennes visibles qu'ils connaissaient en Ukraine[302]. En parallèle, ils

[298] John Warden, "The Enemy as a system", *Airpower Journal*, vol. 9, n° 1, 1995, p. 40-55.
[299] Jean-Sun Luiggi, « Cyberguerre, nouveau visage de la guerre ? », *op.cit.*, 2016, p. 97.
[300] Martin Untersinger, « Guerre en Ukraine : la Russie accusée d'être derrière la cyberattaque ayant visé le réseau du satellite KA-SAT », *Le Monde*, 10 mai 2022 (https://www.lemonde.fr/pixels/article/2022/05/10/guerre-en-ukraine-la-russie-accusee-d-etre-derriere-la-cyberattaque-ayant-vise-le-reseau-du-satellite-ka-sat_6125513_4408996.html).
[301] Entretien avec M. Serge Cholley.
[302] Claire Tervé, « Guerre en Ukraine : à Kiev, la tour de télévision détruite par une frappe russe », *HuffingtonPost*, 1er mars 2022 (https://www.huffingtonpost.fr/international/article/guerre-en-ukraine-a-kiev-la-tour-de-television-detruite-par-une-frappe-russe_193237.html).

ont mené des actions de GE pour brouiller les signaux entre le terminal utilisateur et le satellite Ka-Sat. La fréquence utilisée par les Ukrainiens pour communiquer était ainsi hors d'usage[303]. Et pour la première fois, un troisième vecteur a sévi : l'attaque sur le réseau Ka-Sat, de l'opérateur américain Via-Sat. Cette cyberattaque a eu lieu sur les modems, les segments terrestres, utilisés par le satellite Ka-Sat, et non sur le satellite en lui-même (Annexe 1). Cette remarque est fondamentale car de nombreuses erreurs ont été commises dans l'analyse de cette attaque[304]. Le général Friedling, à l'époque commandant de l'espace en France, avait déclaré que « la guerre a commencé dans l'espace[305] ». L'erreur analytique avait aussi été retrouvée dans des rapports institutionnels, qui mentionnaient une atteinte au satellite lui-même[306]. Il y avait toutefois de quoi s'y perdre : la confusion avait été entretenue par l'opérateur ViaSat lui-même, qui avait refusé, dans un premier temps, de reconnaître l'attaque comme une cyberattaque. À l'époque, l'entreprise parlait d'un « cyber événement[307] » plutôt que d'une cyberattaque. Elle redoutait que l'événement soit considéré comme un acte de guerre, ce qui aurait annulé toute prise en charge par les assurances. En évitant le terme « attaque », ViaSat espérait rester dans le champ des incidents techniques, afin de pouvoir être indemnisée[308]. Ce flou sémantique avait favorisé la diffusion d'analyses erronées, y compris jusque dans les plus hautes sphères politico-militaires. En réalité, aucune composante spatiale n'a jamais été attaquée. L'opération ne visait ni le segment spatial ni les gateways du système. L'attaque cyber s'est concentrée exclusivement sur les modems du segment terrestre, les fameux VSAT[309], composés d'une petite antenne et d'un modem, qui avaient été déployés en Ukraine. Ce qui s'apparente à du détail ici est en fait une distinction fondamentale pour comprendre la triple dimension de cette attaque, ainsi que le mode opératoire des Russes pour y parvenir.

[303] Entretien avec M. Serge Cholley.
[304] Entretien avec M. Serge Cholley.
[305] Europe 1, « Ukraine : "La guerre a commencé dans l'espace", declare le Général Michel Friedling, *Europe 1*, 25 juin 2022 (https://www.europe1.fr/international/ukraine-la-guerre-a-commence-dans-lespace-declare-le-general-michel-friedling-4119684).
[306] Clémence Poirier, *The War in Ukraine from a Space Cybersecurity Perspective*, Vienna : European Space Policy Institute, 2022. ESPI Report 84.
[307] Alice Vitard, « Le satellite KA-SAT aurait dysfonctionné à cause d'une cyberattaque », *L'Usine Digitale*, 4 mars 2022 (https://www.usine-digitale.fr/article/le-satellite-ka-sat-aurait-dysfonctionne-a-cause-d-une-cyberattaque.N1791052).
[308] Entretien avec M. Serge Cholley.
[309] Stations terrestres bidirectionnelles qui permettent de transmettre / recevoir des données par satellite, de n'importe où. Ces dispositifs offrent une connexion sans frontière, et sans contraintes liées aux installations filaires, puisqu'elle se base sur les satellites placés en orbite autour de la Terre. (Globaltel Networks)

La nature inédite de cette attaque n'est pas le résultat d'un hasard ou d'un pari réussi. Le choix de mobiliser les compétences cyber sur les VSAT était rationnel : cette cyberattaque a été le fruit d'une longue préparation, bien avant le début de la guerre en février 2022. Et pour le comprendre, il faut remonter aux élections présidentielles de 2019 en Ukraine. Dans un contexte de tensions régionales avec la Russie, et d'ingérences russes dans plusieurs élections occidentales[310], la Commission électorale centrale d'Ukraine annonce la présence de 2 344 observateurs internationaux pour surveiller le déroulement de ces élections[311]. Au-delà des centaines de membres mandatés par l'OSCE[312], l'organisation déploie également des VSAT afin d'éliminer toute possibilité de fraude à grande échelle. Ces modems, physiques, sont ainsi installés à côté d'un grand nombre de bureaux de vote à travers le pays, notamment dans les zones indépendantistes, russophones, comme le Donbass et Lugansk. À la fin du processus, ces élections sont jugées crédibles, les observateurs repartent, mais pas les VSAT. L'OSCE répond aux autorités ukrainiennes qu'ils peuvent leur être utile pour la connectivité de leur territoire. Toutefois, le pays ne se contente pas de les utiliser à des fins civiles : il intègre ces VSAT à l'armée ukrainienne[313]. Il n'y a aucune information sur comment les Russes ont pu avoir connaissance de cette utilisation dans l'armée ukrainienne, cependant, le fait que les petits hommes verts aient récupéré un VSAT et l'aient ramené en Russie laisse peu de doute sur leurs intentions. Une fois à Moscou, l'armée russe a bénéficié de plusieurs années pour le désosser, l'étudier, voir comment le dispositif était constitué, et surtout, quelles étaient ses failles. Il convient de souligner que ce type de modems relevait d'une architecture civile, et donc peu protégée. Les terminaux utilisés provenaient de la première génération du réseau Ka-Sat, déjà jugé obsolète par l'opérateur américain ViaSat, qui avait cessé d'investir dans sa sécurisation[314]. Contrairement aux réseaux militaires durcis, ces modems n'étaient ni chiffrés, ni blindés, ni préparés à un usage en zone de guerre. La Russie n'a donc pas seulement profité d'un modem à sa disposition, elle a aussi pu bénéficier d'une vulnérabilité technique structurelle. La cyberattaque laisse supposer que les chercheurs russes ont découvert une faille 0-day[315], c'est-à-dire, une vulnérabilité pas encore

[310] Darin E.W. Johnson, "Russian election interference and race-baiting", *Columbia Journal of Race and Law*, vol. 9, n° 1, 2019.
[311] Ukrinform, « La CEC a achevé l'inscription des observateurs étrangers à l'élection présidentielle en Ukraine », *Ukrinform*, 26 mars 2019 (https://www.ukrinform.fr/rubric-elections/2667355-la-cec-a-acheve-linscription-des-observateurs-etrangers-a-lelection-presidentielle-en-ukraine.html).
[312] OSCE, *Presidential Elections, 31 March and 21 April 2019*, OSCE Office for Democratic Institutions and Human Rights, s.d.
[313] Entretien avec M. Serge Cholley.
[314] Entretien avec M. Serge Cholley.
[315] Kaspersky, « Qu'est-ce qu'une attaque zero-day ? », *Kasperky*, s.d. (https://www.kaspersky.fr/resource-center/definitions/zero-day-exploit).

identifiée et qui peut de fait être exploitée sans que les cibles, en l'occurrence l'Ukraine, n'en aient connaissance. Cette étude du modem en amont explique pourquoi ce sont les modems VSAT précisément qui ont été attaqué, et comment la Russie est parvenue à déclencher une attaque sans précédent. Elle a mobilisé ses forces là où elle pouvait gagner un avantage stratégique. Or, là où le satellite ne pouvait pas être étudié en profondeur de manière discrète, ni les autres dispositifs, les modems VSAT le permettaient.

> *Ils [les Russes] n'ont pas attaqué le circuit, les réseaux qui sont dans le satellite, ou les réseaux et les puces qui sont dans la gateway, ni dans les points of presence, ni dans le cloud ou autre chose. Ils ont attaqué les réseaux qui sont dans les modems parce qu'ils en disposaient*[316].

La compréhension de cette attaque et des dimensions en jeu aide à identifier la nature inédite de l'épisode Ka-Sat, mais elle donne aussi la possibilité de cerner des faiblesses de ce nouveau modus operandi. Il est indéniable qu'il s'agit d'une attaque sans précédent. Néanmoins, les aspects novateurs mis en avant par les analyses ne doivent pas cacher les limites d'une telle combinaison de moyens. Dans cet épisode, le déclenchement de l'attaque de type 0-day, donc de la cyberattaque, a provoqué plus de dégâts en Pologne, en Allemagne, en Grande-Bretagne, en France et au Maroc, qu'en Ukraine[317]. Environ 40 000 modems ont été physiquement cassés par l'attaque cyber et cela a engendré des répercussions très concrètes, au-delà de l'Ukraine. L'exemple utilisé dans la presse est celui des éoliennes allemandes[318], dont le C2 a été interrompu. Autrement dit, les éoliennes ont continué à tourner, il n'y a pas eu de rupture de fonctionnement. En revanche, toutes les liaisons qui permettaient au centre de contrôle de l'entreprise de commander et surveiller les opérations de ces éoliennes ont été endommagées : l'entreprise ne recevait plus d'indications de bon ou de mauvais fonctionnement[319]. Pour revenir au cas de l'Ukraine, la cyberattaque n'a pas eu d'effets dans ses premières minutes. Et cela s'explique par le brouillage qui a empêché, ou en tout cas retardé, l'attaque cyber sur les terminaux utilisateurs ukrainiens[320]. Ce n'est que quand les troupes russes s'en sont rendu compte qu'ils ont stoppé le brouillage pour laisser les effets de la cyberattaque être pleinement efficaces. Cette remarque est intéressante pour

[316] Entretien avec M. Serge Cholley.
[317] Mika Kerttunen, Kim N. Schuck and Jonas Hemmelskamp, *Major Cyber Incident: KA-SAT 9A*, European Repository of Cyber Incidents, 2023, p. 1-3.
[318] Elsa Bembaron, « 6 000 éoliennes allemandes touchées par une cyberattaque russe », *Le Figaro*, 3 mars 2022 (https://www.lefigaro.fr/secteur/high-tech/6000-eoliennes-allemandes-touchees-par-une-cyberattaque-russe-20220302).
[319] Joe Slowik, "Reviewing the 2022 Ka-Sat incident & implications for distributed communication environments", *Virus Bulletin*, 2024, p. 7-8.
[320] Entretien avec M. Serge Cholley.

notre étude : même si ce sont l'historique et l'évolution de la convergence cyber-électronique qui sont analysés ici, cette observation permet de voir qu'à un certain degré de convergence, entendue ici comme une coordination poussée, voire intégration, les effets de l'un peuvent annuler ceux de l'autre. Même s'il faudrait y consacrer une tout autre étude, il est pour l'instant déjà possible d'ajouter ce constat aux caractéristiques inédites de cette attaque sur le réseau Ka-Sat : ce nouveau type d'attaque exige une coordination particulière, adaptée aux conséquences de la simultanéité des vecteurs d'attaque.

Ka-Sat est la première attaque qui combine et coordonne, en même temps, les actions cinétiques, électroniques et cyber. Malgré son caractère inédit[321], le manque de recul sur l'usage cyber-électronique laisse planer une ambivalence dans ses effets. D'une part, cette convergence peut revêtir une portée stratégique et déstabilisatrice ; d'autre part, elle comporte des limites opérationnelles, qui apparaitront probablement au fur et à mesure des nouveaux usages qui en seront faits. L'épisode Ka-Sat ne se résume pas à une innovation technologique : il marque une étape dans la manière dont les outils cyber et électroniques peuvent être pensés comme leviers simultanés de rupture dans la conduite des opérations[322].

3.2.2. Les capacités cyber-électroniques russes : une coordination inédite avec les opérations cinétiques

L'usage combiné des vecteurs cyber-électronique s'observe à plusieurs reprises dans les phases du conflit en cours. Dès le 24 février 2022, l'attaque Ka-Sat a annoncé les débuts d'un recours massif et coordonné aux outils cyber et électronique. Depuis, de nombreux épisodes ont illustré les usages réguliers à cette convergence pour maximiser les effets d'une attaque dans le conflit. Les moyens de GE continuent, sans surprise, d'être utilisés pour des actions de brouillage, de leurrage, déjà analysées précédemment. Les équipements ont été modernisés et sur le champ de bataille, la GE russe a atteint un niveau de maturité opérationnelle rarement égalé. Les systèmes comme le Leer 3 permettent non seulement de perturber les communications GSM, mais aussi de repérer les émetteurs et ainsi de transmettre leurs positions à l'artillerie. D'autres systèmes comme le Borisoglebsk-2 ou le Krasukha-4S[323] étendent ce brouillage aux fréquences tactiques, aux drones, et même aux satellites de reconnaisse. Selon Patrick Smith, le niveau de sophistication tactique atteint

[321] Entretien avec M. Serge Cholley.
[322] Entretien avec M. Serge Cholley.
[323] Yannick Genty-Boudry, « Guerre électronique. Le multiplicateur de force russe », *op.cit.*, 2019, p. 100-102.

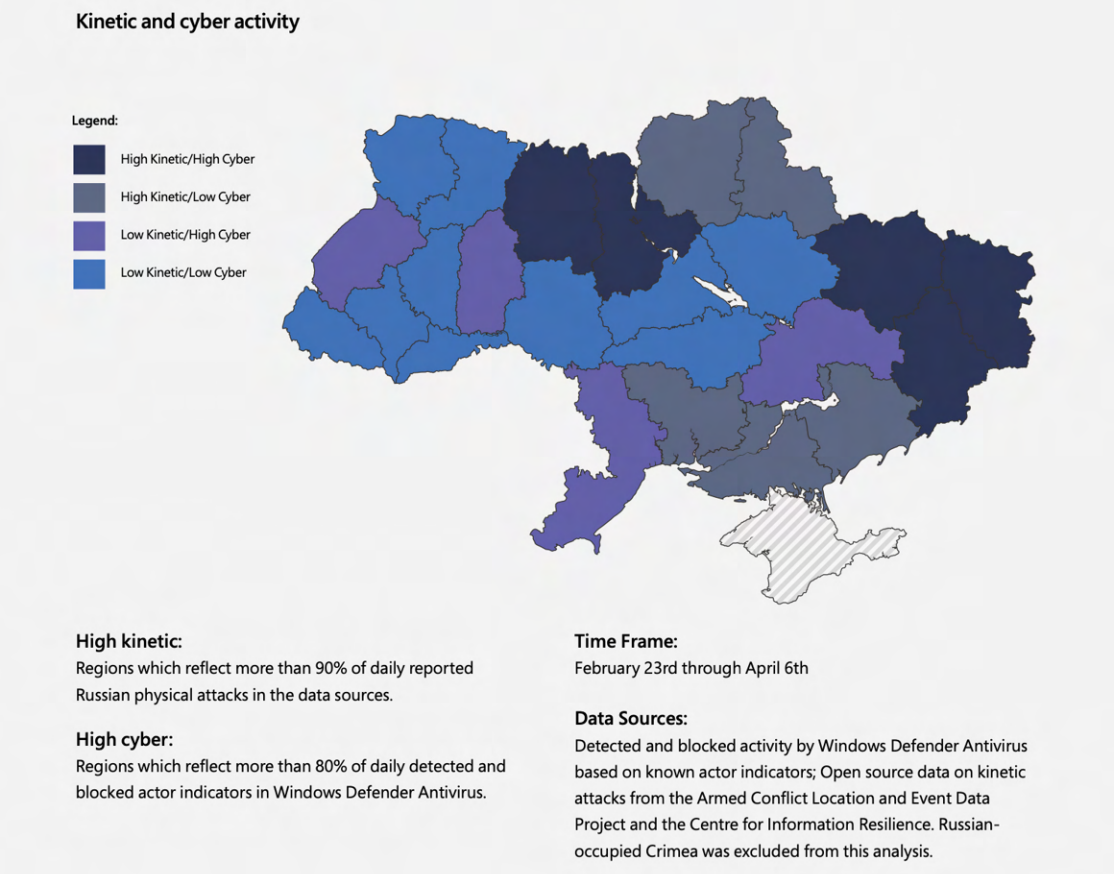
avec le Leer-3 notamment, dépasse les capacités des EC-130 Compass Call américains dans certaines configurations[324]. Yannick Genty-Boudry reconnait également la montée en puissance des systèmes russes par rapport à ceux américains : « Les EC-130 Compass Call, qui font figure de référence en matière de brouillage tactique depuis la campagne de Mossoul, ont été incapacités à plusieurs reprises [par les Russes][325]. » Contrairement à 2008 en Géorgie, la GE est désormais intégrée au niveau tactique et coordonnée aux autres milieux traditionnels. Son emploi dans les régions de Marioupol, Kharkiv ou Kherson confirme cette capacité à brouiller, infiltrer, et désorganiser la chaîne adverse en appui direct de la manœuvre terrestre.

> *Bien équipées, coordonnées, et intégrées aux autres unités de combat, à l'image de l'artillerie ou de la défense aérienne, les entités de guerre électronique sont devenues en quelques années un outsider incontournable dans l'ordre de bataille russe. Un outsider qui, en quelques années, est parvenu à créer la surprise au point d'incapaciter les plates-formes américaines les plus rompues à ce type de menaces[326].*

Au niveau cyber, les données compilées par Microsoft sur les attaques russes depuis février 2022 montrent une intensification de l'emploi des capacités cyber en parallèle immédiat des actions militaires[327]. Ce n'est plus seulement une logique de « shaping » du théâtre avant engagement, en amont de l'offensive terrestre, mais bien une action conjointe et en ce sens, un appui aux opérations cinétiques[328]. Dans de nombreuses régions ciblées par les forces russes, notamment Kyiv, Dnipro, Odessa, Sumy, Microsoft a observé un chevauchement spatial et temporel entre cyberattaques et frappes physiques[329]. Ces actions cyber simultanées se traduisent par l'altération des services publics, des coupures de réseaux, des attaques contre les médias locaux, etc. La carte ci-dessous croise les données cyber, relevées à partir de Windows Defender Antivirus, la composante anti-virus de Microsoft ; et les frappes militaires, répertoriées par Armed Conflict Location & Event Data Project. Cette

[324] Patrick Smith, "Russian Electronic Warfare: A growing threat to U.S. Battlefield Supremacy", *op.cit.*, 2020, p. 3-4.
[325] Yannick Genty-Boudry, « Guerre électronique. Le multiplicateur de force russe », *op.cit.*, 2019, p. 102.
[326] Yannick Genty-Boudry, *ibid.*, p. 102.
[327] Digital Security Unit, "An overview of Russia's cyberattack activity in Ukraine", *Microsoft*, 2022, p. 8.
[328] Anthony Namor, « Les opérations numériques dans les conflits contemporains », *op.cit.*, 2023, p. 239.
[329] Digital Security Unit, "An overview of Russia's cyberattack activity in Ukraine", *op.cit.*, 2022, p. 10.

modélisation montre clairement que les zones de haute intensité cinétique sont très souvent les plus densément visées par des intrusions ou des destructions cyber.

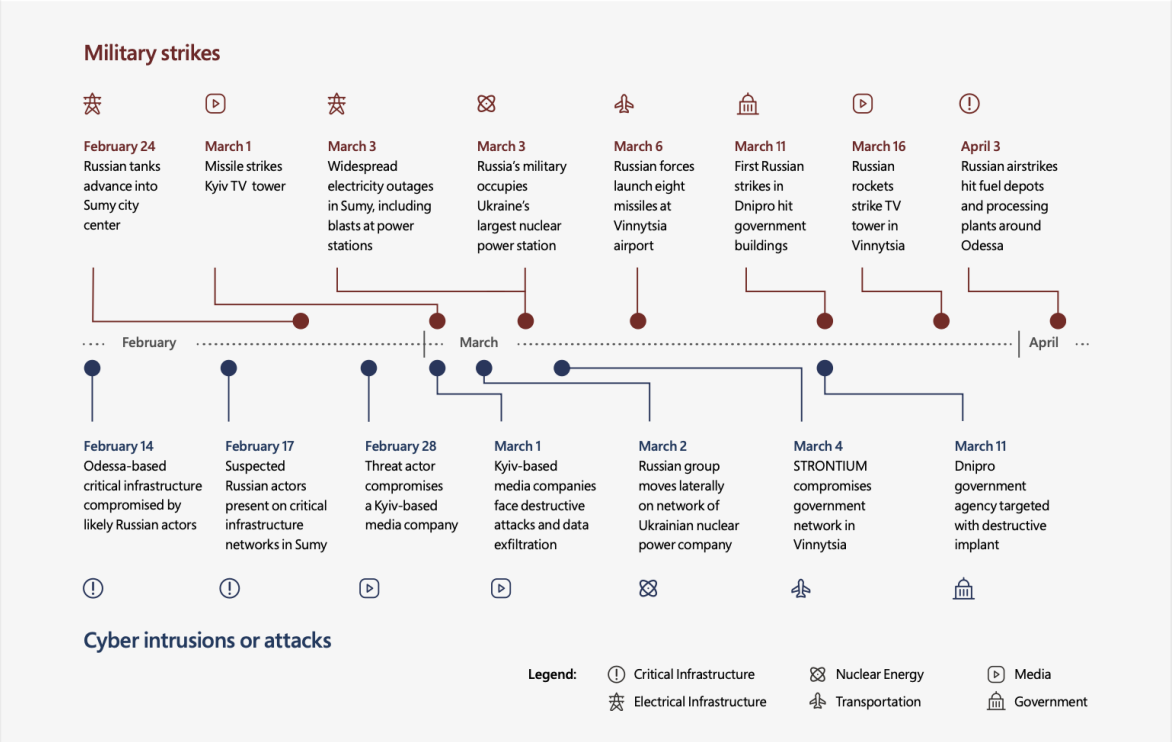


Source : Digital Security Unit, "An overview of Russia's cyberattack activity in Ukraine", *Microsoft*, 2022, pp. 10.

Un exemple particulièrement éclairant de cette convergence cyber-cinétique est l'épisode du 1er mars 2022 sur une chaîne de diffusion ukrainienne. Ce jour-là, une cyberattaque destructrice utilisant le malware DesertBlade est déclenchée contre les systèmes de diffusion, tandis que les forces russes frappent simultanément la tour de télévision de Kiev à l'aide de missiles[330]. Trois jours plus tôt, à Berdyansk, la tour de diffusion avait été occupée physiquement par des troupes russes, afin de couper les signaux localement. De la même manière, plusieurs autres cyberattaques documentées contre des infrastructures à Kiev, Sumi, Dnipro, Odessa, Vinnytsia[331], précèdent de peu, ou accompagnent, des opérations tactiques russes. Le modèle opérationnel qui se dessine est

[330] Digital Security Unit, "An overview of Russia's cyberattack activity in Ukraine", *op.cit.*, 2022, p. 12.
[331] Digital Security Unit, *ibid.*, p. 8.

celui d'un appui simultané aux actions militaires, conçu pour désorganiser le commandement local, ralentir la prise de décision, et saturer la réponse ennemie.



Source : Digital Security Unit, "An overview of Russia's cyberattack activity in Ukraine", *Microsoft*, 2022, pp. 8.

Au-delà des coordinations cyber-cinétique et cinétique-électronique dans les offensives du champ de bataille[332], l'intégration opérationnelle de ces trois vecteurs, cyber, électronique et cinétique, est aussi renforcée par les efforts de centralisation structurelle et technique. De nombreuses unités spécialisées et brigades ont été créés[333], et parmi elles, beaucoup ont été dédiées au cyber et à la GE, notamment au sein du 1084e centre d'entraînement de Tambov[334]. Sur un spectre plus global, un centre de commandement unique, Bylina, a été mis en place pour permettre à chaque brigade de piloter l'ensemble de son dispositif[335]. Ce centre est lui-même connecté au C2 ouvert des bataillons, autrement dit, au système Less. Bylina est ainsi en mesure de centraliser les flux SIGINT, les effets de brouillage, les retours d'intrusion cyber et les données civilo-militaires collectées par les ministères de l'Intérieur, des Télécommunications et de l'Énergie, le FSB ou le FSO. Et la réorganisation russe pour favoriser l'intégration des capacités cyber-électroniques se

[332] Rémy Hémez et Anthony Namor « L'apport des actions cyberélectroniques aux opérations de déception tactiques et opératives », *op.cit.*, 2022, p. 199-209.
[333] Jack Watling, Oleksandr V Danylyuk and Nick Reynolds, "The Threat from russia's Unconventional Warfare Beyond Ukraine, 2022-24", *Royal United Services Institute*, 2024, p. 1-3.
[334] Yannick Genty-Boudry, « Guerre électronique. Le multiplicateur de force russe », *op.cit.*, 2019, p. 100.
[335] Yannick Genty-Boudry, *ibid.*, p. 90.

poursuit. Selon Yannick Genty-Boudry, l'objectif de ce « nouveau système de systèmes » de l'état-major est d'automatiser les processus de traitement les plus chronophages, toujours dans l'objectif de déployer des opérations de déception combinées[336].

Cette synchronisation des services fait émerger un réseau de commandement pensé pour maximiser la coordination des effets tactiques. Il est aussi possible d'y voir une tentative d'institutionnaliser une sorte d'artillerie plus invisible, capable de frapper des fonctions, des systèmes, et non plus seulement des unités. Ce n'est plus seulement une guerre de l'outil, mais une guerre de la chaîne de décision : saturer, brouiller, désinformer, pour neutraliser sans toujours avoir à détruire. C'est en tout cas la perspective russe depuis 2010, connue sous le nom de « New Generation Warfare[337] ». Cette stratégie ne repose plus sur la confrontation directe ou la recherche de la supériorité matérielle, mais sur une logique systémique de désorganisation. Elle combine des moyens militaires conventionnels avec une large panoplie de moyens non militaires, actions cyber, GE, désinformation, instrumentalisation du droit international, coercition économique, dans le but de paralyser l'adversaire par d'autres vecteurs que la bataille frontale[338]. L'un des fondements de cette approche est sa temporalité étendue : le conflit commence bien avant les opérations armées visibles, par des actions de sabotage, d'influence ou d'intrusion numérique, et se poursuit dans un flou stratégique constant, ce qui rend difficile toute riposte symétrique. C'est exactement le mode opératoire adopté par la Russie depuis 2007. Cette forme de guerre, souvent qualifiée de « non linéaire » ou « multidomaine », s'établit sur une convergence méthodique des effets, dans laquelle les sphères cyber et électronique jouent un rôle clé en permettant des attaques simultanées sur les systèmes techniques et cognitifs adverses. Le champ de bataille devient un espace d'effets et de confusion, où le cyber, la GE et l'information se croisent pour affaiblir l'adversaire par-delà les opérations cinétiques[339].

Ainsi, ce que les doctrines anticipaient, les opérations russes depuis 2022 l'ont confirmé : la convergence entre le cyberespace et le spectre électromagnétique est aujourd'hui une réalité opérationnelle, pleinement intégrée aux logiques d'engagement. Le conflit russo-ukrainien

[336] Yannick Genty-Boudry, *ibid.*, p. 100.
[337] James Derleth, "Russian New Generation Warfare: Deterring and Winning the Tactical Fight", *Military Review*, 2020, p. 82-91.
[338] Thibault Fouillet et Bruno Lassalle, « Le concept russe de "guerre nouvelle génération" du Général Gerasimov : quelle exploitation pour l'armée de Terre ? », *Fondation pour la Recherche Stratégique*, note n° 285, 2017, p. 2-10.
[339] Jean-Marc Wasielewski, « L'emploi de la cyber-électronique en Ukraine », *Revue Défense Nationale*, n° 859, 2023, p. 90.

opère un franchissement de seuil : l'articulation ne se cantonne plus aux marges du champ de bataille, mais est désormais pleinement intégrée à la planification et à l'exécution des manœuvres conventionnelles. L'usage coordonné de ces deux vecteurs engendre des effets tangibles, en appui direct des manœuvres militaires, et reconfirme une volonté claire de désorganiser les fonctions vitales adverses. La notion d'articulation ne suffit plus pour décrire la simultanéité et la coordination poussée du cyber et de la GE. Ce couplage ne constitue pas seulement un multiplicateur d'efficacité, mais un changement de nature dans la conduite des opérations, où la guerre ne se joue plus seulement sur les terrains physiques, mais aussi sur les flux, les signaux, et les chaînes de décision. Dans cette priorité tactique de neutralisation des capacités adverses, la combinaison cyber-électronique permet d'ouvrir des brèches décisives. Cette évolution marque un tournant : elle ne renvoie pas à un simple appui technologique, mais à une transformation profonde des modes d'action militaires contemporains.

L'analyse des opérations russes depuis 2007 montre que la convergence entre GE et cyberespace n'est plus une hypothèse théorique, mais une réalité opérationnelle. Cette articulation s'est progressivement incarnée dans les faits, avec des degrés d'intégration croissants selon les contextes. Loin d'être immédiatement efficace ou pleinement maîtrisée, cette convergence a d'abord été expérimentée de manière tâtonnante dans des conflits hybrides. De l'Estonie à l'Ukraine, en passant par la Géorgie, ces épisodes ont constitué autant de laboratoires tactiques qui ont permis à la Russie d'identifier ses vulnérabilités, de corriger ses lacunes, et de perfectionner la coordination de ses moyens. Cette accumulation d'expériences hybrides a rendu possible l'intégration plus aboutie et plus fluide du couple cyber-électronique, jusqu'à sa consécration en 2022 avec l'entrée en guerre de la Russie par le réseau lié au satellite Ka-Sat. Le cas ukrainien, y compris depuis 2014, constitue la démonstration par excellence de cette synergie : les actions menées dans le spectre électromagnétique et dans le cyberespace ne se juxtaposent plus, elles s'articulent et se renforcent, et convergent avec les opérations cinétiques.

Conclusion

Ce mémoire s'est construit autour d'une interrogation centrale : l'émergence du cyberespace dans les conflits contemporains a-t-elle eu un impact sur le paradigme et l'utilisation de la guerre électronique ? Ce questionnement partait d'un double constat : alors que la GE reste un outil central dans l'arsenal des puissances, elle semble avoir été éclipsée dans les discours contemporains par l'omniprésence du cyber. Ce paradoxe, peu exploré par la littérature académique, justifiait d'enquêter sur la réalité de cette marginalisation supposée, et d'en identifier les évolutions réellement liées à l'apparition du cyber. L'analyse menée montre que la GE n'a jamais disparu des pratiques militaires. Ses usages ont certes évolué, mais ces transformations tiennent autant à des dynamiques technologiques, doctrinales, budgétaires ou stratégiques qu'à l'émergence du cyber lui-même. Le cyber a influencé certaines manières d'agir, et a contribué à transformer l'environnement global de la conflictualité, mais il n'a pas remis en cause les fondements ni la pertinence de la GE. Il a plutôt participé, au même titre que d'autres facteurs, à une mise à jour continue de la GE, qui s'opère sans cesse depuis ses débuts. Ce qui s'est affirmé au fil du temps, c'est une coordination croissante entre les effets cyber et électromagnétiques, pensés comme complémentaires dans les opérations. En ce sens, le cyber s'est intégré aux côtés de la GE, sans la supplanter.

Le premier chapitre a permis de comprendre comment la GE s'est construite historiquement, comme une réponse aux mutations technologiques et aux besoins stratégiques de la conflictualité depuis la fin du XIX^{e} siècle. Par l'appropriation progressive du spectre électromagnétique, les armées ont développé des capacités qui structurent encore aujourd'hui l'architecture des opérations. L'arrivée du cyber, loin de rendre obsolète cet outil, a plutôt posé la question de ses fonctions : leurs objets, effets et modes opératoires étant distincts, une fusion n'était ni souhaitable ni techniquement possible. Ce chapitre a de facto mis en évidence que la GE ne pouvait pas être remplacée par le cyber, mais que les deux objets pouvaient en revanche être complémentaires. Cette première mise au point technico-historique a ouvert la voie à une interrogation plus large : pourquoi a-t-on pu croire à un recul de la GE lors de l'arrivée du cyber ? Le deuxième chapitre a montré que cette baisse apparente d'intérêt pour la GE à partir des années 1990 ne relevait pas d'un choix stratégique ou doctrinal, mais de dynamiques externes plus larges : désescalade post-guerre

froide, réorganisations militaires, rationalisation budgétaire. C'est d'ailleurs l'ensemble de ces facteurs qui a conduit à une convergence de fait, davantage que doctrinale, entre GE et cyber. La réaffectation des moyens et des compétences dans un contexte de rationalisation des ressources militaires a favorisé leur rapprochement, sans pour autant les confondre. La convergence s'est ainsi installée dans les structures, les équipements et les compétences, selon une logique de mutualisation progressive plus que d'unification. Ces constats ont apporté des éléments de réponse clés à la question structurante de ce mémoire. Mais l'analyse n'aurait pas été complète sans une vérification empirique et une observation plus concrète de cette convergence cyber-électronique dans les opérations réelles. Le troisième chapitre a ainsi permis d'observer, à travers les conflits récents liés au cas russe, que la convergence entre GE et cyber n'est pas qu'une observation théorique ou une simple dynamique structurelle. L'évolution étudiée sur plus d'une décennie montre un mouvement graduel : d'abord juxtaposées, les actions cyber et électromagnétiques ont fini par être coordonnées dans le temps et dans l'espace, jusqu'à intervenir simultanément aux côtés des opérations cinétiques. Cette synergie traduit une forme de maturité de la convergence cyber-électronique, tangible dans la conduite même des opérations. C'est à partir de ces trois niveaux d'analyse qu'une réponse claire et nuancée a pu être formulée.

Ce mémoire présente plusieurs apports notables. Le premier est son approche originale : traiter la convergence cyber-électronique à travers un regard à la fois historique, globale et empirique. La littérature existante sépare encore souvent les deux objets, ou se contente de les analyser d'un point de vue technique, et/ou appliqué à un cas d'étude isolé. Ce travail a croisé plusieurs temporalités, plusieurs échelles d'analyse et plusieurs types de sources pour construire une analyse solide. Un autre point fort est l'effort de clarification conceptuelle dans un champ où les définitions sont mouvantes et souvent confondues. En mettant en regard les terminologies liées au cyber et à la GE, et en retraçant leur généalogie et leurs logiques propres, ce travail a permis d'éclaircir un vocabulaire stratégique souvent instrumentalisé ou flou, et ainsi d'éviter les confusions. Le deuxième apport majeur est d'avoir articulé des cas d'étude concrets, en les recontextualisant dans les évolutions stratégiques plus larges de cette convergence cyber-électronique. Cela a permis de faire émerger une démonstration fondée sur des exemples réels, loin des généralisations abstraites ou prospectives souvent présentes dans les travaux sur le cyber. Ce travail se distingue également par sa démarche épistémologique : il ne prétend pas produire une théorie générale, mais proposer une analyse ancrée, progressive, vérifiée empiriquement. Il cherche à poser

clairement une question restée implicite dans la littérature, et à y répondre par des faits et des raisonnements. Enfin, le choix d'un traitement transversal permet de mettre en évidence la persistance du paradigme de la GE là où certains discours actent déjà sa disparition.

Ces points forts doivent toutefois être nuancés par des limites méthodologiques et structurelles. La première tient à la fragmentation des sources disponibles. Les publications sur la GE sont souvent datées, techniques ou industrielles ; celles sur le cyber sont nombreuses mais souvent diluées dans des concepts vastes et parfois mal définis. Rares sont les travaux qui abordent frontalement la relation entre les deux champs, et encore plus rares ceux qui la pensent dans la durée. Ensuite, les asymétries entre les deux domaines rendent difficile une comparaison totalement équilibrée : différences d'ancienneté, d'échelle d'action, de visibilité institutionnelle. Il a donc fallu adopter une posture adaptative, multiplier les angles d'entrée, mener des échanges assez techniques et sélectionner des cas concrets pour ensuite faire ressortir des lignes de fond pertinentes et originales. Concernant l'empirie, la rareté des données ouvertes sur les opérations concrètes, due à la sensibilité stratégique des deux domaines, a limité les possibilités d'analyse. Cette opacité a aussi orienté le recours à des sources majoritairement occidentales, en raison de leur accessibilité. Si certaines pratiques d'acteurs non occidentaux ont pu être observées, le traitement analytique demeure en partie structuré par des cadres interprétatifs occidentaux, plus abondamment documentés. Il ne s'agit pas d'une limite choisie, mais plutôt de la conséquence directe d'un déséquilibre structurel dans l'accès et la diffusion des données stratégiques liées au sujet. Enfin, le choix de rester à un niveau d'analyse non technique – pour maintenir l'accessibilité du propos et éviter une sur-spécialisation – pourrait être vu comme une faiblesse pour qui chercherait une modélisation fine de cette convergence. Enfin le phénomène de la convergence cyber-électronique étant en constante évolution, les conclusions restent nécessairement partielles, et sujettes à réactualisation en fonction de l'évolution de cette convergence dans les conflits à venir.

Ce travail pourrait être prolongé dans deux directions. Sur le plan empirique, une analyse comparative entre différents États – les États-Unis, Israël, ou la Chine – permettrait de tester la robustesse des conclusions formulées ici sur d'autres terrains doctrinaux et opérationnels. Sur le plan théorique, il serait fécond de pousser l'analyse en direction d'un troisième niveau de convergence : celui de la guerre cognitive. En effet, la combinaison des effets cyber et électromagnétiques ne vise plus uniquement les systèmes ou les réseaux : elle

tend de plus en plus à viser les représentations mentales, les perceptions, les processus décisionnels. Dans cette perspective, la convergence cyber-électronique devient un vecteur de la guerre informationnelle, voire de la guerre psychologique. Certaines attaques visent à désorienter les esprits autant que les stratégies militaires. Explorer ce déplacement des effets techniques vers les effets cognitifs ouvrirait l'analyse à une nouvelle échelle – celle de la guerre des perceptions – et constituerait une suite logique et nécessaire à cette recherche.

BIBLIOGRAPHIE

Articles scientifiques

Alberto N. Gomez Miguel, “Arming Cyebrspace: The Militarization of a Virtual Domain”, *Global Security and Intelligence Studies*, vol. 1, n° 2, 2016, p. 43.

Aras Harun and Süvari Kahraman, “Unveiling Russia’s secret weapon: cyber-electronic operations in hybrid warfare”, *Journal of Military and Strategic Studies*, vol. 25, n° 1, 2024, p. 1-16.

Arquilla John and Karasik Theodore, “Chechnya: A Glimpse of Future Conflict?”, *Studies in Conflict & Terrorism*, vol. 22, n° 3, 1999, p. 207–229.

Bauer Alain, « La doctrine militaire russe et les leçons à en tirer pour l’Occident », *Les Cahiers de la Revue Défense Nationale*, 24 février-24 août : 6 mois de guerre en Ukraine, 2022, p. 52-61.

Bektas Yakub et Albaret Michèle, « La télégraphie au service du sultan ou le messager impérial », *Réseaux*, vol. 12, n° 67, 1994, p. 143-152.

Bréhat Chapuis Victor, « Aéronautique – L’informatique dans l’Armée de l’air – Coupes et congrès dans l’aéronautique militaire – Le Xe Salon de Hanovre », *Revue Défense Nationale*, n° 335, 1974, p. 162-168.

Cahen Louis, « La télégraphie électrique des origines au début du XXe siècle », *Revue d'histoire des sciences et de leurs applications*, vol. 1, n° 2, 1947, p. 142.

Cazenobe Jean, « Les origines de la télégraphie sans fil », *Cahiers d’Histoire et de Philosophie des Sciences*, vol. 16, n° 15, 1981, p. 35.

Coste Jean-Charles, « De la guerre hybride à l’hybridité cyberélectronique », *Revue Défense Nationale*, vol. 2016/3, n° 788, 2016, p.19-23.

Cox Jacob, Bennett Daniel, Lathrop Scott, Walls Chris, LaClair Jason, Tracy Clint, Esquibel Judy, “The Friction Points, Operational Goals, and Research Opportunities of

Electronic Warfare and Cyber Convergence", *The Cyber Defense Review*, vol. 4, n° 2, 2019, p. 81-83.

David Christophe, « Histoire des Lois de programmation militaire (LPM) », *Les Cahiers de la Revue Défense Nationale*, Au(x) défis de la puissance – Regards du CHEM, 72e session, 2023, p. 198.

Degoulange Jean-Marc, « Verdun sur écoute », *Inflexions*, 2021/2, n° 47, 2021, p.57-61.

Douillet Matthieu, « Opérer en environnement multi-milieux/multi-champs : de la théorie à la formation : Complexité et innovation dans les opérations militaires », *Revue Défense Nationale*, vol. 8, n° 863, 2023, p.74.

Douzet Frédérick. « La géopolitique pour comprendre le cyberespace », *Hérodote*, 2014/1, n° 152-153, 2014, p. 6-7.

Ebert H Hannes and Maurer Tim, "Contested cyberspace and rising powers", *Third World Quarterly*, vol. 34, n° 6, 2013, p. 54-74.

Ellul Jacques, « Wiener (Norbert) - Cybernétique et société. Traduit de l'anglais », *Revue française de science politique*, n°1, 1955, p. 171-172.

Ercan Yilmaz Muzaffer, "Intra-state conflicts in the post-cold war era", *International Journal on World Peace*, vol. 24, n° 4, 2007, p. 11-33.

Faivre Maurice, « Défense en France – Le Plan "Armées 2000" », *Revue Défense Nationale*, n° 502, 1989, p. 177-179.

Fontanel Jacques et Matelly Sylvie, « Le coût des dividendes de la paix », *Mondes en Développement*, vol. 28, n° 112, 2000, p. 2.

Grimaila Michael R., "The Genesis of the NATO Cooperative Cyber Defense Centre of Excellence", *Information Systems Security Association Journal*, vol. 16, n° 8, 2018, p. 21.

Guénec Michel, « La Russie face à l'extension de l'OTAN en Europe », *Hérodote*, 2008/2, n° 129, 2008, p. 221-246.

Haig Zsolt, “Electronic warfare in cyberspace”, *Security and Defence Quarterly*, vol. 2, n° 7, 2015, p. 22-35.

Johnson Darin E.W., “Russian election interference and race-baiting”, *Columbia Journal of Race and Law*, vol. 9, n° 1, 2019.

Kempf Olivier, « Distinguer le cyberespace et l’espace électromagnétique », *Revue Défense Nationale*, 2015/9, n° 784, 2015, p.15-21.

Kennedy Paul M., “Imperial cables communications and strategy, 1870-1914”, *The English Historical Review*, vol. 86, n° 341, 1971, p. 731.

Kostyuk Nadiya and Zhukov Yuri M., “Invisible Digital Front: Can Cyber Attacks Shape Battlefields Events?”, *Journal of Conflict Resolution*, vol. 63, n° 1, 2017, p. 317-347.

Latham Robert, “History, Theory, and International Order: Some Lessons from the Nineteenth Century", *Review of International Studies*, vol. 23, n° 4, 1997, p. 419–443.

Liaropoulos Andrew N., “Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-Stakeholderism, and Power Politics.” *Journal of Information Warfare*, vol. 15, n° 4, 2016, pp. 14–26.

Licklider Joseph C. R., "Man-Computer Symbiosis," in *IRE Transactions on Human Factors in Electronics*, vol. HFE-1, n° 1, 1960, p. 4-11.

Maliarchuk Tamara, Danyk Yuriy and Briggs Chad, “Hybrid Warfare and Cyber Effects in Energy Infrastructure”, *Connections: The Quarterly Journal*, vol.18, n° 2, 2019, p. 97.

Malizard Julien, « Le financement des armées au sortir de la guerre du Golfe et de la guerre froide », *Revue Défense Nationale*, n° 843, 2021, p. 26.

Marangé Céline, « Le nucléaire russe : un instrument de dissuasion et d’intimidation », *Revue Défense Nationale*, n° 802, 2017.

Maurin Anne, « La guerre en Ukraine et le théâtre spatial », *Les Cahiers de la Revue Défense Nationale*, n° 97, 2023, pp. 35.

Mazzucchi Nicolas, « La cyberconflictualité et ses évolutions, effets physiques, effets symboliques », *Revue Défense Nationale*, vol. 821, n° 6, 2019, p. 138-141.

McMahon Robert J., “Decolonization and the Cold War: The Superpowers and the Anti-Colonial Insurgencies in Indonesia and Vietnam”, *Journal of Global Strategic Studies*, vol 3, n°2, 2023, p. 3-19.

Queylar Francis, « La guerre électronique, une réalité majeure (I) », *Revue Défense Nationale*, n° 340, p. 41-55.

Rogalski Michel, « Dépenses militaires et dividendes de la paix », *Revue Défense Nationale*, n°532, p. 126.

Sébastien Vincent, « Qui s’y frotte, s’y pique : une stratégie intégrale pour réduire la subversion cyber », *Revue Défense Nationale*, Hors-série (HS3), 2022, p. 41-57.

Slack Chelsey, “Wired yet disconnected: the governance of international cyber relations”, *Global Policy*, vol. 7, n° 1, 2016, p. 69-78.

Strate Lance, “The Varieties of Cyberspace: Problems in Definition and Delimitation”, *Western Journal of Communication*, vol. 63, n° 3, 1999, p. 382–412.

Tabansky Lior, “Basic Concepts in Cyber Warfare”, *Military and Strategic Affairs*, vol. 3, n° 1, 2011.

Thorez Julien, « Géorgie-Ossétie-Russie. Une guerre à toutes les échelles », *EchoGéo*, 2009.

Thurbon Michael T., “The Origins of Electronic Warfare”, *The RUSI Journal*, vol. 3, n° 122, 1977, p. 58.

Suslov Mikhail, “‘Russian World’ Concept: Post-Soviet Geopolitical Ideology and the Logic of ‘Spheres of Influence’”, *Geopolitics*, vol. 23, n° 2, 2018, p. 330–353.

Veljovski Gjorgji, Taneski Nenad and Dojchinovski Metodija, “The Danger of ‘Hybrid Warfare’ from a Sophisticated Adversary: The Russian ‘Hybridity’ in the Ukrainian Conflict”, *Defense & Security Analysis*, vol. 33, n° 4, 2017, p. 292-307.

Waltz Kenneth N., “The New World Order”, *Journal of International Studies*, vol. 22, n° 2, 1993, p. 189.

Wasielewski Jean-Marc, « L’emploi de la cyber-électronique en Ukraine », *Revue Défense Nationale*, n° 859, 2023, p. 90.

Ouvrages généraux

Betz, David J. and Stevens, Tim, *Cyberspace and the state: toward a strategy for cyber-power*, Londres : Routlegde, 2011, p. 107.

Billois, Gérôme, *Cyberattaques : les dessous d'une menace mondiale*, Paris : Hachette, 2022, p. 19.

Bonnemaison, Aymeric et Dossé, Stéphane, *Attention : Cyber ! : Vers le combat cyber-électronique*, Paris : Economica, 2014.

Browne, J. P. R, and Thurbon, Michael T., *Electronic Warfare*, Washington : Brassey's, 1998.

Gat, Azar, « VII. Les révolutions technologiques dans la guerre, des débuts de l'âge industriel au XXIe siècle », in Jean Baechler et Christian Malis, *Guerre et Technique*, Paris : Hermann, 2018, p.107-119.

Fuller, John F.C., *The Foundations of the Science of War*, Londres : Hutchinson & Co., 1926.

Kahn, David, *Seizing the Enigma: the race to break the German U-Boat cades, 1939-1943*, Barnsley : Frontline Books, 2012, p. 31-48.

Middleton, Bruce, *A history of Cyber security attacks: 1980 to present*, Abingdon-on-Thames : Taylor & Francis Group, s.d., p. 25-64.

Price, Alfred, *The History of US Electronic Warfare*, Alexandria : Association of Old Crows, vol. 1, 1984, p. 41.

Price, Alfred, *Instruments of Darkness: The History of Electronic Warfare, 1939-1945*, Annapolis : Naval Institute Press, 2017, p. 48-51.

Richardson, Doug, *Electronic warfare. A revealing insight into one of the most closely guarded areas of military activity: the clandestine world where threat and countermeasure battle constantly for supremacy*, Londres : Salamander Books Limited, 1985, p. 16-83.

Terrien, Olivier, *Les 36 stratagèmes de la guerre électronique*, Paris : JePublie, 2012, p. 72.

Whipple, Tom, *The Battle of the Beams: The secret science of radar that turned the tide of the Second World War*, New York : Bantam, 2023, p. 19.

Von Clausewitz, Carl, “Chapter II. End and Means in War”, in *On War*, 1832.

Chapitres d’ouvrage

Bezut, Michel, « Turing, Alan », in Moutouh, Hugues et Poirot, Jérôme, *Dictionnaire du renseignement*, Paris : Perrin, 2018, p. 795-798.

Bonifas, Gilbert et Faraut, Martine, « Les liaisons dangereuses (1902-1914) », in *Pouvoir, classes et nation en Grande-Bretagne au XIXe siècle*, Paris : Elsevier Masson, 1992, p.225.

Brun, Olivier, « ROEM », in Moutouh, Hugues et Poirot, Jérôme, *Dictionnaire du renseignement*, Paris : Perrin, 2018, p. 658-661.

Bruns, Alex, “The redundant spy”, in Morgan Jones, Stuart Glover, Amy Barker, Chad Parkhill, Jessica Dennis, Michael Ferguson, Eugénie FitzGerald, Trudi Plaschke, and Lyndal Ross, *A Most Provoking Thing: new writing from QUT*, Brisbane : Creative Industries, DOTLIT, Queensland University Technology, 2004, p. 123-130.

Douzet, Frédérick, « Chapitre 21. Le cyberespace, un champ d’affrontement géopolitique », in Giblin, Béatrice, *Les conflits dans le monde* : *Approche géopolitique*, Paris : Armand Colin, 2016, p. 327-343.

Gomez, Éric, « Focus 2. La guerre électronique », in Marangé, Céline et Quessard, Maud, *Les guerres de l'information à l'ère numérique*, Paris : Presses Universitaires de France, 2021, p.79.

Graham Fry, Michael, “Decolonization”, in The International Politics of Eurasia: The End of Empire? Comparative perspectives on the Soviet Collapse, Londres : Routledge, 1997, p. 34.

Kennan, George F., “Cold War and Decolonization, 1945-1961”, in Richards, Michael D. and Paul R. Waibel, *Twentieth Century Europe: A Brief History, 1900 to the Present*, Oxford : Wiley Blackwell, 2014, p.207-229.

Marnot, Bruno, « Chapitre 8 - Révolution maritime et communications transatlantiques », in *La mondialisation au XIXe siècle (1850-1914)*, Paris : Armand Colin, 2012, p. 213.

Namor, Anthony, « Les opérations numériques dans les conflits contemporains », in Taillat, Stéphane, Cattaruzza, Amaël et Danet, Didier, *La Cyberdéfense : Politique de l'espace numérique*, 2e éd., Paris : Armand Colin, 2023, p. 233-243.

Poirot, Jérôme, « Tour Eiffel », in Moutout, Hugues et Poirot, Jérôme, *Dictionnaire du renseignement*, Paris : Perrin, 2018, p.774-776.

Sarale, Jean-Marc, « La bataille de Tsushima - Discours de presse et déplacements de représentations », in Savelli, Dany, *Les Carnets de l’exotisme 5 : Faits et imaginaires de la guerre russo-japonaise*, Sète : Kailash Éditions, 2005, p. 91-109.

Tzu, Sun, « Article XIII : Le Renseignement », in *L’art de la guerre*, Paris : Milles et une nuits, 1996, n° 122, p. 100.

Articles de presse ou de blog

AGEAT, « Le suivi de la Bataille de la Marne par les écoutes secrètes françaises - journée du 8 septembre 1914 », *Association de la guerre électronique de l’armée de terre*, 8 septembre 2013 (https://www.ageat.asso.fr/spip.php?article130).

Airforce Technology, “The Israeli ‘E-tack’ on Syria – Part I”, *Airforce Technology*, 9 mars 2008 (https://www.airforce-technology.com/features/feature1625/).

Alfred, Randy, “March 10, 1876: 'Mr. Watson, Come Here ...”, *Wired*, 10 mars 2008 (https://www.wired.com/2008/03/dayintech-0310/).

AviationsMilitaires.net, « Douglas DC-8 SARIGuE » (https://aviationsmilitaires.net/v3/kb/aircraft/show/12508/douglas-dc-8-sarigue).

Bembaron, Elsa, « 6 000 éoliennes allemandes touchées par une cyberattaque russe », *Le Figaro*, 3 mars 2022 (https://www.lefigaro.fr/secteur/high-tech/6000-eoliennes-allemandes-touchees-par-une-cyberattaque-russe-20220302).

Berthet, Bruno, « La guerre électronique en ébullition », *Le Magazine des ingénieurs de l'Armement CAIA*, n° 132, 16 juin 2024 (https://www.caia.net/revue-auteurs-rubriques-numeros/article/la-guerre-electronique-en-e-bullition/1407).

Davis, Joshua, "Hackers take down the most wired country in Europe", *Wired*, 21 août 2007 (https://www.wired.com/2007/08/ff-estonia/).

Elwes, Jay, "How the third world war was narrowly averted ", *The Spectator*, 8 mai 2021 (https://www.spectator.co.uk/article/how-the-third-world-war-was-narrowly-averted/).

Europe 1, « Ukraine : "La guerre a commencé dans l'espace", declare le Général Michel Friedling, *Europe 1*, 25 juin 2022 (https://www.europe1.fr/international/ukraine-la-guerre-a-commence-dans-lespace-declare-le-general-michel-friedling-4119684).

« Histoire de la machine Enigma », Cryptographie et codes secrets, *Bibmath*, (https://www.bibmath.net/crypto/index.php?action=affiche&quoi=debvingt/enigmaguerre).

Hollis, David, "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, 1er juin 2011 (https://smallwarsjournal.com/2011/01/06/cyberwar-case-study-georgia-2008/).

Greenberg, Andy, "The Untold Story of NotPetya, the most devastating cyberattack in history", *Wired*, 22 août 2018 (https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/).

Kaspersky, « Qu'est-ce qu'une attaque zero-day ? », *Kasperky*, s.d. (https://www.kaspersky.fr/resource-center/definitions/zero-day-exploit).

Lagneau, Laurent, « L'US Air Force envoie un avion de guerre électronique EC-130H "Compass Call" en Pologne », *Opex360.com*, 9 juin 2019 (https://www.opex360.com/2019/06/09/lus-air-force-envoie-un-avion-de-guerre-electronique-ec-130h-compass-call-en-pologne/).

Landler, Mark and Markoff, John, “Digital fears emerge after data siege in Estonia”, *The New York Times*, 29 mai 2007 (https://www.nytimes.com/2007/05/29/technology/29estonia.html).

Le Monde avec AP, AFP et Reuters, « Le président destitué, Timochenko libérée : l’Ukraine bascule », *Le Monde*, 22 février 2014 (https://www.lemonde.fr/europe/article/2014/02/22/proche-de-ianoukovitch-le-president-du-parlement-ukrainien-demissionne_4371588_3214.html).

MacIsaac, David, “Through World War II: Air warfare”, *The Editors of Encyclopaedia Britannica* (https://www.britannica.com/topic/air-warfare).

Mannes, Aaron and Hendler, James, “The First Modern Cyberwarfare?”, *The Guardian*, 22 août 2008 (https://www.theguardian.com/commentisfree/2008/aug/22/russia.georgia1).

Matishak, Martin, “Western powers blame Russia for Ukraine satellite hack”, *The Record*, 10 mai 2022 (https://therecord.media/eu-uk-blame-russia-for-ukraine-satellite-hack).

Namor, Anthony, « Le combat cyberélectronique russe en Ukraine », *Le Rubicon*, 8 juillet 2022 (https://lerubicon.org/le-combat-cyberelectronique-russe-en-ukraine/).

Noé, Jean-Baptiste, « Qui va toucher les dividendes de la paix ? Entretien Charles Million », *Revue Conflits*, 2 mai 2023 (https://www.revueconflits.com/qui-va-toucher-les-dividendes-de-la-paix-entretien-charles-millon/).

Nova, “5 Little-Known Facts About the Eiffel Tower”, *NOVA Tech + Engineering*, 15 juillet 2024 (https://www.pbs.org/wgbh/nova/article/5-little-known-facts-about-the-eiffel-tower/).

Philippe, Julie, « Poutine, l’homme qui veut ressusciter l’URSS, à tout prix », *Public Sénat*, 15 décembre 2016 (https://www.publicsenat.fr/actualites/non-classe/poutine-l-homme-qui-veut-ressusciter-l-urss-a-tout-prix-51713)

Schneider, Frédérique, « IMSI-Catcher, ou comment les téléphones portables sont écoutés », *La Croix*, 3 février 2016 (https://www.la-croix.com/Sciences/Numerique/IMSI-Catcher-comment-telephones-portables-sont-ecoutes-2016-02-03-1200737352).

Shimomura, Tsutomu, “Catching Kevin”, *Wired*, 1er février 1996 (https://www.wired.com/1996/02/catching/).

Tervé, Claire, « Guerre en Ukraine : à Kiev, la tour de télévision détruite par une frappe russe », *HuffingtonPost*, 1er mars 2022 (https://www.huffingtonpost.fr/international/article/guerre-en-ukraine-a-kiev-la-tour-de-television-detruite-par-une-frappe-russe_193237.html).

Thomson, Iain, “Russia 'hired botnets' for Estonia cyber-war”, *ITnews*, 1er juin 2007 (https://www.itnews.com.au/news/russia-hired-botnets-for-estonia-cyber-war-82600).

Ukrinform, « La CEC a achevé l’inscription des observateurs étrangers à l’élection présidentielle en Ukraine », *Ukrinform*, 26 mars 2019 (https://www.ukrinform.fr/rubric-elections/2667355-la-cec-a-acheve-linscription-des-observateurs-etrangers-a-lelection-presidentielle-en-ukraine.html).

Untersinger, Martin, « Que sont les IMSI-catchers, ces valises qui espionnent les téléphones portables ? », *Le Monde*, 31 mars 2015 (https://www.lemonde.fr/pixels/article/2015/03/31/que-sont-les-imsi-catchers-ces-valises-qui-espionnent-les-telephones-portables_4605827_4408996.html).

Untersinger, Martin, « Guerre en Ukraine : la Russie accusée d’être derrière la cyberattaque ayant visé le réseau du satellite KA-SAT », *Le Monde*, 10 mai 2022 (https://www.lemonde.fr/pixels/article/2022/05/10/guerre-en-ukraine-la-russie-accusee-d-etre-derriere-la-cyberattaque-ayant-vise-le-reseau-du-satellite-ka-sat_6125513_4408996.html).

Vaizand, Émile, « Comprendre l’impénétrable modèle de la doctrine militaire russe », *Slate*, 14 mars 2024 (https://www.slate.fr/story/266136/guerre-hybride-russie-poutine-guerassimov-doctrine-strategie-militaire-renseignement-armee-ukraine-occident).

Vitard, Alice, « Le satellite KA-SAT aurait dysfonctionné à cause d’une cyberattaque », *L’Usine Digitale*, 4 mars 2022 (https://www.usine-digitale.fr/article/le-satellite-ka-sat-aurait-dysfonctionne-a-cause-d-une-cyberattaque.N1791052).

Sources institutionnelles

Arbaretier, Vincent, *Les écoutes de la Victoire, Général (2S) Jean-Marc Degoulange, Éditions Pierre de Taillac, 2019, 255 pages*, Paris : Revue Historique des Armées, 2019/4, n° 297, 2019, p.139-140.

Armistead, Thomas and Armistead, Leigh, *A new Frontier in war: Cyber Warfare in Estonia*, Kruger National Park : NATO CCDCOE, 2015. 10th International Conference on Cyber Warfare and Security, p. 10.

Badsey, Stephen, *An overview of the Falklands War: politics, strategy and operations*, Tokyo : National Institute of Defense Studies (NIDS), 2011, p. 161.

Baratault, Pierre, « La recherche en guerre électronique et ses retombées depuis 1960 », in *La Guerre électronique en France au XXe siècle*, Paris : Centre d'études d'histoire de la Défense, 2002. Actes du colloque organisé le 20 avril 2000 à l'École militaire, p. 97-116.

Bigelow, Brad, *The Topography of Cyberspace and Its Consequences for Operations*. Tallin : NATO CCDCOE, 2018. 10th International Conference on Cyber Conflict.

Cebrowski, Arthur K. and Garstka, John H., "Network-Centric Warfare: Its Origin and Future", *US Naval Institute Proceedings*, 1998.

Daniel, Jean-Marc, « Finances publiques : les dividendes de la paix ? », *Observations et diagnostiques économiques (Observatoire français des conjonctures économiques)*, n° 47, 1993, p. 91.

Degoulange, Jean-Marc, « La tour Eiffel : premier système de guerre électronique », *Revue Historique des Armées*, 2017/3, n° 288, 2017, p.112.

Department of Defense, *Summary of the Joint All-Domain Command & Control* (JADC2), p. 3-5.

Doctrine interarmées – 3.6, La guerre électronique (GUERELEC), Paris : CICDE, EMA, ministère de la Défense, n°1522/DEF/EMA/EMP.1/NP, 2008.

Eldebek, Amer, « Le cyber en Israël : quelle stratégie ? », in *Réflexions sur le cyber : quels enjeux ?*. Paris : Centre d'études stratégiques aérospatiales, IRSEM, n°32, 2015, p. 137.

Faivre, Maurice, *Le plan Challe*, Paris : Revue Historique des Armées, n° 238, 2005, p. 108-117.

Giles, Keir, *"Information Troops" – a Russian Cyber Command?* Tallin : NATO CCDCOE, 2011. 3rd International Conference on Cyber Conflict.

Gillyboeuf, Jean-Paul, « Guerre de l'information », in *La Guerre électronique en France au XXe siècle*, Paris : Centre d'études d'histoire de la Défense, 2002. Actes du colloque organisé le 20 avril 2000 à l'École militaire, p. 153-154.

Jaitner, Margarita and Mattson, Peter A., *Russian Information Warfare of 2014*, Tallin : NATO CCDCOE, 2015. 7th International Conference on Cyber Conflict, p. 45.

Karim Baram, Abdul, *Technology in Warfare: the Electronic Dimension*, Abou Dabi : The Emirates Center for Strategic Studies and Research, 2008, p. 16.

Knight, Malcolm, Loayza, Norman and Villanueva, Delano, "The Peace Dividend: Military Spending Cuts and Economic Growth", *IMF Economic Review*, vol. 43, 1996, p. 1-37.

Murray, Williamson, "Thinking About Revolutions in Military Affairs", *Joint Forces Quarterly*, n°16, 1997, p. 69-76.

National Security Agency, *Amendment no. 4 to the Appendices to the UKUSA Agreement (third edition)*, Maryland : National Security Agency, 1955. Archives en sources ouvertes.

National Security Agency, *Civil War Signals: Ominous music and drum beat*. Maryland : NSA, s.d.

NATO website, « Electromagnetic Warfare », 2023.

OSCE, *Presidential Elections, 31 March and 21 April 2019*, OSCE Office for Democratic Institutions and Human Rights, s.d.

OTAN, *Communiqué du Sommet de Varsovie*, Varsovie : réunion du Conseil de l'Atlantique Nord des 8 et 9 juillet 2016, Alinéa 7.

Ottis, Rain, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Tallin : NATO CCD COE, 2018, p. 2-4.

Ouali-Djerbi, Samir, « Guerre électronique et combat dans le cyber espace : quelle complémentarité ? », in *Réflexions sur le cyber : quels enjeux ?*. Paris : Centre d'études stratégiques aérospatiales, IRSEM, n°32, 2015, p. 83.

Poirier, Clémence, *The War in Ukraine from a Space Cybersecurity Perspective*, Vienna : European Space Policy Institute, 2022. ESPI Report 84.

Ribadeau-Dumas, Louis, « La guerre électronique en 1914-1918 : deux faits marquants », in *La Guerre électronique en France au XXe siècle*, Paris : Centre d'études d'histoire de la Défense, 2002. Actes du colloque organisé le 20 avril 2000 à l'École militaire, p. 15-17.

Siffre, Jean-Paul, « La conquête du spectre des fréquences électromagnétiques et son utilisation en guerre électronique », in *La Guerre électronique en France au XXe siècle*, Paris : Centre d'études d'histoire de la Défense, 2002. Actes du colloque organisé le 20 avril 2000 à l'École militaire, p. 10.

Singh, Mohinder, *Electronic Warfare*, New Delhi : Popular Science & Technology Series (DESIDOC), 1988, p. 11-13.

The United States Army War College, *A Return to Information Warfare*, U.S. Army Heritage and Education center, p. 2-3.

Tikk, Eneken, Kaska, Kadri and Vihul, Liis, *International cyber incidents: Legal Considerations. Estonia 2007*, Tallin : NATO CCD COE, 2010, p. 14.

Wright, Steve, *An Appraisal of Technologies of Political Control: Interim Study*, Luxembourg : European Parliament, 1998. Scientific and technological options assessment p. 19-20.

Littérature grise

Ablon, Lillian, Binnendijk, Anika, Hodgson, Quentin E., Lilly, Bilyana, Romanosky, Sasha, Senty, David, Thompson, Julia A., *Operationalizing Cyberspace as a Military Domain: Lessons for NATO.* Santa Monica : RAND Corporation, 2019.

Antoine, Pierre-Alain, « De la nécessité de développer la Guerre Électronique sous toutes ses formes pour l'armée de l'Air et de l'Espace », *Athéna-Défense*, 2023, p. 2.

Aubert, Jean-Pierre, Bruggeman, Frédéric et Carli, Jean-Pierre, « Les Restuctuations de défense : Un modèle pour l'industrie ? », *Le Journal de l'École de Paris du management*, vol. 3, n° 65, 2007, p.30-36.

Conseil des ministres, « Plan "Armées 2000" », *Vie publique*, 26 juillet 1989 (https://www.vie-publique.fr/discours/154657-conseil-des-ministres-du-26-juillet-1989-le-plan-armees-2000).

Derleth, James, "Russian New Generation Warfare: Deterring and Winning the Tactical Fight", *Military Review*, 2020, p. 82-91.

Digital Security Unit, "An overview of Russia's cyberattack activity in Ukraine", *Microsoft*, 2022, p. 8.

Dossé, Stéphane et Guerry, Joffrey, "Combat dans le cyberespace : la bataille des câbles au XXIe siècle ?", *Défense et Sécurité Internationale*, n° 74, 2011, p. 54–55.

Dujardin, Olivier, « Guerre électronique : la guerre qu'il ne faut (surtout) pas perdre ! », *Centre français de Recherche sur le Renseignement*, note n° 35, 2021, p. 8.

Dujardin, Olivier, « La guerre électronique dans les conflits aujourd'hui », *Institut d'Études de Géopolitique Appliquée*, 2021.

Duval, Jean-Yves, « La NSA et le réseau ÉCHELON », *Diplomatie*, n° 5, 2003, p. 51-54.

Fouillet, Thibault et Lassalle, Bruno, « Le concept russe de "guerre nouvelle génération" du Général Gerasimov : quelle exploitation pour l'armée de Terre ? », *Fondation pour la Recherche Stratégique*, note n° 285, 2017, p. 2-10.

Genty-Boudry, Yannick, « Guerre électronique. Le multiplicateur de force russe », *Défense et Sécurité Internationale*, n° 143, 2019, p. 98.

Gerasimov, Valery, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Industrial Kurier*, 2013.

Givens, Austen, "Putin's Cyber Strategy in Syria: Are Electronic Attacks Next?", *The Cyber Defense Review*, 2015.

Goya, Michel, « Comment neutraliser un pays sans le dire », *Défense et Sécurité Internationale*, n° 144, 2019, p. 68-71.

Grant, P. M. and Collins, J. H., "Introduction to electronic warfare", *The Institution of Engineering and Technology Proceedings*, vol. 129, n° 3, 1982.

Gros, Philippe, Tourret, Vincent, Mazzucchi, Nicolas, Fouillet, Thibault et Wohrer, Paul, « Intégration multimilieux / multichamps : enjeux, opportunités et risques à horizon 2035 », *Fondation pour la recherche stratégique*, Rapport n°35/FRS/M2MC, 2022, p. 108-110.

Guillet, Romain, « S'adapter sans improviser : les enjeux de transformation organisationnelle », *Revue Défense Nationale*, Hors-série n° 15, 2024, p. 253-267.

Hémez, Rémy et Namor, Anthony, « L'apport des actions cyberélectroniques aux opérations de déception tactiques et opératives », *Stratégique*, vol. 128, n° 1, 2022, p. 200.

James, J. R., "Magical microwaves: the exploitation of the century", *The Institution of Engineering and Technology Proceedings*, vol. 136, n° 1, 1989.

Kempf, Olivier, « Cyber et surprise stratégique », *Stratégique*, vol. 106, n° 2, 2014, p. 111-123.

Kempf, Olivier, « Du cyber et de la guerre », *Fondation pour la Recherche Stratégique*, note n°17/19, 2019, p. 5-7.

Kerttunen, Mika, Schuck, Kim N., and Hemmelskamp, Jonas, *Major Cyber Incident: KA-SAT 9A*, European Repository of Cyber Incidents, 2023, p. 1-3.

Kjellén, Jonas, “Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces”, *Swedish Defence Research Agency*, 2018, p. 51.

Kuzio, Taras, “Euromaidan Revolution, Crimea and Russia–Ukraine War: Why It Is Time for a Review of Ukrainian–Russian Studies”, *Eurasian Geography and Economics*, vol. 59, n° 3, 2018, p. 529–553.

Letertre, Olivier, Justel, Patrick, Lechâble, Romain et Dossé, Stéphane, « Regards croisés sur la guerre électronique », *IFRI*, Focus stratégique 90, 2019, p. 9.

Libicki, Martin C., *Cyber deterrence and Cyberwar*, Santa Monica : RAND Corporation, 2009.

Luiggi, Jean-Sun, « Cyberguerre, nouveau visage de la guerre ? », *Stratégique*, vol. 2, n° 112, 2016, p. 91-100.

Marshall, Andrew W., “Some thoughts on Military Revolutions – Second version”, *Office of the Net assessment*, Memorandum for the record, 1993, p. 3.

Maurer, Tim and Janz, Scott, “The Russia-Ukraine Conflict; Cyber and Information Warfare in a Regional Context”, *International relations and Security Networks ETH Zurich*, 2014, p. 33.

Mirman, I. R., “Electronic Warfare”, *National Defense Industrial Association*, vol. 53, n° 291, 1968, p. 297–301.

Peters, Anne, “The Crimean vote of March 2014 as an abuse of the institution of the territorial referendum”, *Max Planck Institute for Comparative Public Law and International Law*, 2014, p. 256.

Perspective Monde, “Tenue d’un référendum en Crimée », *Perspective Monde*, 2014.

Ramm, Aleksei, “The Russian Army: Organization and Modernization”, *CAN National Security Analysis*, 2019, p. 8.

Sanchez Medero, Gema, « Cyber-crime, cyber-terrorisme et cyber-guerre : les nouveaux défis du XXIe siècle », *Revista Cenipec*, n° 31, 2012.

Seskuria, Natia, “Russia’s ‘Hybrid Aggression’ against Georgia: The Use of Local and External Tools”, *Center for Strategic and International Studies*, 2021, p. 2-4.

Slowik, Joe, “Reviewing the 2022 Ka-Sat incident & implications for distributed communication environments”, *Virus Bulletin*, 2024, p. 7-8.

Smith, Patrick, “Russian Electronic Warfare: A growing threat to U.S. Battlefield Supremacy”, *American Security Project*, 2020, p. 3-5.

Sur, Serge, « Analyse, interprétation et conséquences des évènements militaires en Géorgie », *Centre Thucydide*, Cahier Thucydide n° 9, 2010, p. 18-21.

Thompson, Matt, “Blurring the Lines: The Overlap between cyber and electronic warfare”, *The Journal of Electromagnetic Dominance*, 2023.

Tisseyre, Didier, « Le cyberspace, nouveau théâtre de conflits », *L’ENA hors les murs*, vol. 504, n° 3, 2021, p. 40-42.

Tremblay, Étienne, « La guerre “non-linéaire” russe appliquée en Ukraine analysée à travers la guerre « hors limites » chinoise" », *Canadian Forces College*, Exercise Solo Flight, 2016.

Van Niekerk, B., and Maharaj, M., “The Future Roles of Electronic Warfare in the Information Warfare Spectrum”, *Journal of Information Warfare*, vol. 8, n° 3, 2009, p. 1–13.

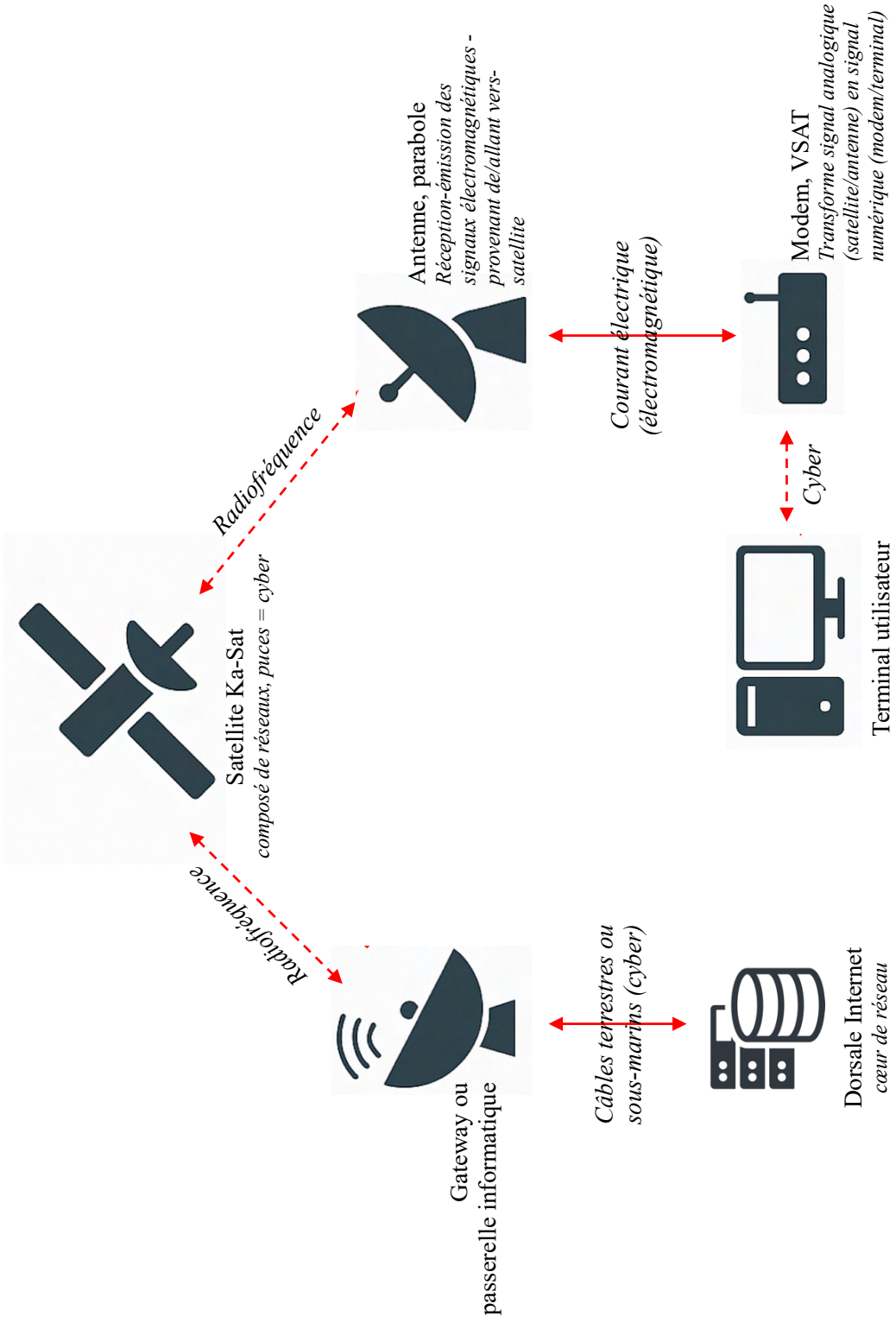
Warden, John, “The Enemy as a system”, *Airpower Journal*, vol. 9, n° 1, 1995, p. 40-55.

Watling, Jack, Danylyuk, Oleksandr V., and Reynolds, Nick, “The Threat from russia’s Unconventional Warfare Beyond Ukraine, 2022-24”, *Royal United Services Institute*, 2024.

Watts, Barry D., “The maturing Revolution in Military Affairs”, *Center for Strategic and Budgetary Assessments*, 2011, p.2.

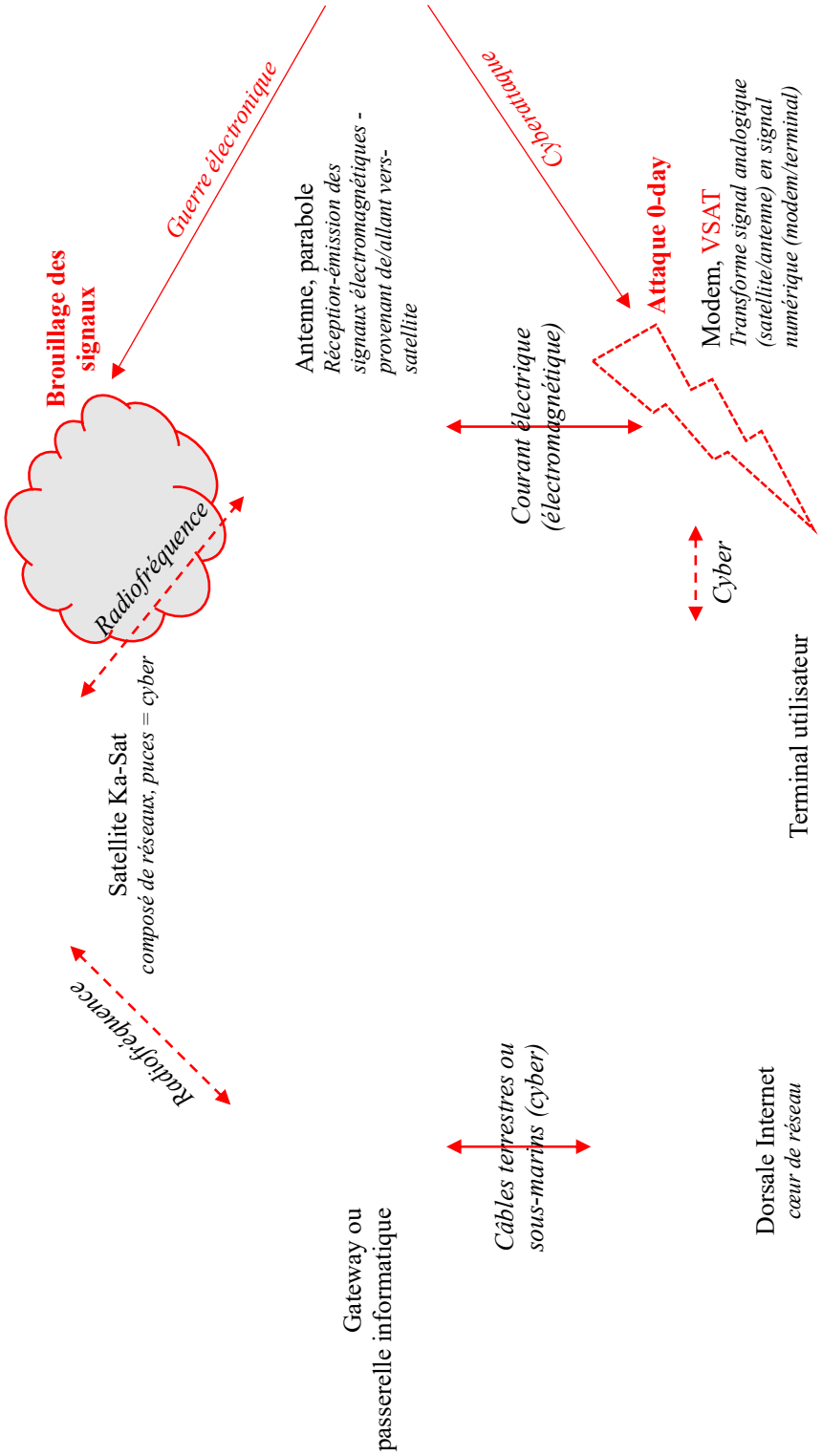
ANNEXES

Annexe 1. Modélisation du fonctionnement du réseau satellitaire Ka-Sat, en temps normal.



Source : schématisation personnelle effectuée à partir de l'entretien conduit avec M. Serge Cholley.

Annexe 2. Modélisation de la cyberattaque sur le réseau satellitaire Ka-Sat, dans la nuit du 23 au 24 février 2022.



Source : schématisation personnelle effectuée à partir de l'entretien conduit avec M. Serge Cholley.

TABLE DES MATIÈRES