N° 2507

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 18 février 2026

# RAPPORT D'INFORMATION

DÉPOSÉ

*en application de l'article 145 du Règlement*

PAR LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES

en conclusion des travaux d'une mission d'information

*sur le thème de* ***« la guerre électronique »***

ET PRÉSENTÉ PAR

MM. DIDIER LEMAIRE ET THIERRY TESSON

Députés

**SOMMAIRE**

___

Pages

# INTRODUCTION

Lorsque Katherine Maxwell explorait avec son mari James la décomposition des ondes lumineuses à l'aide de boîtes ressemblant, selon l'expression de leurs amis, à des cercueils, elle était loin de penser que ces recherches allaient déboucher sur une des découvertes les plus déterminantes du XIX$^{ème}$ siècle : l'existence de champs magnétiques qui se propagent dans l'espace à la vitesse de la lumière sous la forme d'une onde.

Elle aurait été encore plus étonnée de savoir que ce prodige physique, de mieux en mieux compris et maîtrisé après les travaux pionniers du couple, aurait de nombreuses applications pratiques, devenues plus d'un siècle plus tard quasi- universelles.

**Accélérateur connu d'innovations technologiques, le monde militaire a très rapidement pris sa part dans l'usage du spectre électromagnétique**, comprenant qu'il surpassait définitivement le son du canon ou l'envoi d'estafettes comme moyens de coordination des troupes à toutes les échelles de manœuvre.

**Cet envoi d'un signal entre un émetteur et un récepteur en s'affranchissant des distances, donnait en effet à celui qui le maîtrisait un avantage certain sur l'adversaire ne le possédant pas**. Caractéristique foncière de la guerre électronique, cette asymétrie, autre version de la théorie « du glaive et du bouclier », garde aujourd'hui toute sa validité, comme le montre le foisonnement d'innovations techniques qui n'ont pas cessé depuis les origines, de la télégraphie sans fil (TSF) au radar en passant par les satellites.

**Très tôt, la guerre électronique (GE) s'est structurée en trois grands volets.**

**Le premier, lié aux communications qui ont été la première utilisation militaire du spectre, est celui du renseignement d'origine électromagnétique** (ROEM) basé sur l'interception et l'analyse d'émissions adverses (radios, radars, télécommunications).

Désigné sous le terme anglais de « *signals intelligence* » (SIGINT), **le ROEM se décline en deux composantes, « *l'electronic intelligence* » (ELINT) et le « *communication intelligence* » (COMINT).**

L'ELINT concerne l'exploitation des signaux électroniques émis par les radars, missiles, systèmes de guidage ou aéronefs. L'analyse de leurs caractéristiques physiques (fréquence, forme d'onde, durée ou impulsion) permet d'identifier les

équipements, de reconnaître leur « signature électromagnétique » et d'en estimer les performances. Ces informations sont répertoriées au sein de « bibliothèques », dont les mises à jour sont essentielles dans le maintien des capacités d'une armée à ternir tête à un compétiteur sur le champ électromagnétique.

Le COMINT porte, quant à lui, sur l'interception des communications humaines, qu'elles soient vocales ou sous forme de données. Même lorsque les contenus sont chiffrés ou inintelligibles, l'analyse des flux de communication (volume, rythme, localisation) fournit des renseignements exploitables, notamment pour suivre les réseaux adverses, détecter des mouvements ou localiser des postes de commandement.

**Le second volet est celui de la GE offensive qui repose sur des attaques ou des contre-mesures électroniques visant à dégrader, neutraliser ou détruire la capacité de l'adversaire d'exploiter le spectre par deux modes d'action : le brouillage et le leurrage.**

Le premier vise à saturer une bande de fréquences en émettant une énergie plus puissante que celle de l'émetteur ennemi, empêchant ainsi la transmission ou l'exploitation. La forme la plus simple, celle « du bruit » qui sature le récepteur adverse, est moins performante que la perturbation ciblée d'un type de liaison, certes plus complexe à mettre en œuvre, mais plus efficace car limitant les émissions inutiles et le risque de détection.

Le leurrage trompe les capteurs ou les systèmes en se substituant à l'émetteur ennemi. Concrètement, il peut s'agir de générer de faux échos radar imitant la signature d'un aéronef ou d'un missile, afin d'induire l'adversaire en erreur sur la nature, la position ou le nombre de menaces réelles. On vise moins à bloquer le système adverse qu'à l'amener à prendre une mauvaise décision, ainsi en le poussant à tourner ses moyens de défense vers une cible inexistante.

**Le troisième et dernier volet, défensif, repose sur la protection contre les actions électromagnétiques adverses pour préserver la liberté d'action des forces en leur réservant l'usage du spectre.**

Cette stratégie, qui s'appuie sur des techniques de résilience des systèmes face aux attaques de brouillage ou de leurrage, prend la forme de plans rigoureux d'utilisation des fréquences, d'application de procédures de silence radio ou radar, de durcissement des systèmes ainsi que des chiffrements robustes des transmissions.

Elles peuvent aussi s'appuyer sur des techniques alternatives, comme les centrales à inertie ou les transmissions filaires, toutes deux inaccessibles à la détection ou l'interception et assurant de fait la poursuite d'une mission initiée par une onde électromagnétique.

**La guerre électronique demeure un domaine peu connu du grand public. Cette relative invisibilité tient sans doute d'abord à une technicité qui résiste parfois à l'analyse, comme à la sensibilité des informations qui s'y rapportent.** Ses liens avec le monde du renseignement n'ont pas, effectivement, à être démontrés.

Cette discrétion médiatique s'accompagne ensuite d'une évidente ambiguïté terminologique. La « guerre électronique » n'est pas une « guerre électrique » mais bien celle du « champ électromagnétique » où se propagent les ondes hertziennes.

Si un accord existe sur les principes fondamentaux de la « GE », les limites de son champ d'action diffèrent en fonction des approches opérationnelles, industrielles ou scientifiques, créant une zone grise souvent définie par des besoins propres à chaque organisation.

**Pour autant, dans un souci de clarté, vos rapporteurs ont retenu la définition du ministère des armées : la « *guerre électronique est l'action militaire qui exploite l'énergie électromagnétique pour fournir une appréciation de situation opérationnelle et délivrer des effets offensifs ou défensifs* ».**

De fait, la proximité grandissante avec la « cyberdéfense » qui s'accentue au cœur de conflits aujourd'hui de plus en plus hybrides, interroge l'étanchéité du concept de guerre électronique, soumis par ailleurs à l'influence d'innovations techniques incessantes.

**Les opérations militaires se déroulent désormais dans un environnement de plus en plus numérisé et interconnecté.** En effet, les systèmes d'armes, les réseaux d'information, les moyens de commandement, les navigations par satellite, les drones, reposent tous sur l'exploitation du spectre électromagnétique. Or, il est certain que ce dernier sera durablement impacté par les grandes révolutions techniques qui s'annoncent : l'apparition massive de l'intelligence artificielle bientôt suivie par les nombreuses applications issues de la physique quantique.

Le présent rapport s'attachera, dans une première partie, à dresser un panorama historique et conceptuel de la guerre dans le champ électromagnétique, de ses origines jusqu'aux défis les plus contemporains.

Il analysera, dans une seconde partie, la situation de nos forces de guerre électronique, pour formuler diverses recommandations quant à leur souhaitable évolution face aux défis que posent aujourd'hui les déséquilibres géopolitiques.

## I. APRÈS DES DÉCENNIES D'ATONIE, LA GUERRE ÉLECTRONIQUE REVIENT AU CŒUR DES CONFLITS CONTEMPORAINS

La guerre électronique (GE) redevient un facteur structurant des conflits modernes. Si elle ne suffit pas à elle seule pour gagner un conflit, en être privé revient à offrir à l'adversaire une supériorité opérationnelle décisive.

Au fil du XX$^{e}$ siècle, les usages militaires du spectre électromagnétique n'ont eu de cesse de s'étendre, au fur et à mesure que progressaient les technologies de télécommunications.

## A. DE L'OUTIL INDISPENSABLE À LA MARGINALISATION PROGRESSIVE

### 1. Les usages militaires du spectre électromagnétique

#### a. *L'invention pionnière est d'abord civile*

La découverte des ondes électromagnétiques constitue un tournant majeur dans l'histoire des sciences et des technologies modernes.

**En 1864, le physicien écossais James Clerk Maxwell démontre mathématiquement l'existence d'ondes électromagnétiques se propageant à la vitesse de la lumière.**

Vingt ans plus tard, Heinrich Hertz confirme cette théorie en parvenant à produire et détecter le phénomène en laboratoire (donnant par la même occasion son nom à l'unité des ondes).

**Ce prodige technique débouche rapidement sur diverses applications pratiques dont d'abord la télégraphie sans fil (TSF).**

Ainsi, en 1897, des ingénieurs de la Royal Mail parviennent, en utilisant l'équipement de Guglielmo Marconi, à réaliser au Pays de Galles une transmission radio – en morse - entre Lavernock et l'île de Flat Holm, soit à 14 km du continent.

Les progrès en termes de distances sont ensuite fulgurants. **Si, en 1899, Marconi, avec la collaboration d'Édouard Branly, réussit la première communication télégraphique transmanche, il établit en décembre 1901 la première liaison intercontinentale entre la Cornouailles et Terre-Neuve** (soit une distance de 3 500 kilomètres).

#### b. *L'utilisation militaire stimule le développement de la TSF*

**Cette innovation technologique majeure, qui permet aux communications humaines de s'affranchir des distances sans autre moyen que les ondes électromagnétiques, conduit rapidement les diplomates mais surtout les militaires à s'intéresser à ses applications pratiques.**

Dès 1898, le capitaine Ferrié, futur général, est chargé par l'état-major de développer la télégraphie sans fil, mission qui aboutira, entre autres, en 1903, à dédier la Tour Eiffel à l'usage militaire, permettant les communications lointaines, notamment avec les colonies d'Afrique et d'Asie.

Hors de France, **au début du XX^e^ siècle, toutes les armées modernes se dotent de matériels de TSF.**

Pour autant, en termes de conflit, la première manifestation identifiable de guerre électronique s'est produite lors de la guerre russo-japonaise, au cours de la bataille navale de Tsushima en mai 1905.

**Dotée d'un équipement radio des plus modernes, la flotte japonaise est capable,** en dépit de la faible visibilité, **de coordonner le positionnement de ses bâtiments au débouché du détroit**, ce qui lui permet d'anéantir les navires adverses, moins rapides et moins bien armés.

Diverses sources indiquent qu'en dépit de cet échec militaire retentissant qui conduira l'empire russe à capituler, **les bâtiments russes auraient tenté,** compte tenu de la similarité de leurs équipements radios avec ceux des Japonais, **de perturber les signaux ennemis en augmentant la puissance de leur émetteur.**

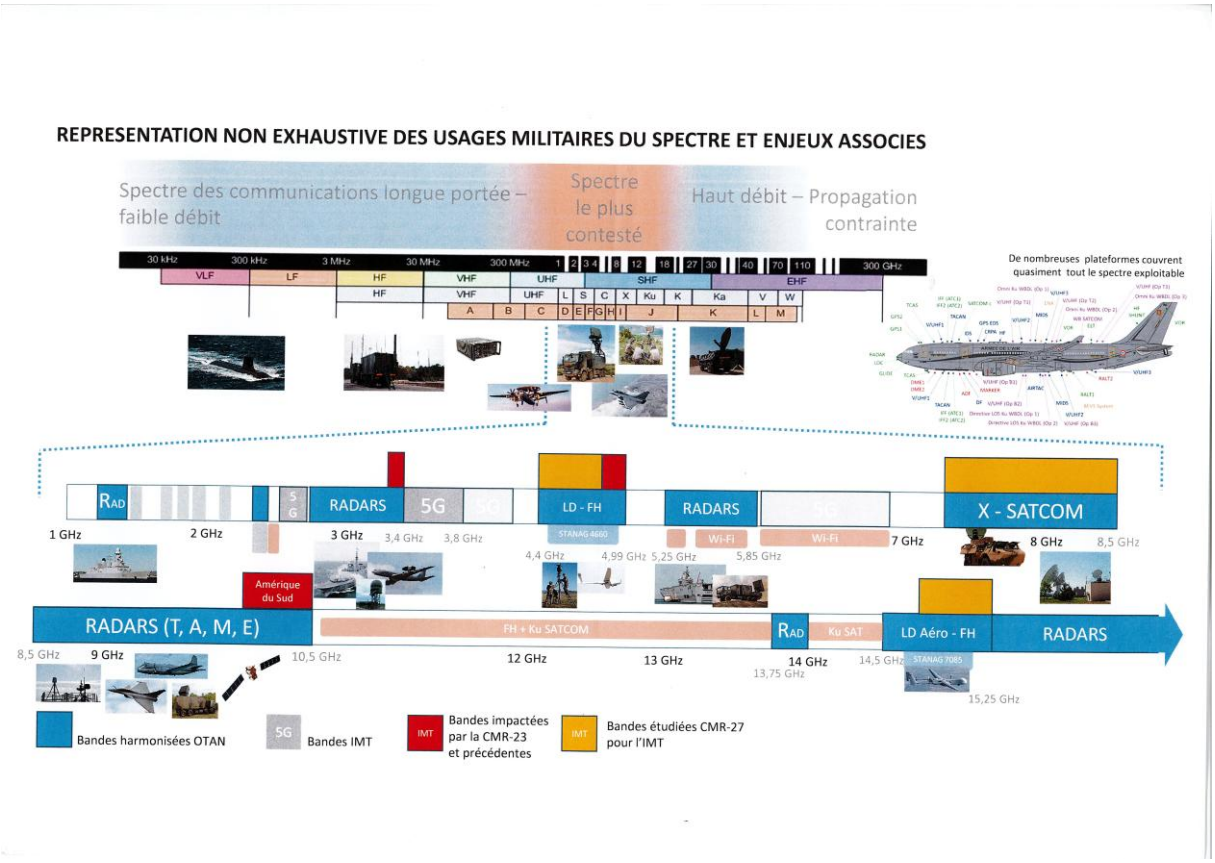
Cette action aurait été **le premier emploi de contre-mesures électroniques en situation de combat.**

### c. *Un paradigme d'emploi très tôt fixé*

Si la connaissance exacte du phénomène électromagnétique n'est pas totalement assurée dans ces phases pionnières[1], **les chercheurs**, à la suite de Maxwell, **ont rapidement mesuré les dimensions d'un spectre électromagnétique qu'ils ont classé en fréquences, subdivisées elles-mêmes en gammes de fréquences,** sachant que chacune d'entre elles revêt un usage spécifique en fonction de ses caractéristiques et de ses propriétés.

Ainsi, **plus les fréquences utilisées sont basses (3 à 30 Hz), plus l'onde porte loin** (100 000 à 10 000 km) avec l'avantage de réclamer une faible énergie d'émission. *A contrario*, **plus monte la gamme de fréquences** (30 GHz à 300 GHz), **plus le débit d'informations transmises est précis pour une longueur d'onde réduite** (1 cm à 1 mm).

[1] Trop connu, méconnu : le tube à limaille (1890), Jean Cazenobe, Revue d'histoire des sciences Année 1976 29-2 pp. 143-165




**Au plan militaire, comme vu *supra* avec la guerre russo-japonaise, l'utilisation des ondes électromagnétiques a très rapidement présenté un enjeu**. Au fur et à mesure de l'avancée technologique, d'ailleurs plus en fonction de son utilisation par les armées que des caractéristiques du spectre lui-même, l'usage de celui-ci s'est établi en trois volets distincts.

**Le premier, découlant des communications de l'adversaire, est le renseignement.** Cette « écoute » permet la connaissance de la localisation des émetteurs mais aussi de collecter des informations de toutes natures, tactiques ou stratégiques, sur l'ennemi.

**Le second est celui de l'offensive** visant à dégrader, neutraliser ou détruire les capacités ennemies. Cela consiste au leurrage (faire croire ce qui n'est pas) mais surtout le brouillage qui consiste à émettre plus fort sur la longueur d'onde ennemie et donc empêcher toute communication.

**Le troisième renvoie à la défense,** c'est-à-dire la protection de son spectre électromagnétique par divers moyens isolés ou cumulés, soit par du chiffrement des communications, des changements de fréquences planifiés, la perception du leurrage ennemi ou, plus radicalement, par la destruction cinétique de ses moyens de GE.

## 2. Le rôle de la guerre électronique s'est fortement accru au XX$^{e}$ siècle

### a. *La Première Guerre mondiale*

**Lors de la Grande Guerre, la radio, du fait de son emploi grandissant, devient un appui déterminant pour les armées.**

Au déclenchement du conflit, l'équipement de la flotte allemande, civile ou militaire, permet aux navires de se mettre aussitôt à l'abri dans des ports neutres tandis que les navires alliés non informés, restés en mer, subissent de nombreuses pertes.

Quelques mois plus tard, la Grande-Bretagne sectionne les câbles de communication allemands vers l'Afrique, contraignant Berlin à recourir davantage à la radio, rendant ainsi ses échanges vulnérables à l'écoute des adversaires, désavantage augmenté par la destruction de ses stations TSF dans le Pacifique.

**Lors de la bataille de Tannenberg en août 1914, l'armée allemande parvient à intercepter les transmissions radio ennemies** après avoir été initialement bousculée par les Russes. Cet avantage lui permet de connaître la localisation des divisions tsaristes et d'anticiper leurs mouvements, d'être renseignée sur le moral du commandement et *in fine* de remporter une victoire décisive.

**Stimulés par les nécessités vitales de la défense, les chercheurs français développent toute une série d'innovations qui révolutionnent les moyens d'une guerre électronique qui ne sera plus en 1918 ce qu'elle était en 1914**. On peut citer les dispositifs à tube thermoïonique dont la célèbre « triode de la Télégraphie Militaire » (lampe TM), les amplificateurs à basses fréquences, les récepteurs superhétérodynes, les radios à bord des aéroplanes, les réseaux d'écoute et de goniométrie *etc*.

**Menée au sein du 8$^{ème}$ régiment de génie sous l'impulsion du Général Ferrié,** à l'aide de l'antenne de la Tour Eiffel, **l'exploitation des différences d'intensité de réception des signaux radio donne la localisation approximative des émetteurs** donc les déplacements des postes de commandement de l'adversaire jusqu'à la fixation du front en octobre 1914.

Lors des attaques sur la capitale par les « Zeppelin », les opérateurs mènent d'abord des actions de brouillage puis modifient ensuite des balises radio, ce qui contribue à désorienter les dirigeables ennemis. Ainsi, en octobre 1917, les navigateurs allemands se servant de la Tour pour s'orienter lors de leurs raids, Ferrié interrompt ses émissions pour les remplacer par celles, de même puissance, de la station de Lyon-La Doua. Ce leurrage électromagnétique fut un succès complet. Les dirigeables désorientés furent incapables de retourner vers leurs bases.

**Plus généralement, le développement de la TSF dans toutes les armées belligérantes a facilité les communications des unités comme celles des échelons de commandement.** Si le chiffrement s'est perfectionné au même rythme, la possibilité d'être écouté – l'urgence, la désorganisation poussant parfois aux échanges non cryptés – a augmenté à son tour.

**Si les exemples de ces interceptions sont nombreux**, notons l'interception réussie en janvier 1917 par le Royaume-Uni d'un télégramme adressé à l'ambassadeur allemand au Mexique, évoquant une alliance entre ces deux pays, dévoilement qui aurait accéléré l'entrée en guerre des États-Unis.

Avec le même succès, les opérateurs et déchiffreurs français parviennent à accéder aux communications allemandes les informant de l'imminence de l'offensive de juin 1918.

### b. *La Seconde Guerre mondiale*

**Après les années 1920 et 1930 qui sont une période d'innovation intense dans le domaine des ondes, le conflit mondial voit logiquement la guerre électronique devenir un outil central des opérations militaires, la maîtrise de l'information devenant vitale dans toutes les conduites d'opérations.**

**Le saut technologique majeur est celui du radar** (« *Radio detection and ranging* »), système utilisant les ondes électromagnétiques pour détecter la présence, la position, la vitesse, d'avions, de bateaux ou même de phénomènes météorologiques.

À partir d'expérimentations menées dès les années 1930, les Britanniques sont capables en 1939 de mettre au point la « *Chain Home* », réseau de radars qui joue un rôle essentiel lors de la bataille d'Angleterre par le repérage préventif des vagues d'attaque de la Luftwaffe.

Du côté allemand, la technologie est elle aussi très avancée, avec toute une gamme de matériels dont les plus connus sont les modèles Freya (pour l'alerte aérienne) et Wurzburg (pour le guidage des avions), qui se compteront à la fin du conflit en plusieurs milliers d'exemplaires.

Autre innovation mais cette fois-ci **dans le milieu aquatique. Les Britanniques inventent l'ASDIC qui donne aux Alliés le moyen de repérer les U- Boots dans l'Atlantique**. Sous l'eau, l'envoi d'un signal sonore à intervalle régulier puis le délai de réception de son écho permettaient d'évaluer la distance de la menace. Au début d'une capacité de détection d'environ 2 000 mètres, la portée fut rapidement doublée.

**À la suite de l'essor de ces technologies, une fois encore stimulée par les nécessités de la guerre, aucune opération militaire ne fait l'impasse de l'utilisation de la radio sans fil, des forces de mêlée aux états-majors**.

Pour autant cette utilisation massive - risque déjà rencontré à la fin de la Grande Guerre - présente une faiblesse importante **: celle de l'interception possible des communications.**

**Leur protection doit donc être accrue, ce qui donne au chiffrement,** y compris à l'aide de machines perfectionnées (cf la célèbre « *Chiffriermaschine Enigma* » de l'armée allemande), un développement sans précédent. S'ajoute aussi une discipline de plus en plus ferme quant aux pratiques quotidiennes des opérateurs (habitude du secret, émissions brèves, changements de fréquences etc.).

Sans qu'il soit nécessaire de détailler à l'excès les manifestations des trois domaines exposés plus haut (renseignement, attaque et défense), **rien n'expose avec plus de clarté la combinaison de toutes les composantes de guerre électronique que l'opération *Overlord d*e juin 1944.**

Au cœur de cette dernière, **le volet « *Fortitude* » doit, entre autres, cacher les véritables intentions des Alliés et convaincre les Allemands que le débarquement aura lieu dans le Pas-de-Calais.**

À cette fin, dès le mois de décembre 1943, une évaluation exhaustive des défenses ennemies est lancée, principalement par des moyens électroniques mais tout autant par de l'imagerie aérienne et les remontées d'information des groupes de résistance locale.

Lors de cette phase, un **recensement minutieux des caractéristiques de tous les signaux ennemis** – radars, radios etc. – est entrepris afin de préparer les opérations de brouillage du jour J.

L'accent est mis ensuite sur des bombardements massifs (2 000 missions durant dix semaines) sur les stations radar, d'écoute, de brouillage ainsi que les réseaux de communication sur toute la côte française. Cette destruction est intentionnellement partielle. Les Alliés conservent 16 stations sur 92, afin de pouvoir les utiliser à des fins de leurrage ou de désinformation.

Lors du lancement d'*Overlord*, **deux stratégies de leurrage** sur le lieu du débarquement - Pas de Calais plutôt que Normandie - **une navale et une autre aérienne, sont entreprises.**

La première, dérivée de « *Moonshine* » britannique, falsifie les échos d'un radar ennemi en amplifiant la puissance du signal réfléchi. Quatre vedettes sont équipées d'un ballon capable de renvoyer chacune l'écho d'un navire de 10 000 tonnes.

Lors de la seconde, une vingtaine de Lancaster dirigés vers Le Havre, se relaient pour larguer des bandelettes d'aluminium appelées « Windows » qui renvoient le même écho qu'un navire ou un avion. L'utilisation reste mesurée et ciblée pour ne pas éveiller la méfiance des Allemands.

Enfin**, lors du débarquement proprement dit, un brouillage intense est déclenché sur les communications ennemies, parachevant toute la stratégie électronique des Alliés.**

**Le bilan tiré après la guerre des effets de cette stratégie est nuancé**. Si elle a été efficace pour rendre les batteries côtières inopérantes (un seul navire coulé), son efficacité semble plus nuancée sur les opérations aériennes. La faiblesse de la *Luftwaffe* est certes en partie liée à l'empêchement de ses communications mais résulte tout autant du manque d'avions ou de carburant des escadrilles. Enfin, en dépit des destructions, du leurrage ou du brouillage, les radars allemands ont été capables de repérer l'avancée de la flotte de débarquement.

**Reste enfin qu'au plus haut niveau du commandement nazi, la confusion subsista longtemps quant à la possibilité d'une attaque dans le Pas de Calais**, la Normandie étant considérée longtemps comme une diversion, croyance qui disparut trop tard au bénéfice évident des Alliés[2].

**Cette conclusion démontre ainsi l'efficacité indéniable de la guerre électronique quand elle est combinée dans tous les domaines de guerre. *« Réductrice des forces ennemies et multiplicatrice des forces amies* », elle est devenue lors du conflit mondial un facteur décisif de supériorité opérationnelle.**

### c. *La guerre électronique fut au cœur de la Guerre froide*

#### i. Le Pacte de Varsovie a placé la GE au cœur de la lutte anti-OTAN

Après les enseignements du conflit mondial, **la période de Guerre froide,** dans laquelle l'information est une ressource stratégique majeure, accentue cette dynamique. L'impossibilité d'un affrontement direct, en raison du risque nucléaire, **pousse les États-Unis et l'Union soviétique à développer des moyens indirects de domination dans lesquels la guerre électronique occupe une place centrale.**

Les armées du Pacte de Varsovie sous l'autorité de l'Union Soviétique définissent une doctrine spécifique qui repose sur une connaissance fine des capacités et intentions de l'adversaire, finalité conservée jusqu'aujourd'hui.

---

[2] *La Guerre électronique - Maître des ondes, maître du monde, Jean Paul Siffre, Lavauzelle, 2002.*

**De 1950 jusqu'à la chute du Mur de Berlin, le bloc de l'Est s'avère un redoutable compétiteur de guerre électronique**, comme l'ont montré les très nombreuses péripéties dans lesquelles les techniques d'espionnage prenaient souvent la forme d'une maîtrise décomplexée du spectre.

On peut ainsi citer les systèmes d'écoute généralisés, dans les ambassades des États d'Europe de l'Ouest et plus encore celle des États-Unis. Dans ce dernier cas, un dispositif sophistiqué permettait à partir de 1945 la perception des échanges par la pose d'un appareil passif « *The Thing* » activé à distance par une onde radio, et permettant de capter les conversations internes sans source d'énergie propre.

De même, **les systèmes de surveillance et de brouillage ont été systématiques, par exemple à partir des États du Pacte de Varsovie en proximité du Rideau de Fer,** en direction des émissions de « *Radio Free Europe* » et « *Radio Liberty* », financées secrètement par la CIA.

Parallèlement, l'essor rapide de la puissance de calcul a rendu possibles des équipements flexibles et reconfigurables. Ces évolutions ont favorisé **l'apparition de capacités offensives avancées**, telles que les plateformes aériennes spécialisées dans le brouillage ou les armes conçues pour neutraliser les capteurs radar. **Le domaine spatial s'est également imposé,** avec le déploiement de satellites, à l'image des satellites soviétiques Tselina dédis au renseignement d'origine électromagnétique (ROEM).

**L'URSS et ses alliés instaurent des unités spécialisées et des équipements dédiés à l'écoute, à l'analyse et à l'exploitation des signaux**. Des systèmes terrestres sont également déployés au niveau des bataillons et compagnies de reconnaissance pour intercepter les communications de l'OTAN en cas de conflit sur le front central européen[3].

**Les conflits régionaux ont également servi de terrain d'expérimentation pour les matériels.** Ainsi, la guerre du Vietnam a stimulé le développement des systèmes de neutralisation des défenses anti-aériennes. L'aviation américaine s'y est heurtée à espace aérien électroniquement bien couvert, défendu par une artillerie antiaérienne et une artillerie sol-air équipées « à la soviétique », redoutables pour les avions tactiques.

En 1967, les États-Unis ont perdu 326 appareils au-dessus du Nord-Vietnam, dont 85 % du fait de la défense sol-air.

D'autres évènements ont permis de tirer des leçons opérationnelles des avancées de guerre électronique comme la guerre du Kippour, le conflit des Malouines ou encore la plaine de la Bekaa[4].

---

[3] *Ukraine Just Captured Another Rare Russian Electronic Warfare Vehicle*

[4] *LA GUERRE ÉLECTRONIQUE EN ÉBULLITION*

La première guerre du Golfe a quant à elle montré que les armes connectées, même en provenance des deux blocs, pouvaient être neutralisées électroniquement[5].

ii. L'Occident s'est adapté à la menace

**L'exploitation massive des communications a conduit à une approche intégrée du renseignement, donnant naissance à de vastes dispositifs d'interception et d'analyse,** à l'image du réseau ECHELON dont le déploiement est resté inconnu du grand public pendant près de quarante ans.

**Dans le climat stratégique de la Guerre froide, les États occidentaux investissent rapidement dans des capacités d'interception plus puissantes et à portée étendue.** Dès le milieu des années 1970, les États-Unis mettent en service une installation spécifiquement destinée à capter les communications relayées par les satellites civils de télécommunications[6].

Dans le contexte de la confrontation entre blocs, **l'Alliance atlantique organisait la préparation de ses membres face à un adversaire** étudié collectivement, tant dans ses doctrines que dans ses moyens et ses modes d'action.

**De nombreuses opérations sont menées durant cette période** à l'image de l'opération « *Gold* » menée par la CIA et le MI6 à Berlin dans les années 1950. Elle consistait en une écoute directe de câbles téléphoniques soviétiques permettant la collecte d'informations sur le dispositif militaire du Pacte de Varsovie. Cette opération constitue l'une des sources de renseignement les plus productives de la CIA sur l'armée soviétique durant la Guerre froide.

Ces opérations se poursuivent tout le long de la Guerre froide, à l'image de l'opération « *Ivy Bells* » dans les années 1970 qui permet aux Américains d'intercepter les communications soviétiques en posant des dispositifs d'écoute sur des câbles sous-marins stratégiques.

iii. La France a beaucoup investi à cette période dans la GE

À la sortie du conflit mondial, **la France possède un vivier de chercheurs de grande qualité qui permet au pays de reprendre l'initiative** et de s'affranchir pour partie du matériel américain. Les moyens sont modestes mais de nombreux ingénieurs, souvent polytechniciens, perfectionnent les matériels, notamment les antennes ou les radars.

---

[5] *La guerre dans le champ électromagnétique (GCEM) | Ministère des Armées et des Anciens combattants*
[6] LA GUERRE ÉLECTRONIQUE EN ÉBULLITION

**Dans les années 1970 et 1980**, le secteur de la défense a continué sur cette lancée. **Des infrastructures essentielles**, comme celles de la DGA-MI situées à Bruz (Ille-et-Vilaine), **ont été construites durant cette période**. Les chambres anéchoïques qui y sont installées permettent notamment de tester la signature électromagnétique des armements.

**La dissuasion française a particulièrement bénéficié de ces apports**. Le Mirage IV, vecteur de la composante nucléaire aéroportée (CNA), a été le premier aéronef de l'AAE équipé de moyens d'autoprotection.

Les forces aériennes stratégiques ont ainsi régulièrement modernisé leurs systèmes d'autoprotection (SAP) pour s'adapter à la menace, au point de faire de la France un expert mondialement reconnu pour la qualité et le niveau de ses équipements, par ailleurs étendus à l'ensemble des aéronefs de l'AAE dont les hélicoptères et les avions de transport.

**En outre, dans les années 1980, l'Armée de l'Air disposait de capacités de GE offensives aéroportées significatives** comme les POD de leurrage EM « BOZ », destinés à créer des couloirs de paillettes afin de masquer les raids offensifs amis pour franchir les défenses sol-air du rideau de fer ou encore le missile anti-radar AS37 MARTEL, destiné à détruire les radars de veille ou de conduite de tir des systèmes sol-air.

Ce dernier missile, employé au Tchad en 1987 à Ouadi Doum, a permis la destruction d'un radar de veille « *Flat Face* » libyen. À cette époque, un escadron consacré à la guerre électronique, l'EC 2/11 « Vosges », mettait en œuvre ces moyens de brouillage, leurrage et anti-radar.

### 3. Les dividendes de la paix ont marginalisé la GE au sein des armées françaises et occidentales

#### a. *La prévalence des conflits asymétriques a marginalisé la GE*

À la fin de la guerre froide, la prévalence de conflits asymétriques de type « *gestion de crise* » a abouti à rendre la GE moins prioritaire. Ces conflits impliquaient principalement le domaine des communications (GE radio) tandis que la GE radar et le segment offensif étaient globalement délaissés.

D'après les éléments communiqués par l'armée de Terre à vos rapporteurs, « ***Les engagements, essentiellement tournés vers la contre-insurrection depuis le début des années 2000, ont conduit l'armée de Terre à satisfaire prioritairement les besoins du segment de la surveillance électronique*** *avec un effort sur les capacités légères d'interception et de localisation, de protection des forces contre la menace RC-IED (brouilleurs d'autoprotection contre les engins explosifs improvisés radio commandés).*

*Les combattants de la GE spécialisée étaient alors souvent employés au sein d'unités multi-capteurs. Les capacités légères déployées avaient pour objectif principal la détection et le ciblage d'individus, et devait s'intégrer sur des porteurs de circonstance. (…)* ***Aucune capacité de surveillance des radars, ni de brouillage forte puissance n'étaient nécessaires dans ce contexte particulier. »***

Un constat qui a été clairement corroboré par l'état-major de la Marine nationale (EMM): « *D'une manière générale, la période qui s'achève, du fait de son orientation « gestion de crise » plutôt que « guerre de haute intensité », a conduit à ne pas développer le segment offensif.* ***La guerre électronique, dans son acception globale, n'était pas prioritaire.***

***En pratique, cette période peut être décrite selon deux critères : diminution du nombre d'unités navales, éviction d'équipements dans les programmes capacitaires.*** *Le premier sujet, d'un point de vue de la guerre électronique, diminue le maillage de la Marine en mer et, de fait, ses capacités de recueil d'informations électromagnétiques. Cela impacte les bases de données de guerre électronique qui permettent une identification rapide des menaces. ».*

Cette évolution a été également confirmée par l'état-major de l'armée de l'air et de l'espace (EMAAE) :

« *Le modèle expéditionnaire de contre-insurrection qui était celui adopté pendant des décennies sur les théâtres d'opérations extérieures (TOE) était adapté à la menace GE, évaluée à un niveau faible.* ***En effet, les aéronefs de l'AAE engagés sur ces TOE évoluaient dans un environnement EM quasiment permissif.*** *Ainsi, la menace GE rencontrée se résumait à la menace infrarouge matérialisée par les missiles sol-air très courte portée guidés par infrarouge souvent anciens (menace proliférante et facile à mettre en œuvre) et à une menace de brouillage GPS émise par des brouilleurs rudimentaires.*

***La capacité GE adaptée à ce niveau de menace était donc assurée par les systèmes d'auto protection de nos aéronefs. »***

### b. *Une GE peu à peu devenue une variable d'ajustement capacitaire*

**Au même titre que les capacités de soutien et d'autres appuis (artillerie, génie etc.), les investissements dans le champ de la GE ont constitué une « *variable d'ajustement dans la variable d'ajustement* »,** aboutissant *de facto* à un déficit capacitaire.

Au plan géopolitique, la fin de la Guerre Froide et surtout l'éclatement du Pacte de Varsovie, ont eu un impact non négligeable sur le niveau d'équipement des armées occidentales.

**La France n'a pas échappé aux effets des « *dividendes de la paix* », comme le montre, de 1990 à 2001, la baisse du budget de défense**. L'éloignement de la probabilité d'un conflit massif en Europe et la disparition d'un certain nombre de menaces directes sur le territoire national, ont été une occasion historique de réduire durablement les dépenses militaires pour réaffecter les ressources libérées à d'autres postes budgétaires. En part de PIB, notre pays est passé de 2,8 % en 1990 à 2 % en 2001.

**Cette contraction de la dépense s'est accompagnée par ailleurs d'une profonde restructuration de l'industrie d'armement par la privatisation des entreprises publiques et la concentration des nouvelles entités industrielles**. Outre les déterminations géopolitiques évoquées plus haut, plusieurs auteurs soulignent que ces choix stratégiques ont aussi été liés au coût - insoutenable pour l'État - des innovations technologiques que réclament par définition la BITD.

La guerre électronique a évidemment pâti de ces diverses déterminations. Le poids des investissements initiaux des programmes d'armement, notamment la R&D, a obligé une affectation prioritaire de la dépense dans des secteurs perçus comme plus prioritaires, comme le nucléaire.

**Signe de cette relative marginalisation, les 30 aptitudes critiques à détenir par les forces françaises, détaillées dans la revue nationale stratégique de 2017, n'incluent pas la maîtrise du spectre EM et la lutte dans ce champ**.

Par ailleurs, il faut aussi évoquer le trait intrinsèque de la guerre électronique, celui de sa difficile perception par les acteurs, sachant qu'elle s'avère très technique, invisible et silencieuse.

Plus encore, elle représente une matière extrêmement sensible en raison de son haut niveau de classification au point d'être assimilée par certaines personnes auditionnées par vos rapporteurs à un « *club fermé* » ne concernant que quelques centaines de spécialistes militaires et/ou industriels en France.

### c. *La GE occupe une place trop discrète dans la LPM 2024-2030*

**La guerre électronique occupe une place faiblement lisible dans la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense**[7]. Le terme « électromagnétique » lui-même n'intervient qu'à trois occurrences dans le texte promulgué.

Pour autant, la modernisation et le renforcement des capacités interarmées de ROEM stratégique et tactique, initiés bien avant la LPM 2024-2030, sont *de facto* intégrés à la trajectoire de la LPM en cours.

---

[7] *https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047914986*

On y trouve notamment la rénovation et la modernisation du dispositif terrestre militaire de renseignement d'origine électromagnétique (ROEM) stratégique actuellement en service et l'acquisition de moyens mobiles d'interception pour le volet surveillance de la GCEM et pour le ROEM tactique des trois armées.

**D'après les informations transmises en audition, près de 660 M€ seraient programmés pour le ROEM stratégique et tactique interarmées sur la période 2024-2030.**

**L'opération budgétaire « ROEM Stratégique » vise à doter les armées d'une composante fixe et déplaçable de renseignement d'origine électromagnétique de niveau stratégique.** Elle modernise les systèmes de commandement et d'exploitation du ROEM stratégique, la capacité de localisation et d'interception des émissions électromagnétiques stratégiques au profit de l'ensemble des armées et de la direction du renseignement militaire (DRM).

Cette capacité a été lancée en 2011 et livrée à partir de 2017. Elle est composée des capacités de recueil automatisé des signaux de radiocommunications, de localisation stratégique, d'exploitation et valorisation des écoutes, de traitement de signaux de communication par satellite ainsi que d'exploitation en masse et enrichissement ROEM.

**L'opération budgétaire « Système interarmées ROEM tactique » vise également à doter les armées de moyens de surveillance de spectre électromagnétique**.

Cette capacité de détection, d'identification, de localisation et d'écoute de signaux de radiocommunications est destinée à fournir **aux unités déployées dans une opération terrestre, aérienne ou navale les informations nécessaires à la prise de décision pour la conduite de l'opération.** La capacité a été lancée en 2018, les premières livraisons ont été réalisées en 2023 au profit de la Marine et sont employées depuis dans les opérations en mer Rouge notamment.

**D'après les informations transmises aux rapporteurs en audition et préalablement à son actualisation imminente, la LPM 2024-2030 prévoirait 238 M€ pour le programme à effet majeur ROEM tactique, répartis entre 160 M€ pour l'incrément surveillance radio et 78 M€ pour l'incrément attaque.**

L'Armée de Terre a reçu ses deux premiers véhicules blindés multi-rôles légers (VBMR-L) Serval du programme SCORPION dédiés à la guerre dans le champ électromagnétique à l'été 2025.

D'après les éléments transmis par l'armée de Terre, 10 % des véhicules de l'avant blindé (VAB) dédiés à la GE devraient avoir été renouvelés par des Serval de GE à la fin de l'année 2025 dans le cadre du programme baptisé SYMETRIE[8], sachant que l'étape 2 du programme SYMETRIE prévoit une augmentation des capacités de brouillage en portée et puissance. **En 2026, huit Serval ROEM tactiques devraient être livrés par THALES à l'armée de Terre.**

**En 2023, le besoin de la Marine nationale a été ajusté et s'est traduit par une modification de la nature et des quantités des livraisons (24 bâtiments de surface et neuf avions de patrouille maritime Atlantique 2 seront équipés pour recevoir les charges utiles**). Le calendrier de livraison a également été mis à jour, les premières devant avoir lieu en 2026.

Dans le cadre de l'incrément surveillance radio, la Marine sera livrée de plusieurs capteurs SHF qui seront employés de manière mutualisée sur l'ensemble de la Marine (bâtiments de surface et aéronautique navale).

Or, le besoin de la Marine sur ce segment est d'équiper l'ensemble de ses unités d'intercepteurs numériques large bande. Or, ces équipements sont financés sur les programmes porteurs et font néanmoins ponctuellement l'objet d'éviction.

Seules les grandes unités sont équipées à ce jour. Dans ce contexte, la Marine s'équipe *via* les crédits de la Marine nationale au sein du Programme 178 de la mission Défense de moyens d'interception radio complémentaires pour ses unités (bâtiments de surface, sous-marins, aéronautique navale, commandos) à hauteur de quelques millions d'euros par an.

Concernant l'incrément attaque, la Marine devrait être livrée d'une capacité de brouillage radio de moyenne puissance. Elle manifeste son intérêt principal sur les études envisagées sur le brouillage radar dont les contours restent encore néanmoins à définir. Le besoin de la Marine est d'équiper l'ensemble de ses grandes unités de moyens EM offensifs pouvant possiblement être « dronisés ».

**En outre, en matière d'innovation, la LPM 2024-2030 a été construite sur la base d'un « *patch innovation* » de 10 milliards d'euros comportant plusieurs démonstrateurs :**

- Le premier d'arme à énergie dirigée (AED) EM de puissance 200 kW intégré d'ici 2027 sur porteur terrestre ou naval (LAD, frégates) visant la neutralisation simultanée de plusieurs drones autonomes (insensibles au brouillage) et gains de portée grâce à l'augmentation de leur puissance,

---

[8] *SYMETRIE pour « Système tactique de ROM interarmées ».*

- Le second d'une constellation de nanosatellites équipés d'une charge utile spécialisée dans la détection et la localisation d'interférents GNSS (Maîtrise de l'espace NAVWAR). Ce dernier permettra une capacité à opérer en environnement « *GNSS denied* » par détection et localisation d'interférents GNSS (type brouillage GPS/Galileo),

- Le troisième de suppression des défenses aériennes ennemies par combinaison d'effets cinétiques et guerre électronique (application SEAD, RAFALE) : capacité d'entrée en premier face à des systèmes intégrés de défense aérienne présentant des composantes hautement mobiles.

Les rapporteurs saluent la prise en compte de ces efforts en espérant que leur mise en œuvre pourra donner lieu à un rapide passage à l'échelle en cas d'expérimentation réussie.

**Toutefois, ils regrettent que le domaine aéroterrestre ne soit pas davantage ciblé par ces démonstrateurs alors que des besoins évidents sont pourtant observés dans ce segment.**

L'armée de Terre a néanmoins bénéficié du financement au titre du P144[9] de plusieurs opérations d'expérimentation réactives ces dernières années concernant les véhicules de direction et de contrôle de l'efficacité du brouillage ainsi que le brouillage de forte puissance, la guerre électronique élémentaire ou encore les moyens de surveillance des radars adverses.

Nonobstant, ces opérations représentent un montant global proche de 2 M€ ce qui semble relativement peu au regard des montants affichés de 10 milliards d'euros.

En outre, au titre de son P178[10], l'armée de Terre a lancé en 2025 différentes expérimentations dans le domaine de la GE pour un montant proche de 6 M€[11].

**Par ailleurs, afin de remédier aux silences de la LPM 2024-2030 sur le sujet, 80 M€ ont été obtenus en A2PM[12] 2024 afin de permettre aux trois armées de se redoter d'une primo-capacité d'attaque électronique.**

Cet ajustement pourrait notamment être l'occasion pour l'armée de Terre d'obtenir un module de véhicules blindés de brouillage forte puissance.

---

*[9] Programme « Environnement et prospective de la politique de défense » de la mission « Défense » du budget de l'État*

*[10] Programme « Préparation et emploi des forces » de la mission « Défense » du budget de l'État*

***[11] 5 M€ GE élémentaire, 1 M€ GE spécialisée***

*[12] Ajustement annuel de la programmation militaire (A2PM)*

## B. UNE PRISE DE CONSCIENCE RÉCENTE

### 1. Les conflits contemporains remettent la GE au centre de l'ordre de bataille interarmées

#### a. *Un tissu conjonctif de la quasi-totalité des fonctions opérationnelles dans l'ensemble des milieux*

**Parce que l'exploitation du spectre EM revêt une importance toujours croissante, la GE s'impose au croisement de l'ensemble des fonctions opérationnelles**. Elle concerne l'essentiel des capteurs, des communications diverses du niveau stratégique au niveau tactique, et de la fonction positionnement/navigation/temps (PNT), du commandement des opérations au pilotage ou la lutte contre les drones.

**La GE se déploie sur tout le spectre des fréquences radio et radar des armées mais aussi dans l'espace ou la très haute altitude** (brouillage, attaque EM et/ou écoute de satellites militaires ou duaux, charge EM sur des « ballons » ou autre HAPS[13]). Seul le dioptre sous-marin résiste à la propagation des ondes EM, protégeant ainsi les sous-marins des attaques EM adverses.

Aujourd'hui, d'une certaine façon, la guerre électronique ne fait que retrouver la place centrale qui était la sienne durant la guerre froide. **Pour autant, si les conflits récents imposent de réapprendre des tactiques et des techniques utilisées dans les années 1970 et 1980, la guerre électronique est profondément différente du fait de la progression importante des technologies tant matérielles que logicielles**.

Cette prise de conscience est d'autant plus nécessaire que, dans l'intervalle, la dépendance des armées et de la société civile au spectre électromagnétique s'est considérablement accrue rendant parfois certains systèmes plus vulnérables.

#### b. *Le retour de la haute intensité est aussi celui de la GE*

**Dans un conflit de haute intensité, la supériorité dans le champ électromagnétique est d'emblée contestée.**

**Ainsi que l'a rappelé l'armée de l'air et de l'espace devant vos rapporteurs : «** *Il faut dès lors conquérir la supériorité aérienne, au moins au niveau local, pour obtenir une certaine liberté d'action dans l'autre milieu. Cette supériorité aérienne passe par la maîtrise de l'environnement EM, lui aussi contesté. En effet, l'adversaire y utilise des moyens avancés pour détecter, perturber et interdire l'usage du spectre EM.*

---

[13] *High altitude permanent systems, de type « ballons »*

*Dès lors, il ne s'agit plus seulement de se protéger, mais aussi de surveiller activement et de mener des opérations offensives dans le spectre EM afin de prendre l'ascendant sur l'adversaire et d'établir une liberté d'action dans les airs.* ***Les capacités nécessaires en GE doivent donc être bien plus robustes et sophistiquées, couvrant trois volets essentiels : la surveillance, la défense et l'attaque EM*****. »**

**Le retour d'expérience des conflits récents souligne l'utilisation massive des systèmes de GE qui constituent un facteur de supériorité tactique manifeste dans un environnement où la liberté d'action dans le spectre est compromise.**

i. L'Ukraine

**Évènement majeur de géopolitique des dernières décennies, le conflit ukrainien, qui réinstalle un conflit de haute intensité en Europe, se révèle par ailleurs un théâtre dans lequel la guerre électronique intervient massivement**.

Sans doute, **la culture militaire commune des deux belligérants** est-elle un premier facteur de cette prégnance. Comme vu plus haut, la GE était historiquement inscrite dans l'ADN des armées soviétiques. Plus encore, en 2009, après le retour d'expérience du conflit géorgien, la Fédération de Russie a créé des troupes spécifiques, distinctes des forces armées, dotées d'une doctrine entièrement repensée intégrant la GE dans l'ensemble des manœuvres.

**Aujourd'hui, l'armée russe compterait cinq brigades de guerre électromagnétique, une par district militaire, dont au moins trois seraient engagées en Ukraine.** Dans ces territoires occupés, dès 2014, elle y a démontré sa capacité à agir dans toutes les gammes de fréquences électromagnétiques : radar, satellite, téléphonie mobile, radios tactiques.

Face à cet adversaire, **l'armée ukrainienne bénéficie de la culture héritée de l'Union Soviétique par ses matériels et ses personnels**. **Très rapidement**, après l'invasion russe, à partir de cette base structurelle, **les forces armées ukrainiennes (FAU) ont été capables de multiplier leurs effectifs dédiés** par onze et leurs moyens de brouillage/leurrage par quatre.

<u>Un environnement électromagnétique saturé et structuré</u>

**C'est dans ce contexte que la guerre électronique s'inscrit et prend une part centrale dans le conflit.** Aujourd'hui, le champ de bataille se caractérise par un environnement électromagnétique extrêmement dégradé, marqué par un brouillage massif, permanent et organisé, résultant d'un dispositif multicouche déployé par les forces russes.

**Ce dispositif est souvent qualifié de « mur de brouillage », tant il sature l'ensemble du spectre électromagnétique sur le terrain.**

Il inclut tout d'abord des **brouilleurs de signaux de navigation par satellite**, tels que Jitel ou les R-340 RP « Pole-21 », spécifiquement conçus pour perturber les signaux GNSS utilisés pour la navigation et le guidage des armements. On peut y ajouter les **dispositifs visant les liaisons de données sans fil et les communications radio**, notamment les complexes Borisoglebsk-2, efficaces contre les bandes HF, VHF et UHF, largement utilisées par les unités tactiques.

À ces moyens déjà puissants, s'ajoutent des **matériels combinant détection et brouillage**, comme Murmansk-BN, dédiés à la neutralisation des communications à longue portée sur les bandes HF, ou Krasukha qui, déployés en nombre plus limité, s'adressent aux cibles à forte valeur ajoutée, notamment les radars et certaines capacités aériennes ou spatiales.

Parallèlement, **des équipements plus légers et portables sont mis à disposition des unités au contact,** ainsi que des moyens spécifiquement orientés vers la lutte anti-drones, comme Leer-3 ou Repellent-1, destinés à perturber les liaisons de commande et de transmission des drones adverses.

Cela illustre une transformation importante de la guerre électronique russe, **l'émergence d'une véritable « guerre électronique du combattant » avec l'utilisation de systèmes simples, légers et souvent peu coûteux** par des unités non spécialistes, notamment dans l'infanterie, le génie ou la cavalerie.

De fait, le brouillage russe est d'une grande efficacité sur le terrain. Ainsi que l'a précisé le COMCYBER lors de son audition : « ***La masse des équipements russes*** *et leur puissance de brouillage sur une très large gamme de fréquences* ***constitue probablement la menace la plus forte*** *sur la résilience de nos forces dans l'emploi et la maîtrise du spectre EM en combat de haute intensité.* »

**Cet environnement électromagnétique saturé** ne constitue pas seulement un cadre général des opérations, mais **produit des effets directs et mesurables sur les capacités militaires engagées,** notamment la dégradation concrète de systèmes clés, en particulier ceux reposant sur les services spatiaux et les technologies de navigation et de guidage, aujourd'hui au cœur des doctrines occidentales de combat de précision.

<u>Effets du brouillage sur les systèmes satellitaires et les armements occidentaux</u>

Plus concrètement, **l'un des effets les plus marquants de ce dispositif concerne les systèmes satellitaires, en particulier les signaux de positionnement et de navigation.** La guerre en Ukraine a ainsi mis en lumière leur vulnérabilité face au brouillage, illustrant l'importance croissante de ce que l'on désigne sous le terme

de « *Navigation Warfare* », c'est-à-dire la contestation des capacités de navigation adverses par la perturbation ou la falsification des signaux.

Concrètement, cette forme de guerre électronique se traduit sur le champ de bataille par des zones où les signaux GNSS sont indisponibles, rendant inopérants ou fortement imprécis des armements pourtant conçus pour des frappes de haute précision.

Les technologies de renforcement des signaux GNSS, développées progressivement depuis plusieurs décennies pour accroître la résilience de ces systèmes, se révèlent insuffisantes lorsqu'elles sont utilisées isolément. Seuls les armements combinant plusieurs techniques avancées de guidage et de navigation parviennent à conserver un niveau de précision satisfaisant, au prix d'une complexité accrue et de coûts sensiblement plus élevés.

**La dépendance aux services spatiaux explique également le ciblage des infrastructures satellitaires ukrainiennes par la Russie,** notamment au début du conflit. Les attaques contre les réseaux de communication satellitaire, ainsi que les tentatives répétées de brouillage des satellites de télécommunication et d'observation, ont mis en évidence la dimension stratégique de la guerre électronique appliquée à l'espace.

Au-delà des systèmes satellitaires et des armements de précision, **ces pratiques de brouillage ont également des conséquences majeures** sur l'ensemble du champ de bataille aéroterrestre et cela d'autant plus qu'elles interviennent dans une autre transformation majeure du conflit ukrainien, **à savoir la prolifération massive des drones**, à la fois une opportunité opérationnelle et une vulnérabilité nouvelle face à la guerre électronique.

La guerre électronique au cœur de la lutte anti-drones

**La guerre en Ukraine est en effet marquée par une prolifération sans précédent des drones.** Ces systèmes sont désormais employés pour une grande diversité de missions, allant de l'observation et de la désignation d'objectifs à l'attaque directe, au ravitaillement logistique de l'avant, voire à la mise en œuvre de capacités de guerre électronique.

**Les volumes engagés sont considérables, avec plusieurs centaines de milliers de drones** consommés chaque mois par les belligérants. Cette intensification modifie profondément la physionomie du champ de bataille, en élargissant à la fois la « zone grise », caractérisée par des positions ambiguës et difficiles à attribuer et la « zone létale », qui s'étend désormais en profondeur bien au-delà de la ligne de front.

Dans ce nouveau contexte, la guerre électronique (GE) s'impose comme une composante centrale de la lutte anti-drones en intervenant à toutes les étapes de la chaîne opérationnelle, aussi bien pour la détection et l'identification des vecteurs aériens que pour leur neutralisation, par brouillage, leurrage ou prise de contrôle. **D'après le droniste CERBAIR, auditionné par vos rapporteurs, les drones seraient aujourd'hui responsables de près de 80 % des pertes matérielles et humaines constatées en Ukraine.**

**Dans ce cadre, les moyens de guerre électronique jouent un rôle déterminant dans la limitation de l'efficacité adverse. Selon les mêmes sources, entre 60 et 80 % des drones interceptés en Ukraine le seraient par des moyens de GE.**

Ce chiffre illustre à la fois **l'efficacité opérationnelle de ces capacités et leur caractère désormais indispensable dans tout dispositif de protection des forces, des infrastructures et des populations.** Il souligne enfin la nécessité, pour les armées modernes, de disposer de moyens de guerre électronique robustes, évolutifs et intégrés, capables de s'adapter à des menaces en constante mutation.

L'innovation au cœur de la dialectique du glaive et du bouclier

Ces thématiques s'inscrivent dans **une dynamique** beaucoup plus large **d'adaptation permanente dans laquelle chaque succès tactique entraîne une réponse rapide de l'adversaire**. Cette logique de confrontation accélérée nourrit un cycle d'innovation inédit, tant sur le plan technique que doctrinal.

La guerre électronique connaît en Ukraine **un essor marqué par une dynamique d'innovation continue**. Les deux belligérants adaptent en permanence leurs méthodes, leurs logiciels et leurs équipements afin de prendre l'ascendant électromagnétique sur l'adversaire.

Cette logique d'adaptation et de contre-adaptation est particulièrement rapide. **Selon les éléments portés à la connaissance des rapporteurs, les évolutions logicielles interviendraient tous les uns à deux mois, tandis que les évolutions matérielles se succéderaient environ tous les six mois**.

Dans ces conditions, le paysage de la guerre électronique peut être profondément transformé en l'espace d'une seule année, **ce qui rompt avec les cycles d'innovation traditionnellement longs des équipements militaires**. Comme l'a souligné le ComCyber, lors de son audition, « *l'innovation et la capacité d'adaptation rapide aux nouvelles technologies se sont ainsi révélées essentielles pour conserver une efficacité opérationnelle* ».

**Cette dynamique est renforcée par l'irruption massive de technologies civiles commerciales dans le champ de la guerre électronique** qui dépasse d'ailleurs largement ce seul théâtre d'opérations ukrainien. Des technologies

initialement développées pour des usages civils se révèlent parfois plus performantes et plus résilientes que certains équipements militaires plus anciens.

À titre d'exemple, **les capacités multi-GNSS intégrées à des smartphones récents peuvent offrir une meilleure résistance au brouillage** qu'un récepteur GPS militaire conçu dans les années 1990. De nombreux systèmes civils reposent en outre sur des radios logicielles, dont les paramètres peuvent être modifiés en quelques heures pour exploiter de nouvelles fréquences ou contourner un brouillage adverse. L'enjeu de **la mise à disposition de constellations civiles de télécommunications, comme Starlink**, illustre parfaitement cette imbrication croissante entre capacités civiles et militaires dans le champ électromagnétique.

Parallèlement, **l'intelligence artificielle occupe une place de plus en plus importante** dans la guerre électronique, à l'image de son rôle croissant dans l'ensemble des domaines du champ de bataille.

**Elle permet d'accélérer considérablement le traitement de volumes massifs de données électromagnétiques**, d'améliorer la détection des signaux faibles et de renforcer la résilience des systèmes face aux perturbations. Le théâtre ukrainien voit ainsi émerger les premiers usages de ce que l'on peut qualifier de « guerre électronique cognitive ». Ces outils, fondés sur l'intelligence artificielle, sont capables d'analyser finement un signal adverse et de générer rapidement une forme d'onde adaptée, spécifiquement conçue pour rompre une liaison ciblée de manière précise et efficace.

Une accélération de la détection oblige à la sortie du spectre

**Tout ceci produit une accélération considérable des détections et de la destruction des émetteurs d'ondes électromagnétique.**

Plus concrètement, en Ukraine**, les belligérants concentrent des efforts considérables sur l'accélération de la boucle acquisition–feux, c'est-à-dire la capacité à détecter une cible, l'identifier, puis la frapper dans un laps de temps très réduit.**

Dans ce cadre, **les moyens de guerre électronique jouent un rôle essentiel en tant que capteurs dits de « champ large »**. Ils permettent de détecter et de localiser les émissions électromagnétiques adverses, notamment celles des radars et des systèmes de communication, et d'orienter ensuite des **capteurs dits de « champ étroit », chargés de confirmer visuellement la nature et la position précise des cibles.** Ce rôle est assuré en particulier par des drones d'observation, tels que l'Orlan-10 côté russe, qui viennent compléter et affiner le renseignement initial fourni par la guerre électronique.

De fait, **toute émission électromagnétique non maîtrisée expose immédiatement le système à une localisation précise, puis à une neutralisation rapide,** en l'absence de manœuvre ou de dispositifs de protection adaptés.

Cette vulnérabilité est encore accentuée par les capacités SEAD russes, notamment par l'emploi de missiles antiradar comme le Kh-31P. Ce type de missiles est utilisé aussi bien dans des actions destructrices que dans des missions visant à faire taire temporairement les radars et capteurs adverses, réduisant ainsi leur liberté d'action.

**Face à cette menace permanente, les forces engagées cherchent à réduire leur signature électromagnétique, voire à sortir temporairement du spectre. Cette adaptation se traduit notamment par l'utilisation de drones guidés par fibre optique qui permettent de s'affranchir du risque de brouillage des liaisons de données sans fil.**

Si **ce mode d'action s'avère particulièrement efficace dans des phases statiques du conflit, il présente toutefois des limites en situation dynamique**. De même, le poids et la traînée de la fibre réduisant la vitesse et la manœuvrabilité du drone, le rendant plus vulnérable aux moyens cinétiques classiques.

Parallèlement à la pratique filaire, on observe une diffusion croissante des techniques de reconnaissance automatique de cibles grâce à l'intelligence artificielle, qui permettent à un système de mener une phase d'attaque terminale de manière autonome une fois l'objectif désigné.

Les drones filoguidés : la parade ultime pour contrer le brouillage ?

**Les drones filaires sont particulièrement résilients face au brouillage.** Leur développement est donc logique dans un environnement électromagnétique particulièrement saturé où 75 % des drones étaient abattus par des systèmes électroniques en juillet 2024.

La longueur de la fibre optique utilisée est généralement comprise entre 5 et 20 km (bien que des prototypes atteignant jusqu'à 60 km aient été déployés récemment sur le front), modifiant la profondeur du champ de bataille, notamment pour le soutien et la logistique.

Le câble a une épaisseur d'environ 0,25 mm et la fibre employée est majoritairement de la fibre optique plastique (provenant souvent de Chine).

**Le guidage par fibre optique assure une communication directe et sécurisée entre le drone et son opérateur, pour l'instant insensible au brouillage et au leurrage, puisqu'il n'émet aucune onde radio**. Cette liaison filaire garantit une transmission à très haut débit et plus rapide, offrant des images vidéo d'excellente qualité et permettant une navigation précise jusqu'à l'impact, même en

environnement dégradé. La fibre optique empêche également toute détection ou localisation du drone et de son pilote.

De nouveaux usages de la fibre optique apparaissent régulièrement comme **les drones répéteurs russes. Comme des antennes relais, ils reçoivent le signal de l'opérateur par une connexion filaire et le transmettent à plusieurs drones d'attaque** autour de lui, ce qui augmente leur portée et permet de frapper des cibles plus éloignées.

Malgré leurs nombreux avantages **les drones à fibre optique présentent plusieurs limites opérationnelles.** Le tambour de fibre alourdit l'appareil, ce qui réduit l'autonomie, la charge utile (caméras, capteurs, explosifs). La présence du câble complique également les manœuvres rapides et complexes, en particulier à basse altitude, où il peut s'emmêler dans l'environnement ou se rompre. Cette contrainte impose un pilotage plus prudent, rendant **le drone moins rapide et moins maniable qu'un drone FPV classique.** Enfin, ces drones sont plus chers à produire que les drones classiques.

Ces drones ne sont pas non plus invulnérables au brouillage. En effet, **les drones filoguidés continuent d'émettre des émissions électromagnétiques** pendant leur fonctionnement, bien que ces dernières soient très faibles et difficiles à détecter. Un industriel auditionné par vos rapporteurs a confié travailler sur des systèmes de détection de ces émissions, avec quelques résultats.

Enfin, **l'emploi de fibres optiques par ces drones engendre des risques pour l'environnement.** La masse de fils abandonnés peuvent piéger la faune, entraînant asphyxie et entraver la circulation des véhicules civils et militaires, notamment sur les axes routiers. En outre, ces câbles, peu biodégradables, pourraient persister dans l'environnement pendant plusieurs siècles.

ii. Proche et Moyen-Orient

**En Mer Rouge, la Marine nationale s'est illustrée en détruisant des drones qui représentaient une menace contre ses frégates à l'aide de brouilleurs électromagnétiques.**

Lors de la séquence aérobalistique Iran-Israël de 2025, la maîtrise israélienne de la GE a renforcé une supériorité aérienne déjà acquise. L'Iran, malgré quelques tentatives de brouillage GNSS, fut incapable d'opposer une réelle résistance aux raids israélien et américain. **Cette séquence met en évidence la nécessité de disposer de moyens de suppression des défenses aériennes ennemies (SEAD) spécialisés. Ces moyens spécialisés ont été abandonnés par la France à la fin des années 1990 et doivent être reconquis dans les meilleurs délais.**

**Retour sur la séquence aérobalistique israélo-iranienne de 2024/2025**

L'acquisition de la supériorité aérienne dans le ciel iranien a été une condition nécessaire au succès opérationnel israélien dans la récente guerre des 12 jours. **Pour y parvenir, Israël a mené en avril et en octobre 2024, plusieurs vagues de missions de type SEAD visant à supprimer les défenses sol-air adverses, en Syrie, en Irak et en Iran.** Cette fenêtre d'ouverture a permis les dernières opérations menées directement dans l'espace aérien iranien, au plus près des objectifs ciblés, et en particulier l'opération américaine « *Midnight Hammer* » contre les sites nucléaires militaires iraniens.

Pour mémoire, voici un rappel des différentes phases de cette séquence aérobalistique inédite :

1°/ Attaque iranienne du 1er octobre 2024 sur Israël : selon des sources ouvertes, la défense aérienne israélienne aurait intercepté 99 % des salves balistiques iraniennes.

2°/ Puis réplique israélienne du 26/10 (« *Jours de repentance* ») : ciblage des batteries antiaériennes iraniennes à longue portée, des radars d'alerte avancée (opération de SEAD, destruction préventive des DSA iraniennes). **Ces frappes ont préparé une possible poursuite des opérations contre les installations nucléaires critiques et ont exposé la vulnérabilité de l'Iran, temporairement privé de ses défenses sol-air. Cette mission SEAD a considérablement accru la liberté d'action israélienne tout en renforçant sa manœuvre de dissuasion contre une nouvelle attaque iranienne,** dans un contexte où la force aérienne iranienne ne permettait pas de compenser la perte des batteries sol-air de longue portée.

3°/ Opération israélienne « Rising Lion » / « Guerre des 12 jours » : Israël a revendiqué deux objectifs dont la réalisation a conduit l'Iran à accepter la suspension des hostilités ; politique pour le premier (porter un coup d'arrêt au programme nucléaire militaire iranien avec des frappes sur les sites de Natanz, Fordow et Arak) et militaire pour le second (frapper l'arsenal balistique iranien avant qu'il ne puisse saturer le système multicouches de défense aérienne israélien).

En 12 jours, l'armée de l'air israélienne a effectué environ 1 500 sorties de combat, plus de 600 ravitaillements en vol et frappé près de 900 cibles iraniennes. **Ces raids ont mobilisé jusqu'aux deux tiers de la flotte d'aviation de chasse israélienne dans les jours qui ont suivi le 13 juin** et ont pu être menés grâce à un travail de ciblage et de renseignement, réalisé sur le temps long, avec l'appui américain. *Rising Lion* a ainsi permis aux Israéliens de démontrer leurs capacités à créer la surprise stratégique et opérative, dans une planification intégrée entre l'armée de l'air israélienne (IAF), le service de renseignement extérieur (MOSSAD), le tout grâce à l'emploi de moyens de guerre électronique. **Ils ont ainsi imposé leur propre *tempo* et obtenu des effets militaires rapides tout en minimisant les risques humains.**

### c. *La GE est l'affaire de quelques puissances militaires*

**La guerre électronique reste l'affaire d'un club restreint de puissances**. Les caractéristiques techniques détaillées des capacités de guerre électronique de nos compétiteurs et alliés demeurent difficiles à évaluer concrètement. Les puissances, les portées et gammes de fréquences des systèmes adverses sont des déductions ou des extrapolations, la coopération interalliée sur le sujet étant très limitée en raison du haut degré de classification de ces matériels.

**Les États-Unis demeurent probablement la puissance militaire la plus avancée en matière de GE** qui a été historiquement facteur de supériorité opérationnelle (furtivité, missiles antiradars, attaques électroniques incluant des intrusions cyber-électroniques testées dès le Kosovo en 1999, *etc*). Elle s'appuie notamment sur :

- ***La puissance de la R&D*** *(par exemple la maîtrise de la conception des composantes électroniques et de l'informatique embarquée à la pointe de la sophistication s'adossant sur la maîtrise des matériaux)*

- ***Le passif d'exploitation supérieur américain en matière de renseignement depuis des décennies*** *(recueil spatial et humain par les forces expéditionnaires, renseignement technique sur les équipements récupérés par divers moyens dans l'ensemble du globe) permettant probablement des bases de données ROEM uniques au monde.*

**Des puissances militaires comme Israël et l'Ukraine pourraient être aussi à de nombreux égards presque aussi avancées que les États-Unis**, en raison de leur écosystème d'innovation, de leur situation de guerre et de leur expérience opérationnelle.

**Comme vu précédemment, la Russie capitalise en Ukraine sur une GE historiquement très puissante et fortement modernisée durant les années 2010.** Des observateurs ont rapporté que certaines frégates russes déployées au large de la Syrie seraient équipées d'une version navale de brouilleurs GPS terrestres, ce qui montre une généralisation de cette capacité NAVWAR des unités terrestres vers les unités navales.

**L'armée populaire de libération chinoise n'est peut-être pas au même niveau que les États-Unis en matière de R&D mais elle bénéficie certainement d'un phénomène de rattrapage fondé sur l'espionnage et pleinement exploité par une supériorité maintenant établie en matière d'ingénierie de production**.

En termes de masse, la Chine inonde ses partenaires de composants GE bas coût à la qualité inégale. Pour autant, la modernisation à marche forcée de sa flotte maritime s'accompagne de l'arrivée de radars modernes comparables aux meilleures

productions occidentales. Ces progressions laissent supposer une maîtrise technique capable de concevoir une large gamme de capteurs de guerre électronique dans les domaines radar et radio sur des plateformes navales et aériennes.

### 2. Un objet multiforme selon les armées et les milieux

**Les conflits récents ont remis au goût du jour l'importance de la guerre électronique, particulièrement dans les conflits de haute-intensité entre puissances de force équivalente.**

Pour cette raison, la GE française, dans les espaces d'affrontement actuels pour chacune de ses armées, est essentielle.

#### a. *L'armée de Terre*

**Les particularismes de la guerre électronique terrestre relèvent d'abord de l'environnement contraignant qui lui est imposé. Le milieu terrestre, qu'il soit naturel ou urbanisé, dégrade fortement la propagation des ondes.** Il limite l'efficacité des capteurs comme celle des effecteurs, du fait des masques de terrain, des obstacles bâtis et de la variabilité des conditions de diffusion.

**Ces contraintes structurelles imposent de recourir à des plateformes spécifiquement dédiées, capables de surmonter les limites physiques** par des solutions techniques adaptées, telles que les drones, des mâts antennaires, une mobilité des structures et une capacité de puissance d'émission suffisante.

À ces contraintes physiques s'ajoute **une complexité opérationnelle** propre au milieu terrestre, **liée à la nature des cibles à traiter**. Selon les éléments transmis par l'armée de Terre, « *la gamme des cibles à traiter est différente de celle des autres armées, et beaucoup plus complexe car elles sont "noyées" parmi la multitude de moyens civils. Cela rend bien plus difficile la capacité à discriminer une cible d'intérêt parmi la masse de signaux* ». Cette imbrication étroite entre signaux militaires et civils accroît fortement la charge cognitive des opérateurs et exige des capacités avancées d'analyse, de tri et de discrimination électromagnétique.

Afin de compenser les limitations imposées par le terrain et d'accroître leur portée effective, **les moyens de guerre électronique terrestre sont souvent déployés à proximité immédiate de la ligne des contacts.** Comme le montre l'expérience ukrainienne, cette nécessité opérationnelle les expose toutefois à une détection rapide par l'adversaire et à une vulnérabilité élevée.

Dans un environnement fortement contesté et saturé, leur survivabilité repose donc sur des capacités accrues de mobilité, de discrétion et de protection, notamment sous blindage, condition indispensable au maintien de leur efficacité dans la durée.

La composition des unités de guerre électronique de l'AdT

**La guerre électronique sur le plan terrestre se structure en deux grandes catégories : d'abord les unités dites spécialisées où interviennent des techniciens et les unités dont les soldats - non techniciens - utilisent des équipements de guerre électronique.**

Le cœur de la guerre électronique terrestre française est celui de ses unités spécialisées soit **deux régiments, 44ème et 54ème régiments de transmissions** (environ 800 combattants chacun) et **la 785ème compagnie de GE** (environ cent personnes).

Ce dispositif repose sur des unités complémentaires couvrant l'ensemble du spectre tactique, opératif et stratégique.

**Le 54ème régiment de transmissions constitue le pilier tactique au niveau divisionnaire et corps d'armée**, assurant l'interception, la localisation et l'exploitation des émissions électromagnétiques adverses à courte distance, ainsi que la mise en œuvre de capacités d'attaque des réseaux ennemis.

**Le 44ème régiment de transmissions opère quant à lui aux niveaux opératif et stratégique,** en réalisant une veille permanente depuis le centre de guerre électronique de Mutzig, notamment en interceptant les liaisons radio longue distance et satellitaires au profit des forces et du renseignement national.

**Enfin, la 785ème compagnie de guerre électronique apporte une forte expertise technico-opérationnelle** en interception, exploitation des communications et cyberdéfense, tout en jouant un rôle clé d'innovation rapide grâce à sa capacité à concevoir et prototyper des solutions complètes en réponse à des besoins opérationnels non couverts.

**En terme organisationnel, ces trois unités sont placées sous l'autorité de la Brigade de renseignement et de cyber-électronique (BRCE) de l'armée de Terre.**

Cette brigade relève du commandement des actions dans la profondeur et du renseignement (CAPR), dont **la mission centrale est d'accélérer la boucle renseignement–feux, c'est-à-dire de réduire au maximum le délai entre la détection d'un objectif, la prise de décision et son traitement par les moyens de feu**. La responsabilité du pilotage de la fonction de guerre électronique terrestre est assurée au niveau de ce commandement, sous l'autorité de l'officier général en charge des actions dans la profondeur et du renseignement.

**L'enjeu principal du segment « spécialisé » de la guerre électronique réside aujourd'hui dans la remontée en puissance du volet offensif et dans le renforcement des capacités et de l'expertise en guerre électronique radar.** Ces

deux dimensions apparaissent indispensables pour répondre aux exigences d'un engagement de haute intensité face à des adversaires technologiquement avancés.

Pour ce qui est **de la guerre électronique terrestre des « non-spécialistes », mise en œuvre par des moyens ou des unités non dédiées, peuvent être distinguées deux grandes catégories.**

**La première est la GE dite « *élémentaire* » mise en œuvre au plus près du combat par les sections de renseignement et de guerre électronique des régiments d'infanterie et par les pelotons de renseignement-détection des régiments de cavalerie.**

Ces unités constituent le premier niveau d'emploi de la guerre électronique au sein des forces terrestres. Dotées de véhicules équipés pour la détection, l'écoute et la localisation des émissions électromagnétiques adverses, elles ont pour mission principale d'appuyer directement la manœuvre des brigades interarmes.

Leur action vise à fournir aux chefs tactiques une meilleure compréhension de l'environnement électromagnétique immédiat, en identifiant les communications adverses et en contribuant à la protection des forces engagées. À l'échelle de l'armée de Terre, cette guerre électronique élémentaire représente un volume d'environ 200 combattants, qui, sans être des spécialistes de haut niveau, sont formés et dédiés à l'emploi de ces capacités au contact.

**La deuxième dimension est celle de la guerre électronique dite « *du combattant* », qui correspond à l'emploi direct de moyens de guerre électronique par les troupes de contact.**

Si l'utilisation de tels dispositifs n'est pas totalement nouvelle, ayant déjà été introduite lors des conflits asymétriques à travers les systèmes de brouillage anti-IED, elle prend aujourd'hui une importance croissante en raison de l'évolution des menaces sur le champ de bataille. Cette forme de guerre électronique répond désormais à des besoins opérationnels de plus en plus fréquents et immédiats.

**Le segment de guerre électronique du « combattant » se structure autour de trois enjeux majeurs.**

**Le premier concerne la lutte contre la menace des drones**, qui peut prendre la forme de dispositifs de détection, d'identification ou de brouillage visant à neutraliser ces vecteurs.

**Le second enjeu réside dans l'accroissement de la survivabilité des unités**, en particulier des postes de commandement, grâce à l'emploi de techniques de leurrage et de réduction de la signature électromagnétique.

**Enfin, la guerre électronique du combattant contribue à l'amélioration de la connaissance de la situation tactique** par l'emploi massif de capteurs automatisés, déployés au plus près du terrain, qui alimentent en temps réel la compréhension globale de l'environnement opérationnel.

Pour conclure, **le principal enjeu pour l'armée de Terre réside avant tout dans la diffusion de la guerre électronique au sein des unités.**

**Cet enjeu est double. Il s'agit d'abord de généraliser, sur le champ de bataille, l'emploi des équipements et des capacités de guerre électronique au contact de l'ennemi.**

Pour la guerre électronique dite élémentaire, **l'objectif est d'acquérir des capacités de surveillance électronique des communications adverses,** incluant l'interception et la localisation des émissions, mais aussi le leurrage et le brouillage, en dotant les unités de mêlée d'outils de guerre électronique semi-automatisés adaptés à un emploi tactique.

**Pour la guerre électronique du combattant, l'enjeu réside dans l'acquisition et la multiplication de ces outils au sein de l'ensemble des armes de contact**, en particulier chez les sapeurs, la cavalerie et le génie, afin de répondre aux menaces immédiates rencontrées sur le terrain.

**De même, cette diffusion suppose de rendre la guerre électronique réellement accessible aux unités qui la mettent en œuvre**. Cela implique un effort soutenu de simplification des équipements, mais aussi le développement d'une formation adaptée, permettant aux combattants non spécialistes de maîtriser efficacement ces capacités dans un contexte opérationnel exigeant.

b. *La Marine nationale*

**La guerre électronique navale est soumise à des impératifs et à des contraintes propres, intrinsèquement liés au milieu maritime** dans lequel elle s'exerce ainsi qu'à la structure des marines nationales.

Les caractéristiques de cet environnement, marqué par **de très grandes élongations, un nombre limité d'unités déployées, une logistique contrainte et une forte exposition des bâtiments isolés,** confèrent à la guerre électronique de la Marine nationale un caractère singulier.

En dehors de certains cas particuliers, comme les opérations amphibies ou littorales, elle repose sur une logique de discrétion, d'anticipation et de maîtrise de l'information, qui conditionne directement la liberté d'action des forces navales.

**Du fait des facteurs qui précèdent, la Marine nationale concentre prioritairement ses efforts de guerre électronique sur le domaine radar, avant le domaine radio**. Cette hiérarchisation s'explique par la nature même des menaces auxquelles les unités navales sont historiquement confrontées.

**La menace missile est en effet la plus dangereuse pour les bâtiments de surface.** Elle s'exprime principalement dans le domaine radar et représente à la fois le plus haut niveau d'exigence technologique à contrer et le risque de destruction le plus élevé pour les unités engagées.

**Ces risques, toujours d'une forte actualité, justifient l'équipement des bâtiments en moyens performants de détection, de brouillage et de leurrage radar, destinés à empêcher les chaînes de détection, de poursuite et de guidage adverses**. Ils sont augmentés aujourd'hui par l'essor de la menace drone qui impose une extension des capacités de guerre électronique à des vecteurs plus nombreux, plus discrets et parfois plus difficiles à détecter.

Dans le cadre de ce milieu et des menaces présentes**, la guerre électronique en mer peut être analysée selon deux grands contextes d'emploi distincts,** celui de la haute mer et celui des zones proches du littoral, en particulier à l'approche des points de congestion stratégique.

**En haute mer, la guerre électronique s'articule avant tout autour de l'impératif de supériorité informationnelle**, préalable indispensable à tout engagement opérationnel. Elle vise en premier lieu à assurer la maîtrise du spectre électromagnétique à l'échelle du théâtre d'opérations, ce qui suppose un contrôle rigoureux de la signature électromagnétique des unités de la Marine nationale ainsi qu'une capacité à les leurrer et à les brouiller (autodirecteur, télécommande, position GNSS) avant qu'elles n'atteignent leur cible permanente de détection, d'interception et de localisation des émissions adverses.

**Au-delà de cette maîtrise du spectre, la guerre électronique navale cherche également à perturber l'appréciation de la situation par l'adversaire.** Il s'agit d'introduire de l'incertitude et de la confusion dans sa lecture du champ électromagnétique par des actions de brouillage et de leurrage, afin de masquer les intentions réelles, de contraindre sa manœuvre et de faire peser une menace crédible d'emploi de la force.

Ces actions doivent rester efficaces malgré les distances importantes propres au milieu maritime et s'exercer aussi bien dans les domaines radar que radio. Enfin, **la guerre électronique en haute mer vise à parasiter, voire à neutraliser, le fonctionnement des capteurs adverses en appui direct du combat.** En empêchant ou en dégradant l'usage des capteurs ennemis, elle contribue à réduire leur capacité de détection et de ciblage et à accroître l'efficacité des actions cinétiques, tout en nécessitant une évaluation permanente des effets produits afin d'adapter la manœuvre dans le champ électromagnétique.

**À l'approche des côtes et, plus encore, dans les zones de congestion stratégique telles que les détroits ou les approches portuaires, les priorités de la guerre électronique évoluent sensiblement.** Dans ces environnements contraints, l'enjeu principal devient la protection des unités navales face à des menaces multiples et rapprochées, en particulier les missiles et les drones.

La maîtrise du champ électromagnétique vise avant tout à anticiper l'apparition de ces menaces, à en perturber les systèmes de guidage, de télécommande ou de positionnement, notamment par le brouillage des autodirecteurs et des signaux GNSS, et à empêcher leur acquisition efficace de la cible.

**Dans ce contexte, la guerre électronique s'impose comme un élément central de la défense des bâtiments, étroitement intégrée aux autres moyens de protection, et constitue l'un des déterminants majeurs de la survivabilité et de la liberté d'action des forces navales.**

Enfin, **il est important de rappeler que les ondes électromagnétiques ne traversent pas l'eau, à l'exception des ondes de très basse fréquence, dont la portée et les capacités restent toutefois limitées.** De ce fait, le milieu sous-marin échappe en grande partie au champ de la guerre électronique maritime. La lutte sous-marine ne repose donc pas sur la guerre électronique, mais principalement sur la guerre acoustique, qui constitue le mode d'action déterminant dans cet environnement spécifique.

**Dans ce cadre particulier du milieu, la Marine nationale développe elle-même des spécificités intrinsèques, directement liées à ses missions, à sa mobilité et à la permanence de ses déploiements.**

Du fait **de la présence de la France en Outre-Mer et l'ambition stratégique qui en découle,** ses unités sont présentes en continu sur l'ensemble des zones maritimes, ce qui confère à la guerre électronique navale une dimension à la fois opérationnelle et permanente.

**La particularité majeure réside en effet dans cette présence constante sur les théâtres maritimes**, posture qui permet de déployer en continu des capacités de surveillance du spectre électromagnétique embarquées qui constituent un atout stratégique majeur. Les unités navales contribuent ainsi à cartographier l'activité électromagnétique, à caractériser les comportements des compétiteurs et à enrichir la connaissance globale des environnements radar et radio.

De fait, **la Marine nationale est quotidiennement confrontée à ses compétiteurs dans le champ électromagnétique**, que ce soit à travers des interceptions, des interférences ou des actions de brouillage.

Contrairement à d'autres domaines qui ont pu connaître des phases de désengagement doctrinal, **la Marine n'a jamais délaissé les fonctions de guerre électronique et a maintenu des moyens de surveillance du spectre embarqués sur ses unités.** Elle dispose ainsi d'une expertise approfondie des systèmes radar et des pratiques électromagnétiques du monde maritime.

**Cette expérience s'est particulièrement développée face à la menace missile, historiquement considérée comme la menace majeure pesant sur les unités navales**. La rapidité d'évolution d'un missile, qu'il soit subsonique ou hypersonique, impose des délais de réaction extrêmement courts, exigeant des systèmes de détection et de contre-mesure parfaitement intégrés et maîtrisés.

**Plus récemment, la Marine nationale a également démontré sa capacité d'adaptation face à la menace drone, en obtenant plusieurs succès opérationnels grâce à l'emploi de brouilleurs électromagnétiques embarqués sur ses frégates**. Ces résultats illustrent à la fois la pertinence des choix capacitaires engagés et la capacité de la Marine à adapter ses dispositifs à l'évolution rapide des menaces.

**Enfin, une autre spécificité structurante réside dans l'intégration, au sein d'un même porteur, de l'ensemble des fonctions de guerre électronique**. Les bâtiments de la Marine nationale rassemblent en effet, dans leur système de combat, les capacités de surveillance du spectre, tant dans les bandes radio que radar, ainsi que les moyens de brouillage et de leurrage d'autodéfense destinés à contrer les menaces missiles et drones.

**Cette intégration organique permet une réactivité accrue et une coordination directe entre détection, analyse et action, condition essentielle dans un environnement où les délais de réaction sont extrêmement courts.**

### c. *L'Armée de l'Air et de l'Espace*

**Les besoins spécifiques de l'Armée de l'Air et de l'Espace (AAE) en matière de guerre électronique se distinguent nettement de ceux de l'armée de Terre et de la Marine nationale.**

Ils sont en effet **directement conditionnés par la nature de ses missions, au premier rang desquelles figurent la supériorité aérienne, la projection de puissance dans la profondeur et la crédibilité de la dissuasion nucléaire aéroportée.** Dans ce cadre, la guerre électronique constitue un levier central de liberté d'action et de survie dans des environnements contestés.

La conquête et la maîtrise de la supériorité aérienne

**La première exigence opérationnelle de l'AAE est la capacité à conquérir et à conserver la supériorité aérienne**. Toute opération interarmées repose en effet sur la liberté d'action dans la troisième dimension. Cette liberté

suppose de neutraliser ou de réduire les systèmes de défense aérienne adverses, qui sont aujourd'hui de plus en plus intégrés, mobiles et technologiquement avancés.

**La guerre électronique offensive joue ici un rôle déterminant, notamment à travers les missions de suppression des défenses aériennes ennemies (SEAD**). Celles-ci, à différencier des DEAD (destruction des moyens aériens), sont des moyens dédiés à la destruction des équipements sol-air à l'image par exemple des missiles anti- radiations, quand les DEAD sont un usage détourné d'un équipement, comme un bombe plante tiré sur un système sol-air.

La pénétration des environnements contestés et la crédibilité de la dissuasion

Au-delà de la seule supériorité aérienne, **l'AAE a pour mission de projeter la puissance et de frapper dans la profondeur, y compris au sein d'environnements fortement contestés caractérisés par des dispositifs de déni d'accès et d'interdiction de zone** (A2/AD). Dans ces **« bulles »** de protection durcies, la guerre électronique offensive constitue un outil essentiel pour percer les défenses adverses, désorganiser les chaînes de détection et de conduite de tir et assurer la survie des vecteurs engagés.

**La crédibilité de la composante nucléaire aéroportée repose notamment sur l'aptitude du raid à pénétrer un espace aérien protégé par des systèmes sol-air sophistiqués.** La guerre électronique y occupe une part croissante, tant pour la protection des aéronefs que pour la neutralisation temporaire ou durable des capteurs adverses.

Par ailleurs, **les moyens de la dissuasion étendue doivent être protégés contre toute tentative de contournement « par le bas » susceptible d'entraver leur liberté d'action.**

L'opération *Spider web* en Ukraine – évoquée plus bas - a démontré la vulnérabilité des bases militaires aux attaques de drones sur des matériels d'importance stratégique stockés dans la grande profondeur.

Dans cette thématique, **la guerre électronique joue bien évidement un rôle crucial car elle peut ajouter une couche protection supplémentaire** pour faire face à des attaques de mini-drones, isolés ou en essaims, en complément des dispositifs passifs et des capacités cinétiques.

Le continuum Air–Espace et la dimension verticale de la guerre électronique

**L'Armée de l'Air et de l'Espace** (AAE) présente une spécificité majeure : elle est **responsable du continuum vertical, qui s'étend du sol jusqu'à l'orbite géostationnaire, en passant par la très haute altitude** (THA). Cette responsabilité impose une approche globale et intégrée de la guerre électronique, couvrant à la fois la protection des aéronefs, celle des moyens spatiaux et la maîtrise des nouveaux espaces intermédiaires devenus des zones de confrontation.

Le champ électromagnétique, par nature transverse, irrigue l'ensemble de ce continuum. **Les besoins en guerre électronique de l'AAE doivent ainsi couvrir l'ensemble du spectre aérien et spatial afin de protéger les satellites de communication, de renseignement et de navigation, tout en étant capables de contrer les menaces transitant par ces milieux**. Cette extension verticale du champ de bataille impose une adaptation doctrinale et capacitaire, notamment face à l'émergence de nouveaux vecteurs évoluant en très haute altitude.

**La THA constitue en effet un nouvel espace de confrontation au sein du milieu air.** On y observe le développement de ballons stratosphériques et d'aéronefs solaires dits HAPS (High Altitude Pseudo-Satellites), conçus pour assurer des missions de télécommunication, d'observation, y compris radar et de renseignement. Ces systèmes, par leur endurance et leur positionnement intermédiaire entre aéronef et satellite, représentent à la fois une opportunité et une menace dans le champ électromagnétique.

**Dans ce contexte, plusieurs enjeux structurants émergent pour l'AAE.**

**Le premier consiste à détecter « vers » la THA**. Les HAPS sont difficiles à identifier en raison de leur faible signature électromagnétique et de leur altitude élevée. L'enjeu réside dans la capacité à distinguer des signaux faibles au sein d'un environnement électromagnétique saturé et bruité, ce qui nécessite des capteurs performants et des capacités avancées de traitement du signal.

**Le deuxième enjeu concerne l'interception et la neutralisation des menaces « dans » la THA**. Les intercepteurs devront être capables d'agir contre ces vecteurs malgré d'éventuelles mesures de brouillage ou de protection électronique. À terme, l'emploi de lasers de puissance, dirigés vers la très haute altitude voire vers l'espace, pourrait constituer un moyen électromagnétique pertinent de neutralisation, en complément des capacités cinétiques classiques.

**Le troisième enjeu réside dans la capacité à opérer « par » la THA.** Les HAPS, à l'instar des satellites d'appui aux opérations, peuvent devenir des plateformes d'action dans le champ électromagnétique, qu'il s'agisse de télécommunications, de renseignement ou de surveillance radar. Toutefois, étant par nature des systèmes pilotés ou télécommandés, ils demeurent vulnérables au brouillage de leurs liaisons de commande et de données, ce qui en fait à la fois des outils et des cibles de la guerre électronique.

**Enfin, la THA constitue également un espace de transit pour les armes hypervéloces dont la vitesse et la manœuvrabilité renforcent la survivabilité.** Ces vecteurs, capables de contourner ou de saturer les défenses, apparaissent particulièrement pertinents dans le cadre des missions de suppression des défenses aériennes ennemies (SEAD). Leur développement renforce encore la nécessité pour l'AAE de maîtriser le champ électromagnétique sur l'ensemble du continuum vertical.

Ainsi, **la très haute altitude ne constitue pas seulement un prolongement de l'espace aérien traditionnel, mais un espace stratégique intermédiaire dans lequel la guerre électronique joue un rôle déterminant, tant pour la détection, la protection que pour l'action offensive.**

La guerre électronique dans l'espace

**L'espace est devenu un milieu stratégique particulier, sans frontières et partagé par des usages civils et militaires étroitement interconnectés,** notamment à travers des technologies duales illustrées par Eutelsat ou Starlink.

**Longtemps préservé de la conflictualité, il est désormais marqué par l'émergence de menaces crédibles**, telles que les tirs antisatellites russes générateurs de débris, les capacités chinoises de brouillage et de lasers aveuglants, ou encore les manœuvres rapprochées de satellites à des fins d'espionnage.

Cette dépendance croissante des États aux capacités spatiales transforme l'espace en champ de contestation stratégique, alors même que le cadre juridique international demeure insuffisant.

**Fondé principalement sur le traité de 1967, il ne définit ni clairement le seuil de l'acte hostile, ni le principe de proportionnalité, laissant subsister une zone grise juridique favorable à des actions non cinétiques**, comme le brouillage, difficiles à qualifier et à sanctionner.

C'est dans ce contexte que **la guerre électronique** s'inscrit. Elle **constitue aujourd'hui un mode d'action central dans l'espace, en particulier à travers le brouillage, identifié comme l'un des leviers les plus efficaces et les plus flexibles.** Celui-ci peut être ajusté en intensité, allant de perturbations limitées jusqu'à la neutralisation durable de systèmes spatiaux, ce qui en fait un outil particulièrement attractif dans un environnement où la destruction physique reste risquée.

Toutefois, **dans un contexte de densification orbitale, le brouillage comporte aussi un risque de fratricide**, susceptible d'affecter ses propres capacités ou celles d'alliés, ce qui impose une maîtrise fine des effets produits.

**La protection des systèmes spatiaux passe dès lors par une évolution des architectures satellitaires**. Des satellites civils pourraient être progressivement dotés de capacités de surveillance de leur environnement et de capteurs plus résilients, reposant largement sur les technologies numériques et l'automatisation du traitement des données.

**La furtivité, au sens classique, reste très difficile à atteindre dans l'espace en raison des capacités d'observation radar et optique depuis le sol.** Elle repose donc moins sur l'invisibilité que sur une combinaison de facteurs incluant la réduction de la taille des satellites, le maintien d'une ambiguïté sur leurs capacités

réelles et un usage extrêmement maîtrisé des émissions, limitées dans le temps et déclenchées au moment opportun.

Dans ce contexte, les menaces se multiplient et tendent à se banaliser. La Chine et la Russie disposent déjà de capacités avancées de brouillage depuis le sol, de moyens de repérage précis et de systèmes laser susceptibles d'affecter des satellites.

**Le brouillage du GPS est devenu une préoccupation majeure, y compris pour l'aviation civile**, avec des zones durablement perturbées comme l'enclave de Kaliningrad ou certaines régions du conflit ukrainien, où l'absence de signal est devenue quasi permanente.

**Ce qui relevait autrefois d'un acte hostile clairement identifié est désormais un phénomène fréquent**, affectant régulièrement les équipements militaires occidentaux, notamment sur le flanc Est de l'Europe, au point que la France a saisi l'UIT pour dénoncer certains usages abusifs.

## C. LA GE EST AU CŒUR DES ÉVOLUTIONS TECHNOLOGIQUES DE LA GUERRE MODERNE

### 1. La numérisation de la GE densifie les menaces

#### a. *Le passage de l'analogique au numérique*

**L'évolution de la menace dans le champ électromagnétique résulte notamment de la numérisation des équipements.** Le passage de l'analogique au numérique a révolutionné la GE radio : les cartes radio-logicielles (*software-defined radio* (SDR)) ont permis l'analyse rapide d'un grand nombre de signaux sur un domaine étendu de fréquences.

Les signaux sont définis par des **protocoles informatiques (IP)** s'appuyant en partie sur des radio-logicielles. Alors qu'autrefois, un composant électronique dédié était nécessaire pour traiter le signal, **une carte radio-logicielle permet aujourd'hui de numériser le signal pour le traiter. Lorsque le signal évolue, la mise à jour du logiciel est requise.**

**Les avantages opérationnels du numérique sont nombreux**. À titre d'illustration :

-**La numérisation des équipements permet de changer très rapidement et directement les fréquences utilisées** (quelques heures). Un cœur de brouillage numérique programmable permet d'adapter les formes d'onde de brouillage à la cible ;

-grâce aux « *software-defined radio* » (SDR), **l'accélération des boucles d'innovations technologiques dans le champ EM** (de deux à trois ans en analogique à 6 à 8 semaines *via* des mises à jour des radio-logicielles) ;

**- un séquençage des signaux collectés beaucoup plus fin et précis que celui permis par la GE analogique.** Notamment, la GE numérique passive rend possible une détection avec une probabilité d'interception de 100 % sur 360°, sur l'ensemble du spectre, en permanence, et cela même dans un environnement spectral très dense. Cette dernière condition nécessite de pouvoir détecter même lorsque deux impulsions arrivent en même temps ;

**-La numérisation des équipements permet des charges EM réduites** propices à une dispersion des moyens sur un grand nombre de porteurs dans une optique de résilience (ex : milieu spatial) ;

**La numérisation croissante du spectre entraîne une multiplication des sources EM et une densification de la menace, tant en nombre de signaux à intercepter, que d'extension des bandes de fréquence et de complexification des formes d'onde.**

**b.** ***Un écosystème stimulé par la prolifération des technologies civiles***

**L'écosystème de la GE est largement transformé par la prolifération des technologies commerciales civiles, parfois plus performantes que certaines technologies militaires anciennes**. On peut notamment citer la résilience accrue du multi-GNSS sur un smartphone par rapport à un récepteur GPS développé dans les années 1990. Beaucoup de ces systèmes civils sont « SDR », les radio-logicielles pouvant notamment s'acquérir librement pour quelques centaines d'euros sur les grandes plateformes de vente en ligne.

**Les menaces EM s'exercent potentiellement autant à l'égard des infrastructures civiles que militaires**. Ces infrastructures deviennent par ailleurs de plus en plus difficiles à distinguer tant certaines technologies sont désormais duales, à l'image des réseaux de téléphonie mobile, du *wifi* ou encore des systèmes de positionnement GNSS.

**c.** ***Vers le combat cyber-électronique***

**La numérisation des signaux EM accroît la porosité entre le cyberespace et le champ EM**. En effet, les ondes EM (contenant) peuvent être le vecteur d'une charge cyber (le contenu). On assiste donc à l'émergence d'une convergence des opérations de cyberdéfense et de guerre électronique consubstantielle à un écosystème d'exploitation du spectre EM reposant sur la programmation numérique. La cyberdéfense et la GE ont un domaine de recouvrement principalement au niveau tactique, mais qui est appelé à s'étendre du fait de la numérisation croissante des signaux.

**Le combat cyber-électronique peut être défini comme la combinaison des effets de la GE et des opérations de cyberdéfense visant à dénier l'accès aux spectres électromagnétiques et aux réseaux, à exploiter les vulnérabilités des systèmes adverses ou encore à protéger ses propres systèmes.**

À date, **l'injection d'une charge cyber par les ondes demeure relativement rare et s'exerce plutôt au niveau stratégique.** En Syrie en 2007 lors du raid sur Dar-el-Zor[14], l'aviation israélienne a utilisé les liaisons existantes entre les radars de défense sol-air syriens pour injecter une charge informatique visant à leurrer les DSA à l'aide de faux signaux.

**L'horizon de développement du combat cyber-électronique reste le niveau tactique, au travers notamment de la « lutte informatique offensive » (LIO).**

**En France, le COMCYBER a d'ailleurs été désigné « *pilote de l'aptitude interarmées guerre électronique* ».** Il a conçu une stratégie d'opérationnalisation de la guerre dans le champ EM. De manière générale, les partenaires principaux de la France, tout comme l'OTAN, tendent à structurer le lien entre GE et Cyber sur la base d'une plus forte interaction.

**Les États-Unis conceptualisent la guerre électromagnétique comme une partie intégrante du milieu CYBER**. La reconnaissance de la convergence cyber-électromagnétique a placé le *US Cyber Command* comme responsable de la GE.

**Les Britanniques considèrent que les activités relatives au spectre électromagnétique et au cyberespace forment un seul et même milieu, le « *Cyber and Electromagnetic Domain* » ou CyEM.** À ce titre, la guerre électromagnétique est traitée par le prisme cyber-électromagnétique.

**Le Royaume- Uni considère cette zone de convergence comme un 5ème domaine d'opération à part entière, aux côtés des domaines d'opérations terrestre, aérien, naval et spatial.** La validation par la dernière revue stratégique parue début juin de la création d'un commandement opérationnel, le « *Cyber Electromagnetic Command* », suivant un modèle assez comparable au COMCYBER français, devrait encore renforcer l'intégration des deux composantes.

---

[14] *L'opération Orchard est une opération militaire exécutée par l'armée de l'air israélienne le 6 septembre 2007 sur un bâtiment proche de Halabiyé, dans le gouvernorat de Deir ez-Zor en Syrie.*

### 2. La course à l'innovation réactive la dialectique glaive/bouclier

#### a. *Une accélération du cycle d'innovation*

**La numérisation de la GE se traduit par une évolution accélérée des cycles de vie des systèmes**. La GE programmable par radio-logicielle entraîne ainsi un cycle d'innovation extrêmement rapide. Comme vu précédemment en Ukraine, ce cycle est aujourd'hui de l'ordre de trois mois mais ne cesse de s'accélérer, dans une course incessante entre les moyens d'action et les moyens de parade. **Sur le front, la variation des composants électroniques et des fréquences utilisées est parfois de l'ordre de 15 jours.**

**La capacité des industriels et des opérationnels à s'adapter au rythme accru du cycle d'innovation est un véritable facteur de supériorité opérationnelle**. En l'absence d'une innovation de rupture, l'accélération du cycle d'innovation prend la forme d'une course sans fin, au cours de laquelle les équilibres sont perpétuellement instables.

#### b. *La guerre des contre-mesures*

**L'accélération du cycle d'innovation est rendue possible par une adaptation permanente des contre-mesures et contre-contre-mesures aux dernières innovations tactiques.**

L'automatisation des processus est au cœur de cette accélération. En effet, la réactivité d'un système de GE face à une menace est un élément clé afin d'assurer l'efficacité de sa détection et le déclenchement de la contre-mesure. Le temps de réaction moyen est de quelques millisecondes.

Ainsi que vos rapporteurs l'ont présenté *supra*, face à la généralisation du brouillage des liaisons de données tactiques des drones en Ukraine, les drones filoguidés ou drones filaires ont profondément impacté l'utilisation et les performances des drones sur le front dès 2024.

**L'apparition en 2023 sur le front ukrainien de drones en carton a également constitué une contre-contre-mesure intéressante** puisque ces drones n'avaient pas de surface équivalente radar (SER) capable de réfléchir les ondes électromagnétiques, les rendant plus difficiles à détecter.

### 3. La GE catalyse les ruptures technologiques

#### a. *Les perspectives ouvertes par l'IA*

La mise en œuvre de briques d'intelligence artificielle dans le champ de la GE ouvre de nombreuses perspectives.

L'IA devrait ainsi permettre :

- **Un meilleur recueil du ROEM et une meilleure détection des cibles**. Le déploiement de briques d'intelligence artificielle semble indispensable afin notamment d'aider à la discrimination des cibles ou encore à raccourcir la boucle détection (ex. d'une émission, d'une unité) – réaction (ex. brouillage). Aujourd'hui, dans la lutte anti-drones, les brouilleurs utilisant de l'IA pour détecter la bande de fréquence utilisée par un drone permettent d'éviter d'émettre avec une très forte puissance pour détecter dans beaucoup de bandes de fréquences différentes. En outre, les algorithmes permettant le pilotage des drones seront de plus en plus résistants au brouillage. D'après les éléments transmis par MC2 Technologies, les brouilleurs traditionnels devront brouiller 100 fois plus fort pour neutraliser le drone. L'analyse du protocole de pilotage qui sera conduite par une IA intégrée au brouilleur *« fera gagner un facteur 1000 de puissance* ».

- **Une évolution beaucoup plus rapide des bibliothèques de GE**. Déployer des briques d'IA permettra d'accélérer le traitement des signaux EM (gain de facteur 5 à 10 pour la mise à jour des bibliothèques de GE). Il est ainsi nécessaire que les systèmes opérationnels soient équipés d'enregistreurs spécifiques afin que les données opérationnelles puissent être utilisées pour l'apprentissage des algorithmes utilisés par l'IA.

- **Une meilleure exploitation des données numérisées et une aide à la décision.** L'IA apporte d'ores et déjà une aide significative dans le traitement des informations de masse, à l'instar de nouveaux outils dans l'environnement ARTEMIAS IA aujourd'hui exploités par la DRM. Les algorithmes d'intelligence artificielle utilisés devront être les plus fiables et frugaux possibles afin d'être embarquables dans des plateformes contraintes. Un drone intégrant des briques d'IA pourra prendre des images et ainsi recaler sa trajectoire, même en environnement brouillé (odométrie visuelle). L'IA lui permettra de naviguer de manière autonome.

- **L'émergence de nouvelles capacités** : l'industriel Thales a ainsi expliqué s'appuyer fortement sur son département IA afin d'introduire de nouvelles capacités grâce à cette technologie (pistage de communications hybrides, nouvelles formes d'ondes, classification, etc.) ou à l'amélioration des capacités existantes (par exemple, amélioration de la phonie, identification des menaces). **Les experts évoquent notamment l'émergence d'une « GE cognitive » reconfigurable très rapidement grâce aux techniques d'IA permettant *in fine* des modes d'action proactifs en fonction des modes opératoires de l'adversaire.** Par exemple, il deviendrait possible de générer rapidement une forme d'onde sur-mesure, capable de casser la liaison adverse ciblée de façon précise et efficace.

- **Soulager la charge de travail des opérateurs et programmateurs de GE, qui relèvent souvent de la catégorie des sous-officiers et dont la charge de travail n'a eu de cesse de se complexifier avec la numérisation de la GE.**

De façon générale, ainsi que l'a plaidé l'ONERA devant vos rapporteurs : « *un effort devra porter sur la numérisation le plus près possible derrière l'antenne afin de pouvoir implémenter ensuite des traitements numériques au plus tôt et de tirer profit des capacités de l'IA dès la création.*

*Ces numérisations ont comme caractéristiques de se faire à très haute fréquence (plusieurs milliards d'échantillons par seconde, chaque échantillon étant codé sur un grand nombre de bits.* ***Il faut toutefois prêter une attention particulière au besoin en données réelles pour l'apprentissage car il est indispensable d'enregistrer des données opérationnelles et faire évoluer les traitements basés sur de l'IA sans remettre en cause le « hardware »***.

**L'un des défis tactiques majeurs de la GE consiste aujourd'hui à introduire de l'IA dans des capacités de GE embarquées.** En effet, afin que l'IA soit un véritable « *game-changer* » tactique sur le champ de bataille, les puissances de calcul embarquées doivent encore être considérablement renforcées. Cela implique d'attendre encore quelques années avant que ces technologies atteignent leur pleine efficacité.

*Le défi des Data hub embarqués (DHE)*

**Les DHE répondent au défi du traitement rapide de flux croissants de données par des capteurs toujours plus intelligents et sensibles**. Les DHE permettront d'obtenir rapidement voire instantanément une météo spectrale (hypervision du spectre EM) et d'analyser très rapidement des comptes rendus de missions. Ce faisant, ils permettront d'accroitre la qualité et la rapidité d'actualisation des bibliothèques de GE.

L'enjeu des DHE consiste dans la possibilité de procéder à de la fusion de données en temps réel au sein d'un réseau de capteurs hétérogènes. L'IA des DHE aide à discriminer les sources EM lorsque certaines bandes de fréquences sont saturées.

La Marine nationale notamment a déjà testé l'embarquement de plusieurs DHE à bord de ces bâtiments. Leur utilisation à bord des frégates de premier rang offrirait de véritables atouts.

### b. *Demain, le quantique ?*

**La révolution quantique, telle qu'elle est présentée dans les médias, permettrait, à l'instar de l'IA, de meilleures capacités de recueil et d'exploitation des données de GE.**

Elle pourrait notamment permettre **un renforcement notable des performances des récepteurs de GE (en sensibilité et bande passante) en offrant des capacités de calcul très fortes pour numériser en temps réel toutes les bandes de fréquences et miniaturiser des antennes.**

**Ces capacités pourraient également casser les clés de chiffrement** ainsi que l'aléa des évasions de fréquences, tout en offrant des moyens de synchronisation stables pour la conservation des capacités de positionnement en ambiance EM contestée.

Selon les propos recueillis par vos rapporteurs, **des industriels comme Thales investissent déjà largement dans ce domaine de recherche**, sur de nombreux projets comme les antennes de réception ultracompactes quantiques en bande basse.

**Les technologies quantiques n'ont pas encore atteint leur maturité de développement**. D'après les informations transmises en audition, les technologies quantiques, bien que prometteuses, ne seront pas effectives dans le domaine du renseignement avant 2030.

### 4. Le partage du spectre entre usages civils et militaires est une gageure

Si le ministère des Armées est affectataire exclusif de certaines bandes de fréquences, il en partage aussi un nombre croissant avec des affectataires civils.

**Le spectre électromagnétique est en effet un bien commun partagé entre différents utilisateurs mais pour les forces armées, disposer de la possibilité d'utiliser une bande de fréquences (liberté d'accès) et l'utiliser dans des conditions techniques répondant à leurs besoins spécifiques (liberté d'emploi) est crucial pour les opérations.**

Le cadre national défini par le tableau national de répartition des bandes de fréquence (TNRBF) permet de définir celles réservées pour des usages militaires ou utilisables en partage avec d'autres affectataires. **Pour la Défense, la stabilité de ce cadre est une première garantie en national de la liberté d'accès et d'emploi.**

Au niveau européen, l'harmonisation[15] des bandes de fréquences utilisables à des fins militaires réalisée par l'OTAN correspond aux besoins français.

**Le spectre radioélectrique est cependant une ressource finie dont la limite physique s'impose à ses usagers. Dans ce contexte, une redoutable compétition pour l'accès aux bandes les plus convoitées au regard de leur potentiel d'utilisation est engagée depuis plus de 25 ans**, **chaque affectataire cherchant à faire prendre en compte ses besoins spécifiques.**

**Dans un contexte de pénurie de cette ressource, il est crucial de garantir une utilisation optimale des fréquences attribuées au ministère des armées, sachant qu'en 25 ans, le spectre a connu deux réorganisations** :

---

[15] *L'accord mixte civilo-militaire des fréquences de l'OTAN (NJFA) a été co-construit au sein de l'Alliance atlantique en ce sens.*

- de 2000 à 2015, une réorganisation massive a été entreprise au bénéfice des bandes de fréquences utilisées par la téléphonie mobile 2, 3 puis 4G. À cette fin, des bandes de fréquences ont été « nettoyées » de leurs usages historiques afin de permettre de nouveaux usages. Pour le ministère des Armées, qui disposait historiquement d'un « quasi-monopole » sur le spectre, cette réorganisation a occasionné des opérations de migrations importantes de faisceaux hertziens (FH) dans une partie plus haute du spectre ou de réduction de taille de bande radar.

- de 2015 à 2025 : les possibilités de libération massives de bandes ayant été atteintes, l'effort du ministère s'est porté sur un partage du spectre plus ou moins satisfaisant au profit de solutions comme le *Wifi* et l'Internet des objets. Au plan technique, cette phase s'est accompagnée de développement de solutions permettant d'exploiter les plus hautes fréquences.

**Désormais, les libérations de spectre sont synonymes d'abandon d'usages qui signifient pour le ministère des armées la perte de capacités majeures difficiles ou impossibles à retrouver ailleurs dans le spectre.** L'identification de solutions en partage est extrêmement complexe et les études techniques très longues car mobilisant beaucoup de ressources.

Dans ce contexte, outre l'optimisation des usages en gestion ainsi que les efforts de recherche et développement permettant un usage plus efficace et rationnel de ces bandes, des efforts doivent être conduits afin de conquérir pour les forces armées un accès au spectre là où il est – encore – disponible.

### 5. Une saturation du spectre EM par ses usagers

**Le spectre EM est de plus en plus saturé avec une utilisation de bandes de fréquences de plus en plus hautes, ce qui pose un défi croissant aux armées pour continuer à « entendre » dans un contexte d'émissions croissantes.**

Outre cette difficulté d'écoute, **le risque de brouillage intentionnel ou non est une menace croissante** du fait de l'utilisation croissante des radiofréquences et d'une augmentation importante des débits et de la masse d'information échangée sur les liaisons sans fil.

Selon l'agence nationale des fréquences (ANFR), **cette tendance**, qui ne va faire que s'accentuer, **est encouragée par l'essor massif de certains usages dans le champ de l'Internet des objets** (capteurs intelligents, véhicules autonomes, territoires intelligents, domotique, « *smart grids* », industrie 4.0).

On assiste de fait **à une exploitation toujours plus poussée du spectre radioélectrique qui a un impact sur les infrastructures vitales et particulièrement sensibles.**

**En mer par exemple, la saturation du spectre résulte notamment du nombre très élevé de radars de navigation, essentiellement civils**. À cet égard, l'IA pourra notamment aider à discriminer au sein des interceptions de la Marine nationale entre radars ennemis et amis dans les bandes de fréquences saturées, notamment à proximité des côtes.

**Il importe par conséquent d'avoir un plan de veille actualisé des radars militaires de la zone afin de discriminer les émissions les plus pertinentes du point de vue des forces armées.**

### 6. Le risque d'utiliser le spectre contre soi-même est réel

**L'utilisation de l'énergie EM sur l'ennemi induit un risque fratricide pour l'« ami » : on parle alors de nécessaire « compatibilité électromagnétique » d'une action EM vis-à-vis de son propre dispositif.**

**En voulant rendre sourd l'ennemi par la mise en œuvre d'un brouillage à forte puissance, une force armée peut ainsi se rendre elle-même sourde** et incapable de discriminer les sources d'émissions EM.

Ce cas de figure se présente notamment lorsqu'un brouillage omnidirectionnel est mis en œuvre, *a contrario* d'un brouillage directif qui vise à ne pas disperser l'énergie utilisée aux fins de brouillage.

**La compatibilité électromagnétique est également un risque pour l'armée de l'air et de l'espace lorsqu'elle envisage d'utiliser un brouilleur aéroporté dans un aéronef qui contient de puissants radars.**

Afin d'éviter le risque fratricide, une véritable « manœuvre » de GE est ainsi nécessaire dans le cadre d'outils de maîtrise et gestion du spectre électromagnétique.

## II. LA REMONTEE EN PUISSANCE DE NOS CAPACITES DE GE SOULEVE DES DEFIS MULTIPLES

**Si la France n'est en aucun cas dans une situation critique en termes de maîtrise des techniques modernes de guerre électronique**, la rapidité des évolutions techniques, l'émergence de conflits de haute intensité et la place que cette forme de combat retrouve aujourd'hui, **militent à l'évidence pour une remise à niveau de ses capacités.**

## A. LE DÉFI CAPACITAIRE POUR LES ARMÉES FRANÇAISES

### a. *Une priorité clairement identifiée par le Chef des armées*

**Lors de son discours de Brienne le 13 juillet 2025, le président de la République a évoqué la guerre électronique comme une *« zone de fragilité »*, évoquant la nécessité de « *renforcer notre défense aérienne et nos moyens de guerre électronique* ».**

À l'occasion de ses vœux aux armées le 15 janvier 2026, le président de la République a ciblé la remontée en puissance des capacités des armées françaises dans le champ de la guerre électronique : « *La capacité des armées à s'engager à court terme sera améliorée et accélérée. Ce troisième objectif se décline à travers plusieurs lignes d'action. Il s'agit d'améliorer la protection de nos forces : défense surface-air, lutte anti-drone, guerre dans le champ électromagnétique, où nous avons vu à chaque fois des nécessités d'aller plus vite parce que la compétition est plus forte.* »

**L'EMA, en lien avec le COMCYBER et les armées, pilote les travaux d'opérationnalisation de la « guerre dans le champ électromagnétique » (GCEM).**

**Dans ce cadre, glissement sémantique qui n'est pas indifférent, le terme de « *guerre électromagnétique* » devrait à court terme remplacer le terme de « *guerre électronique* » s'agissant du niveau tactique, tandis que le terme de « *guerre dans le champ électromagnétique* » (GCEM), plus englobant, sera utilisé pour les niveaux opératif et stratégique.**

**Par ailleurs, la GE opérative et offensive devrait notamment faire l'objet d'efforts substantiels de remontée en puissance dans le cadre des « *surmarches* » budgétaires et de l'actualisation de la LPM 2024-2030.**

### b. *Une stratégie visant trois effets opérationnels majeurs*

**La stratégie d'opérationnalisation de la GCEM est aujourd'hui guidée par trois « *effets opérationnels* » majeurs, communs à l'ensemble des milieux.**

i. Réduire la probabilité d'attrition de « forces vives » amies:

- ***Accroître la survivabilité de nos soldats et de nos plateformes habitées,*** *qu'elles soient terrestres, navales ou aériennes, via un renforcement du leurrage EM et du brouillage d'autoprotection directement portées par nos plateformes. Face à la généralisation du brouillage GNSS sur les théâtres, nos systèmes doivent être résilients face à l'absence de GNSS ;*

- ***Multiplier l'emploi de plateformes déportées pour compliquer/perturber l'appréciation de situation de l'adversaire****, grâce, par exemple, à des drones d'accompagnement de force, des vecteurs de charges EM (simulant par exemple des SER[16] d'avions de chasse ou de bâtiments de combat de la Marine.*

ii. Prendre l'adversaire de vitesse :

- ***Détecter rapidement tout système émettant ou recevant un signal afin d'en caractériser et localiser le vecteur.*** *Des efforts sont à porter sur les capteurs spatiaux et sur la capacité à « chaluter » de la donnée de masse et hétérogène, à la stocker dans des « data hub embarqués » (DHE) et à l'analyser rapidement grâce notamment à l'IA ;*

- ***Disposer d'une connectivité robuste et redondante entre capteurs et effecteurs*** *(créer des bulles de connectivité hybrides : 5G, SATCOM LEO[17]) afin de disposer d'un réseau multi-senseurs multi-effecteurs (RM2SE) ;*

- ***Perturber immédiatement l'appréciation de situation et la manœuvre de l'adversaire par des actions coordonnées entre composantes tactiques, en défense et en attaque, dans les domaines EM et cinétiques*** *d'où le besoin d'un C2 robuste capable de planifier, conduire, coordonner nos actions ; de drones offensifs dans les trois milieux et d'actions depuis l'espace comme vers l'Espace.*

iii. Gagner en puissance sur l'adversaire

- ***Gagner d'abord « en masse », à coûts maîtrisés*** *par le biais d'une augmentation du nombre de plateformes habitées complexes, à haute valeur ajoutée (navires, avions et véhicules blindés relativement coûteux) et, en complément, de flottilles de drones/robots dans les trois milieux, répartis sur le théâtre d'opération.*

*Il convient néanmoins de se garder du mirage du « tout low-cost » : l'opération américaine « Midnight Hammer » (21-22 juin 2025), en appui des frappes israéliennes, vient rappeler que les moyens du haut du spectre sont déterminants pour délivrer des effets stratégiques puissants et déstabilisateurs, ce qui plaide en faveur d'un mix équilibré.* ***Le « low cost » sature l'adversaire et ouvre des failles que le « high cost » va venir exploiter.***

- ***Détruire les capacités de l'ennemi par une contribution efficace des capteurs et effecteurs EM à la fonction acquisition-ciblage cinétique*** *grâce notamment à une optimisation de la boucle OODA (Observer, orienter, décider, agir) renforcée par l'emploi d'IA (fusion de données et aide à la décision de manœuvre par une IA de combat ;*

Aujourd'hui, **le contexte géostratégique nous pousse à recouvrer des capacités de brouillage offensif, d'attaque électromagnétique de forte puissance, que ce soit au niveau des communications ou des radars**. Les armées devront être en mesure de conduire des opérations offensives coordonnées dans les champs EM et cyber (enjeu de la « *lutte informatique offensive* » (LIO tactique).

### c. *Des besoins spécifiques selon les armées et certains espaces*

i. L'armée de Terre

**Dans le cadre d'un conflit de haute intensité, la GE de l'armée de Terre a vocation à appuyer les unités interarmes déployées en opération :** la GE du combattant, non spécialisée, permet de protéger les forces et a donc vocation à être déployée de manière « massive ».

La GE élémentaire opère en appui des brigades interarmes. Insérée au sein d'unités multi-capteurs, elle participe aux missions de reconnaissance du terrain et agit sur l'adversaire grâce au brouillage moyenne puissance.

Enfin, les unités spécialisées (54 et 44ème régiments de transmissions) sont déployées en appui des niveaux division et corps d'armée afin de produire le renseignement nécessaire à la manœuvre, de détecter les cibles à valeur ajoutée et de désorganiser la manœuvre adverse grâce au brouillage forte puissance.

**Comme l'ensemble des unités de guerre électronique, ces unités sont confrontées à un besoin marqué de réinvestissement du champ offensif.** Les capacités de brouillage à forte puissance, en particulier, ont été largement délaissées au cours des dernières décennies en raison de l'engagement prioritaire dans des

---

[16] *Surfaces équivalentes radar*

[17] *Communications satellitaires en orbites basses*

conflits asymétriques dans lesquels la supériorité électromagnétique adverse était limitée. Cette situation a conduit à une érosion progressive des savoir-faire et des moyens dédiés au brouillage offensif.

Or, face à des puissances disposant de réseaux de communication résilients, redondants et durcis, cette lacune devient critique. La perspective d'un combat de haute intensité impose ainsi de reconstituer rapidement des capacités de brouillage de forte puissance et de longue portée, notamment dans les bandes VHF, UHF et GNSS, afin de perturber efficacement les communications, la navigation et les systèmes de commandement adverses.

**Par ailleurs, si l'armée de Terre a acquis au fil des années une expertise solide dans le domaine de la guerre électronique radio, elle doit désormais renforcer de manière significative ses compétences en guerre électronique radar, en particulier dans sa fonction de renseignement.**

Cette montée en compétence est essentielle pour « l'acquisition-feux » dans une perspective de neutralisation des moyens adverses à haute valeur ajoutée dans la profondeur.

La capacité à détecter, caractériser et localiser les radars adverses permet, non seulement d'identifier les dispositifs de défense et d'attaque ennemis, mais aussi de prioriser les objectifs, d'éclairer la manœuvre et de faciliter l'engagement des feux, qu'ils soient terrestres, aériens ou de longue portée.

Le renforcement de cette expertise constitue donc un levier clé pour améliorer l'efficacité globale du renseignement et de l'action dans la profondeur.

Enfin, ces ambitions se heurtent à un enjeu transversal de modernisation des équipements dont l'absence ferait peser un risque réel de dépassement technologique face à des adversaires ayant, au contraire, poursuivi des efforts soutenus dans ce domaine.

**La modernisation des capteurs, des effecteurs et des architectures de traitement apparaît ainsi indispensable pour garantir la crédibilité et la pérennité des capacités de guerre électronique spécialisées dans les années à venir.**

**Des investissements budgétaires significatifs abondant le programme 146 de la mission Défense doivent être conduits afin de permettre à l'armée de Terre de mettre en œuvre ses objectifs de GE.** Il sera notamment indispensable de densifier le segment spécialisé en le dotant de capacités sous blindage de détection et de localisation des radars, et d'attaque des communications et des réseaux adverses, pour être en mesure de conquérir la supériorité dans le champ électromagnétique et plus globalement sur le champ de bataille.

**Très concrètement, la capacité détenue par le 54ème régiment de transmissions pourrait être dédoublée, en créant un second régiment tactique de GE pour répondre à l'objectif de l'armée de Terre de constituer un corps d'armée pleinement opérationnel à l'échéance 2030.**

ii. La Marine nationale

**Il apparaît nécessaire que la Marine nationale continue de consolider son socle en matière de maîtrise du spectre électromagnétique : avant d'attaquer et afin de se défendre, il faut être en mesure de comprendre l'environnement**. L'augmentation du nombre de ses capteurs dans les domaines radar et radio et l'amélioration des capacités de traitement (rapidité, qualité de l'analyse, complémentarité des moyens) sont indispensables pour répondre aux défis de la haute intensité.

**Armé par la Marine nationale et mis à disposition de la DRM, le bâtiment Dupuy–de-Lôme (DPL) a toute sa pertinence dans le dispositif stratégique de recueil du renseignement (ROEM)**. Depuis son entrée en service en 2006, le « DPL » suit un programme constant d'évolutions lui permettant de maintenir des capacités de recueil en adéquation avec l'évolution des signaux électromagnétiques.

**Toutefois, il importe dès à présent de préparer la succession de la capacité ROEM stratégique navale, qui devrait intervenir à compter de 2036.**

En matière de défense électromagnétique, **l'objectif est d'équiper les grandes unités de brouilleurs antimissiles ainsi que de brouilleurs anti-drones**. Toutes les frégates de 1er rang devront être équipées, tandis que l'autoprotection des frégates de second rang devra être renforcée.

**Si la Marine conserve une compétence reconnue dans la protection anti-missile et antinavire, cette capacité s'est développée dans un contexte marqué par un sous-investissement dans la guerre électronique.**

**Si les bâtiments sont ainsi dotés d'équipements performants, ils apparaissent en nombre insuffisant, conséquence de choix capacitaires contraints.** Cette situation aboutit à un constat préoccupant : l'ensemble des navires n'est pas aujourd'hui équipé de manière homogène et complète en moyens de guerre électronique, ce qui fragilise la cohérence globale des dispositifs de protection.

**S'agissant de la surveillance du spectre électromagnétique, seules certaines frégates de premier rang disposent de moyens numériques modernes.**

Les frégates multi-missions (FREMM), les frégates de défense aérienne (FDA) et les frégates de défense et d'intervention (FDI) bénéficient de capacités adaptées, tandis que les frégates légères furtives (FLF) restent équipées de systèmes

vieillissants et que **les frégates de surveillance (FS) ne sont dotées que de capacités intermédiaires,** encore en cours de montée en puissance.

**Cette hétérogénéité se retrouve également dans l'aéronautique navale, qui demeure globalement sous-équipée en matière de guerre électronique,** à l'exception du Rafale. À titre d'illustration, les capteurs de guerre électronique de l'Atlantique 2 reposent encore sur des technologies conçues dans les années 1980, malgré les évolutions majeures du spectre électromagnétique et des menaces associées.

**Les moyens de défense électromagnétique navale présentent également des lacunes inquiétantes.**

**Vos rapporteurs relèvent ainsi qu'une des FREMM n'est toujours pas équipée d'un brouilleur d'autodéfense anti-missiles. Plus préoccupant encore, cette capacité n'a pas été intégrée dès l'origine sur les FDI, en raison de contraintes budgétaires et de choix de priorisation lors du lancement du programme.** En pratique, seules les frégates de défense aérienne et sept des huit frégates multi-missions actuellement en service disposent de brouilleurs antimissiles.

**Concernant les frégates de défense et d'intervention, des clauses conservatoires ont été prévues afin de permettre l'intégration ultérieure de brouilleurs actifs.** Toutefois, ce rattrapage *a posteriori* comporte un double risque : celui d'une mise en œuvre tardive, intervenant après l'apparition de vulnérabilités critiques, et celui d'un coût nettement supérieur à une intégration réalisée dès la conception. **Vos rapporteurs jugent cette situation regrettable, au regard des enjeux opérationnels et de la prévisibilité des menaces.**

**La Marine nationale a par ailleurs engagé l'acquisition de brouilleurs anti-drones,** dont l'efficacité opérationnelle a déjà été démontrée en opération. Néanmoins, **le nombre de bâtiments actuellement équipés demeure insuffisant,** limitant l'effet de masse et la capacité de protection généralisée face à une menace drone en forte expansion.

**Dans le domaine de l'aéronautique navale, seule la flotte de Rafales dispose aujourd'hui d'une suite d'autoprotection complète.**

Les avions de patrouille maritime Atlantique 2 et la composante hélicoptère restent en retrait, malgré des perspectives d'amélioration attendues avec l'arrivée de nouvelles plateformes. **Vos rapporteurs déplorent en particulier que la rénovation de la flotte d'Atlantique 2, notifiée en 2013, n'ait pas inclus la guerre électronique dans son périmètre,** alors même que l'évolution des menaces rend cette capacité indispensable.

En définitive, **la Marine nationale conserve des capacités opérationnelles limitées mais satisfaisantes en matière de guerre électronique tactique défensive**,

d’autoprotection navale et aéroportée, de lutte anti-drones ainsi que de dispositifs de neutralisation d’engins explosifs.

**En revanche, les capacités de surveillance électromagnétique, qu’elles soient stratégiques ou tactiques, doivent être considérablement renforcées afin de répondre aux exigences du contexte opérationnel d’aujourd’hui**. Il s’agit en conclusion de garantir la crédibilité, la résilience et la liberté d’action de la Marine nationale dans un environnement de plus en plus contesté.

iii. L’Armée de l’Air et de l’Espace

**Dans le domaine de la surveillance EM, l’AAE souhaite assurer une continuité de la surveillance dans les domaines radios et radar *via* la complémentarité de moyens d'écoute sol et aéroporté** (satellites, ballons THA, avions de mission ELINT (ARCHANGE) et COMINT (ALSR)). La transmission du renseignement en « *temps réel* », facteur de supériorité opérationnelle, passe aussi par un taux de revisite important des capteurs spatiaux.

**À l'horizon 2028, dans le cadre du programme Archange, trois Falcon 8X équipés de la capacité universelle de guerre électronique (CUGE) fourniront une capacité ROEM du « *haut du spectre* »**. Cette capacité est fondamentale pour renseigner les forces, cartographier les menaces EM et programmer les CME des aéronefs de combat avant leurs missions.

**Dans le cadre du ROEM spatial, les capacités françaises sont actuellement englobées sous le programme CERES. La constellation ROEM CELESTE devrait succéder à CERES à horizon 2030. L’actualisation de la LPM doit à cet égard permettre de financer des performances toujours accrues de notre système de ROEM spatial, ce système participant à l’autonomie stratégique de notre Nation.**

La transition entre CERES et CELESTE sur le ROEM spatial

Le programme CELESTE (Composante Électromagnétique SpaTialE) vise à prendre la suite de la capacité CERES de renseignement spatial électromagnétique, qui permet de détecter, localiser et caractériser les menaces électromagnétiques de type radars et télécommunications, à la fois pour établir l'ordre de bataille électronique de l'ennemi mais également pour alimenter les bibliothèques de guerre électronique de nos moyens.

Le capteur spatial aujourd'hui en opération (CERES) constitue la première capacité opérationnelle disponible pour les forces françaises. Elle donne entière satisfaction aux forces et à la DRM en termes de sensibilité et de performance.

Malgré les importants efforts financiers consentis par les industriels, **l'organisation industrielle initialement demandée par la DGA en 2021 (consortium Thales - Airbus) a été remise en cause par la DGA mi-2024 au vu de l'inadéquation entre les ressources financières allouées et les besoins demandés** pour s'assurer du niveau de performances requis par les forces. Quinze mois après, en juillet 2025, la DGA a lancé une compétition sur le système CELESTE, tout en maintenant le niveau de performances. L'appel d'offres a été envoyé à Airbus, Unseenlabs et Thales.

Les industriels devaient remettre leurs premières offres le 15 décembre pour la conception, la réalisation, le lancement et la mise à poste, la recette[18] en vol et le maintien en condition opérationnelle. Des échanges État-industrie auront lieu en 2026 pour un lancement du programme estimé aujourd'hui à fin 2026. **Afin de favoriser la bonne transition entre les systèmes, vos rapporteurs appellent à ce qu'une attention particulière soit accordée au strict respect de ce calendrier.**

Les besoins des forces sont liés à des menaces de plus en plus nombreuses et complexes (extension des bandes de fréquence, densification et complexification des formes d'ondes). **Dans l'objectif de garantir aux forces la mise en œuvre à temps d'une nouvelle capacité ROEM spatial haute performance, il apparaît essentiel d'engager la réalisation du programme au plus vite.**

**Dans le domaine défensif, un effort substantiel doit être mené pour l'autoprotection EM des flottes d'avions de transport et d'hélicoptères.** L'AAE dispose d'aéronefs équipés de systèmes d'autoprotection (SAP) aux performances hétérogènes ce qui induit des différences d'employabilité importantes en fonction du théâtre. Ainsi, face à certains types de menaces, les équipements offrent des niveaux de protection disparates.

**L'autoprotection du RAFALE, à la pointe de la technologie, nécessite de s'adapter en permanence à l'évolution de la menace sol-air et air-air.** Le système d'autoprotection SPECTRA du futur standard F5 doit impérativement bénéficier d'une modernisation afin de lui permettre d'affronter la menace en évolution permanente.

[18] *Opérations au cours desquelles les performances d'un satellite sont vérifiées, peu après sa mise en orbite*

**L'évolution de SPECTRA dans le cadre du standard F5**

**Pour le Standard F5, face à l'évolution constante des menaces et la densification substantielle d'utilisation du spectre électromagnétique, le système SPECTRA bénéficiera de la rénovation complète de la fonction détection électromagnétique et du cœur de traitement**. Cette rénovation augmentera la survivabilité du Rafale pour les missions de dissuasion et d'entrée en premier sur les théâtres contestés.

**La refonte de la chaîne de détection se caractérise par une extension des capacités de détection et la numérisation du signal de bout en bout,** profitant des travaux de maturation technologique déjà déployés dans le domaine naval (SNA Barracuda, FDI) et en cours de développement pour l'aéronautique (Archange). Cette refonte garantira la capacité de détection en environnement électromagnétique dense.

La rénovation du cœur de traitement verra la mise en place d'une architecture modulaire offrant une plus grande agilité dans l'implémentation de nouvelles fonctionnalités opérationnelles.

**Grâce aux améliorations capacitaires apportées à SPECTRA pour le standard F5, le système de GE du Rafale va lui permettre de s'inscrire dans des missions de neutralisation des défenses aériennes ennemies (SEAD/DEAD).** Dans cette perspective, des solutions complémentaires de guerre électronique offensive (nacelle de brouillage, charges GE éjectées ou embarquées) sont actuellement à l'étude afin de compléter les capacités dont le Rafale disposera à cet horizon.

**En outre, si l'avion de transport tactique A400M ATLAS est capable de pénétrer dans des zones contestées grâce à un SAP déjà robuste et à un système de navigation en très basse altitude, sa survivabilité face aux systèmes sol-air et air-air les plus avancés impose des tactiques d'emploi adaptées.**

À cet égard, **le développement d'un détecteur d'alerte missile (DAM) de nouvelle génération est indispensable** dans l'objectif de contrer efficacement la menace missile infrarouge, UV et électro-optique.

**Les avions gros porteurs et les avions de mission devront également être équipés de leurres EM actifs comme les accès GNSS ainsi que les liaisons satellitaires sécurisées.**

**La résilience des munitions au brouillage sera indispensable.** À cet égard, le **missile de croisière SCALP a démontré d'excellentes qualités** de pénétration et de résistance au brouillage lors de conflits récents. Il est équipé d'un système de navigation durci pour résister au brouillage GPS. Le futur missile de croisière STRATUS RS (ex- RJ10) assurera sa survivabilité par sa vitesse supersonique et sa haute manœuvrabilité, le rendant difficilement prédictible et donc interceptable.

**Dans le domaine de la guerre de la navigation (NAVWAR), qui repose largement sur nos capacités spatiales, il s'agira de continuer à développer des outils de PNT** (informations de positionnement, navigation et de temps) résistants aux actions GE ennemies (satellites, aéronefs mais aussi armements guidés), tout en préservant des capacités de « substitution » (centrales à inertie) et nous entraîner à les utiliser en mode dégradé.

**Les besoins capacitaires des Forces aériennes stratégiques (FAS) en matière de GE**

**Les principaux enjeux liés à la GE pour les Forces aériennes stratégiques (FAS) sont d'ordre capacitaire et organique.**

À court terme, les FAS doivent être dotées de capacités leur permettant d'obtenir des effets dans les 3 domaines de la GE suivants :

**Surveillance** : capacité de détection permettant de mettre à jour, en temps réel, l'ordre de bataille électronique adverse afin d'adapter leur propre dispositif et d'optimiser la manœuvre de pénétration ;

**Défense** : capacité d'autoprotection des appareils en vol (MRTT, Rafale *via* le système SPECTRA notamment) au moyen de systèmes embarqués combinant brouillage et leurrage dans toutes les gammes de fréquence. Capacité de protection des moyens des FAS au sol, au sein de leurs zones de stationnement, contre des attaques de drones, grâce des systèmes de brouillage de forte puissance ;

**Attaque** : capacité à mettre en œuvre des munitions rôdeuses ou saturantes à bas coûts, destinées à détruire les systèmes sol/air adverses. Capacité aéroportée de brouillage offensif, permettant d'aveugler les radars de recherche et de conduite de tir de l'adversaire le temps de la pénétration du raid.

**À moyen et long terme, les évolutions constantes de l'aéronef porteur de l'arme nucléaire sont également primordiales pour faciliter la pénétration**. Les évolutions du système d'arme RAFALE, de son rayon d'action et de sa connectivité préparent l'arrivée du standard F5 et du combat collaboratif. Le MRTT connaîtra également des évolutions capacitaires pour améliorer sa survivabilité.

**Les FAS doivent demeurer motrices dans ce domaine de la GE.**

**La résilience de l'aviation de l'AAE face à la guerre électronique est une construction globale qui va bien au-delà des capacités individuelles de chaque appareil.** Elle s'appuie sur une combinaison de plateformes modernes et protégées, de munitions intelligentes et résistantes, et de capacités de renseignement et de programmation de haut niveau, le tout soutenu par un entraînement réaliste et une doctrine complète et cohérente visant à maîtriser le spectre EM.

Pour ne pas seulement subir la GE adverse, **l'AAE doit se doter à nouveau d'une capacité SEAD offensive**. L'objectif est de neutraliser les systèmes de défense, notamment les radars, pour permettre aux aéronefs de pénétrer un espace aérien contesté.

**La capacité à entrer en premier dans le cadre d'une opération conventionnelle impose de se doter de moyens de brouillage offensifs aéroportés (saturation et perturbation de la capacité de détection ennemie) et de missiles anti radars (destruction des radars de systèmes sol-air longue portée).**

L'acquisition d'une capacité de brouillage EM « *sol* » permettra en particulier la défense des bases aériennes de l'AAE et de points sensibles notamment contre tous les types de menace : mini-drones (LADA), drones MALE/HALE, munitions télé-opérées ou guidées par GPS, aéronefs habités.

**Devront également être développées les capacités de brouillage et leurrage depuis la THA et l'espace.** Ces milieux constituent en quelque sorte la nouvelle frontière du champ électromagnétique, certains de nos compétiteurs stratégiques investissant toujours plus sur ces segments.

La capacité de brouillage offensif aéroportée devra être à la fois « *grande distance* » (« *stand off* »), intermédiaire (« *stand in* ») et forte puissance.

iv. La protection des bases militaires

**L'opération ukrainienne Spiderweb a marqué une rupture stratégique en démontrant la capacité à frapper, par drones, des bases aériennes situées à plusieurs milliers de kilomètres de la ligne de front.**

En attaquant simultanément cinq emprises russes de haute valeur, l'Ukraine a montré qu'il est désormais possible de contourner des dispositifs de défense classiques et d'atteindre des actifs stratégiques au cœur du territoire adverse.

L'opération Spiderweb

Pour rappel, **l'opération Spiderweb (Pavutyna), menée le 1er juin 2025 par le Service de sécurité d'Ukraine (SBU), constitue l'une des opérations de frappe en profondeur les plus marquantes du conflit russo-ukrainien**. Préparée pendant environ 18 mois, elle visait spécifiquement l'aviation à long rayon d'action stratégique russe stationnée loin de la ligne de front.

**L'opération a reposé sur l'emploi coordonné de 117 drones FPV, dissimulés dans des conteneurs embarqués sur des camions civils prépositionnés à proximité des bases ciblées.** Les frappes ont été lancées quasi simultanément contre cinq bases aériennes majeures : Belaya (oblast d'Irkoutsk), Dyagilevo (Riazán), Ivanovo Severny, Olenya (Mourmansk) et Ukrainka (Amour).

**Ces sites abritaient des aéronefs de l'aviation stratégique russe**, notamment des bombardiers stratégiques Tu-95MS, Tu-22M3 et Tu-160, ainsi que possiblement des avions de détection radar A-50.

**La profondeur géographique des frappes** - certaines bases se situant à plusieurs milliers de kilomètres de l'Ukraine - **a marqué un tournant opérationnel.**

Concernant les pertes, **les autorités ukrainiennes ont affirmé que plus de 40 aéronefs russes avaient été touchés. Les évaluations occidentales sont plus prudentes** et estiment qu'environ 20 appareils auraient été atteints, dont une dizaine détruite, avec au moins 13 pertes confirmées par imagerie satellitaire.

**Les dommages matériels sont estimés à plusieurs milliards de dollars**, certains bilans évoquant jusqu'à 7 milliards USD. Au-delà du choc symbolique, l'opération aurait temporairement réduit la capacité russe de frappe stratégique à longue portée et mis en évidence **la vulnérabilité d'actifs aériens de haute valeur face à des attaques de drones planifiées en profondeur.**

Dans le même temps, **la Russie a massivement employé des drones de type Shahed/Geran pour saturer les défenses ukrainiennes**, ouvrir la voie à des missiles balistiques et frapper des infrastructures critiques en profondeur. Le drone est devenu un outil stratégique, capable d'éroder durablement les capacités adverses à coût maîtrisé.

Cette dynamique déborde désormais le théâtre ukrainien. **Des incursions ont été constatées en Pologne et dans les États baltes,** illustrant le risque d'extension du conflit.

**La France elle-même a été confrontée, depuis l'automne 2025, à plusieurs survols non autorisés de sites sensibles** comme la base de l'Île Longue, pilier de la dissuasion océanique, mais aussi Mourmelon, Creil ou encore l'entreprise Eurenco à Bergerac.

Même sans attribution étatique formelle, ces incidents révèlent la vulnérabilité structurelle de certaines infrastructures stratégiques face à des vecteurs légers, discrets et difficiles à intercepter.

**La multiplication de ces incidents interroge : notre modèle d'armée échantillonnaire compensé par la dissuasion pourrait-il absorber un choc stratégique comparable à celui infligé par l'opération Spiderweb ?**

**Les armées les plus exposées sont celles qui concentrent leurs capacités critiques. L'Armée de l'Air et de l'Espace apparaît particulièrement vulnérable,** du fait de la concentration de moyens stratégiques comptés sur des bases couvrant de larges surfaces (plateformes aéronautiques) difficiles à protéger en intégralité.

**Si les autorités militaires ont assuré que les bases directement liées à la dissuasion bénéficient de dispositifs renforcés, la protection globale des infrastructures et équipements les appuyant par des fonctions de soutiens demeure un enjeu majeur.**

**Dans ce contexte, la lutte anti-drones sur le territoire national devient un enjeu central de sécurité et de résilience stratégique sachant que la guerre électronique y joue un rôle déterminant.**

Les premiers fusils brouilleurs portatifs équipent désormais certaines bases afin de perturber les liaisons de commande et les signaux de navigation des drones. Toutefois, la protection ne peut reposer sur un seul outil. **Elle doit s'inscrire dans une défense multicouche, combinant détection radar basse altitude, surveillance du spectre électromagnétique, brouillage radiofréquence, neutralisation GNSS, leurrage et, en dernier ressort, moyens cinétiques.**

La guerre électronique intervient ainsi dans une large partie de ses étapes : détection des signaux faibles, identification des vecteurs, rupture des liaisons de télécommande et neutralisation ciblée. Mais au-delà de la réponse immédiate, **l'enjeu est celui de la résilience :** redondance des systèmes critiques, dispersion des moyens, capacité de reconstitution rapide.

**L'expérience ukrainienne démontre que la profondeur géographique ne protège plus. Seule une combinaison de surveillance permanente du spectre et de capacités électromagnétiques robustes permettra de sécuriser durablement les emprises stratégiques françaises**.

## B. LES DÉFIS POUR LA BITD

### 1. Favoriser une logique de flux plutôt qu'une logique de stock

#### a. *Adapter les PEM au tempo de la GE*

**La guerre en Ukraine nous enseigne qu'il importe de ne pas se focaliser à l'excès sur le type d'équipements utilisés par les belligérants, compte tenu de leur rapide caducité.** *A contrario*, il s'agit en priorité de savoir produire rapidement et en flux continu des capacités innovantes pour garder une longueur d'avance sur l'adversaire.

Aussi, la priorité en matière de GE est aujourd'hui de bâtir, ou de mettre en place les conditions de bâtir, l'écosystème industriel qui saura produire en masse et « *au moment où* » nous pourrions être engagés dans un conflit de haute intensité.

**La guerre électronique nécessite une adaptation quasi permanente des réponses en fonction de la menace, réaction qui est souvent en décalage avec les grands programmes d'armement type « *programme à effet majeur* (PEM) »** (cycle long en « V »). Les PEM conçus de manière conventionnelle s'avèrent ainsi peu pertinents dans ce champ hyper-technologique où les besoins des trois armées ne sont pas uniformes.

Auditionné par vos rapporteurs, l'industriel THALES a déclaré que l'un des principaux écueils à **éviter dans le cadre des PEM était de « *freiner l'évolutivité des équipements et des systèmes de Guerre électronique à l'intérieur de programmes structurants et potentiellement contraignants.***

*Sur ce point, la numérisation des équipements et des systèmes de guerre électronique, tant pour la chaîne de détection que pour la chaîne de brouillage, sur la base d'une définition matérielle stable (hardware) et donc sans conséquence majeure sur l'intégration physique à la plateforme, permettra l'évolutivité des aspects logiciels et des capacités de calculs (forme d'onde, forme de brouillages) pour rester efficace face à l'évolution de la menace*. »

**Les forces armées expriment donc un besoin de réactivité « *court terme* » de l'écosystème industriel (réalisation, adaptation, achat d'équipements). Il importe donc d'adapter les PEM au rythme de la GE, en faisant prévaloir une logique de flux plutôt qu'une logique de stock.** Ainsi, l'acquisition en une fois d'une masse de capacités fait courir le risque de disposer de moyens rapidement obsolètes. *A contrario*, l'achat de volume limité de systèmes selon un cycle de rafraîchissement technologique régulier et constant semble plus indiqué.

**Auditionnée par vos rapporteurs, la Direction générale de l'armement (DGA) a indiqué militer pour la mise en place de PEM incluant une partie à flux pour des domaines à cycles industriels et technologiques très courts,** afin de répondre au besoin de réactivité. Ce type de programmes serait en cours de déclinaison pour la guerre électronique.

**Plus généralement, la Direction s'attache à optimiser, dans toutes les opérations d'armement, les phases de qualification et de réception des matériels en mutualisant et en réduisant au strict nécessaire les tests à réaliser dans le but d'accélérer les livraisons des matériels.**

**Afin d'adapter le *tempo* des programmes de GE, la DGA et l'EMA ont mis en place des task-force « *Attaque EM* » (ou GCEM) et « *Lutte anti-drone* » (LAD).** Ces forums permettent de réunir régulièrement l'ensemble de l'écosystème capacitaire et de faire un point sur les retours d'expérience (Retex) opérationnels, les résultats des expérimentations/essais, l'avancement des programmes d'étude et d'armement.

**À terme, il serait nécessaire de pouvoir disposer d'une organisation Forces/DGA/Organisme de recherche/Industrie facilement activable et réactive mais néanmoins pilotée.**

Le COMCYBER a indiqué à vos rapporteurs l'existence depuis quelques années d'ateliers CYBER-GE adossés à la communauté cyber des armées (CCA), ces ateliers regroupant 22 unités opérationnelles offrant **l'opportunité de créer un véritable écosystème de maturation technico-opérationnelle de la GCEM et des synergies GE-Cyber.** L'objectif de ces ateliers est de gagner la bataille de l'innovation, afin d'accélérer la boucle Retex - innovation – développement.

Auditionné par vos rapporteurs, Philippe Gros, maître de recherche à la Fondation pour la recherche stratégique, a notamment promu la mise en place d'un processus combinant sur « *six mois à un an, innovation ouverte et urgence opérationnelle* » et incluant :

- Un suivi permanent des innovations tactiques et techniques,

- Une identification et sélection des options de solutions disponibles sur étagère permettant de contrer ces menaces ou d'exploiter ces opportunités,

- Une capacité à expérimenter rapidement, perfectionner les options retenues puis décider de leur acquisition,

- Acquérir en quantité limitée mais significative ces systèmes,

- Asservir le plan de dotation aux processus de préparation opérationnelle des forces en leur attribuant de nouveaux équipements et en les formant à ceux-ci en phase de préparation avant engagement ou prise d'alerte.

**Cette nouvelle organisation en flux supposerait d'étendre les prérogatives et les crédits des forces en matière d'innovation (STAT, CEPN, CEAM), de mettre en œuvre des mécanismes de financement extrêmement réactifs ainsi que des mécanismes de certification allégés.** Elle supposerait également que les industriels soient en mesure d'accélérer leur cadence de production sur le très court terme, tout en reconnaissant la nécessité de retirer du service rapidement des équipements frappés d'obsolescence.

b. ***Favoriser des architectures ouvertes***

**Autant que de possible, les équipements de GE des armées françaises devront bénéficier d'architectures modulaires « ouvertes » et collaboratives capables d'adaptations précoces sur le terrain** (logique d'une « BITD de l'avant ») dans le cadre de cycles d'innovation accélérés.

Les architectures ouvertes sont au cœur du nouveau paradigme de la GE numérisée entre équipements « *hardware* » immuable et « *software »* devant être mis à jour régulièrement.

**MC2 Technologies a indiqué à vos rapporteurs concevoir l'ensemble de ses produits en architecture ouverte ;** l'entreprise définit le format dans lequel les armées peuvent directement enregistrer les signaux afin que ces derniers soient correctement « interprétés » par les produits.

**La conception de solutions en architecture ouverte réduit les délais de maintenance en condition opérationnelle (MCO) et augmente la disponibilité des équipements.** Cette stratégie permet aux forces armées de s'approprier directement les capacités acquises sans avoir à repasser nécessairement par l'industriel pour toute évolution du produit.

c. ***Préparation des innovations de demain***

**Plusieurs technologies sont susceptibles d'affecter très rapidement et substantiellement le champ de la guerre électronique**. La BITD devra être en mesure de répondre à ces enjeux et de proposer des solutions adaptées aux forces :

•**les armes à énergie dirigée (AED)** devraient se développer et permettre *a minima* la neutralisation rapide et à moindre coût des drones ennemis ainsi que la recharge à distance des batteries des drones amis. La portée des AED électromagnétiques serait limitée dans un futur proche (efficacité <10-12 km). Ces armes présentent néanmoins de fortes contraintes d'emploi et des limites difficilement surmontables (sensibilité aux conditions météorologiques et aérologiques notamment).

•**l'émergence des radars « transhorizon » à onde de ciel comme le radar « haute fréquence** » Nostradamus développé par l'ONERA. Ce dernier voit au-delà de l'horizon, jusqu'à plusieurs milliers de kilomètres, en cassant la furtivité de plateformes non détectées par les radars conventionnels ;

•**dans le domaine de la navigation PNT** (« *NAVWAR* »), les centrales inertielles qui ne dérivent plus et n'ont plus besoin d'être recalées par GPS pendant un certain temps sont utiles dans un environnement EM brouillé) ;

•**la révolution des radars « passifs »** qui n'émettent plus mais récupèrent des signaux d'opportunité pour localiser les cibles et sont donc beaucoup moins détectables par l'ennemi.

•**la miniaturisation des charges de GE embarquées** sur des petits vecteurs est un enjeu d'avenir majeur. La miniaturisation des drones et capteurs permettra la compacité qui favorisera la frugalité énergétique.

La miniaturisation des charges de GE

Interrogé sur ce sujet par vos rapporteurs, Thales a indiqué que « ***cette miniaturisation s'adresse à toutes les composantes de la guerre électronique,*** *du renseignement d'origine électromagnétique à l'attaque électronique en passant par l'autoprotection des plateformes aéroportées, navales et terrestres, dronisées ou non.* »

Elle se décompose selon deux familles de charge utile GE:

• **Une miniaturisation moyenne** (*i.e.* une charge utile de quelques litres) au profit des missions de renseignement à bord de drones employés sur le champ de bataille permettant d'assurer la détection, la localisation, l'identification et l'écoute des radars et moyens de communication. Par ailleurs, sont également en cours de développement d'autres types de charges utiles pour les fonctions d'autoprotection de drones ou « *Remote Carrier* » de moyenne endurance, y compris de type armement.

• **Une miniaturisation très compacte** (*i.e.* charge utile inférieure à un litre) qui offre des fonctions d'autoprotection et d'attaque électronique basique pour des missions de GE offensive visant à perturber les radars et communications adverses. Ces charges GE compactes seraient dispersées en grand nombre, à partir de différents types de plateformes cargo (missiles air/surface adaptés), de drones, d'hélicoptères ou encore depuis la tranche arrière d'avion de transport.

Lors de son audition par vos rapporteurs, l'attaché d'armement français en Ukraine a précisé que la miniaturisation des charges de GE existait sur le champ de bataille ukrainien, dans une optique d'autoprotection.

•**la compacité et conformité des systèmes antennaires** : la réduction de la séparation fréquentielle entre gamme radar et gamme communications, mais aussi l'augmentation des bandes utilisées dans les communications, engendrent des contraintes de coexistence toujours plus fortes et une complexité d'intégration accrue.

•**l'ajustement de la GE des communications aux communications hybrides** notamment satellitaires.

### 2. Le retour d'expérience des conflits est essentiel

#### a. *L'indispensable connaissance des technologies adverses (ROEM)*

**La bonne connaissance des capacités GE de nos adversaires est fondamentale. Il est donc essentiel de mener les actions nécessaires pour parfaire la connaissance de la menace, ceci dans le but d'orienter les travaux de maturation des briques technologiques.**

Cette connaissance peut notamment supposer **une manœuvre des forces ou des industriels afin de se procurer des matériels de GE récupérés sur les théâtres d'opération** permettant une meilleure compréhension des systèmes de GE d'éventuels compétiteurs.

#### b. *Un partage nécessaire mais difficile avec les alliés*

**La coordination avec les alliés est un facteur de succès pour la GE** tout comme dans les autres domaines. Pour autant, chaque État dispose de sa propre organisation, adaptée à ses ressources, ses moyens mais aussi à sa culture.

Surtout**, la GE est une matière très sensible se prêtant peu aux coopérations internationales.** Les matériels et systèmes nationaux, notamment les bibliothèques de GE, ne peuvent ainsi être partagés avec des interlocuteurs étrangers, même alliés.

Comme l'a indiqué à vos rapporteurs le Directeur du renseignement militaire : « *Dans ce domaine, la France n'a pas d'alliés mais des partenaires*. »

**La coordination n'est donc pas automatique et des marges de progression existent, dans la limite des habilitations opposables.**

### c. *Un partage à renforcer entre la BITD et les armées*

S'il semble délicat de partager de manière extensive le renseignement d'origine électromagnétique (ROEM) entre alliés, **il serait toutefois opportun de renforcer la coopération entre la BITD française et les forces armées nationales en matière de GE.**

**L'ensemble des industriels auditionnés par vos rapporteurs, indépendamment de leur taille, ont plaidé en faveur d'une facilitation accrue par le ministère des Armées de l'accès aux données de GE** (nouvelles menaces, signaux réels, *etc*.).

À l'aune du Retex ukrainien, l'écosystème industriel français de GE souhaiterait renforcer ses contacts avec les forces, en leur proposant notamment de tester leurs produits.

La Marine nationale a notamment pu tester les brouilleurs MAJES produits par MC2 Technologies lors de son exercice biannuel *Wildfire* en 2023. Signe de la validité de cette approche, **la Marine a fait le choix d'acquérir plusieurs de ces systèmes, qui se sont révélés extrêmement précieux** pour la protection non-cinétique de ses bâtiments face à la menace houthie en Mer Rouge.

**Les trois services des armées responsables de l'innovation capacitaire (STAT, CEPN et le CEAM) ont tous exprimé le souhait de voir les industriels de la GE davantage associés aux grands exercices des armées afin d'ensuite faciliter, en termes de délais, l'éventuelle contractualisation avec la DGA.**

**Le modèle du cluster « *Brave1* » en Ukraine a notamment été cité par de nombreux acteurs industriels de l'écosystème GE.**

Le cluster Brave1 en Ukraine

**Brave1 est une plateforme du gouvernement ukrainien lancée le 26 avril 2023, visant à rassembler des entreprises innovantes ayant des idées et des développements pouvant être utilisés dans la défense de l'Ukraine.**

D'après le site gouvernemental ukrainien *Digitalstate UA*[19] « *Brave1 est une plateforme de coordination qui réunit tous les acteurs du secteur des technologies de défense, en leur apportant un soutien organisationnel, informationnel et financier afin d'accélérer le développement de projets de défense innovants en Ukraine. Sa mission est de positionner l'Ukraine comme un leader mondial des technologies de défense.* »

***Brave1*** **facilite ainsi l'accès de l'écosystème des armées et de la BITD à la donnée relative aux signaux EM sur le front.**

[19] *https://digitalstate.gov.ua/projects/tech/brave1*

La GE étant un domaine hyper-technologique, l'écosystème industriel de la BITD pourrait renforcer ses formations à la GE à destination des forces armées.

À cet égard, MC2 devrait prochainement créer une formation à Bruz (Ille-et-Vilaine, à proximité du site de la DGA-MI) spécialisée sur la GE, tandis que l'armée de Terre cherche à renforcer les liens existants entre la 785ème compagnie de GE et la BITD.

**Le levier de la réserve opérationnelle pourrait notamment être utilisé pour renforcer les synergies entre industriels de la GE et les forces armées.**

### 3. Le foisonnement de l'écosystème doit être organisé

#### a. *La difficile convergence des objets industriels de GE*

**Les gammes d'équipements de GE sont souvent très morcelées au sein d'une même armée.** La Marine nationale a notamment évoqué « *une mosaïque bigarrée avec des technologies évolutives* (…). » Chaque capteur hétérogène requiert une « traduction » spécifique dans la base de données de chaque porteur, les systèmes de GE étant différents selon les plateformes malgré un cœur de système unifié.

**L'écosystème industriel de GE est lui-même relativement foisonnant, l'acteur industriel historique majeur du segment (Thales) cohabitant avec de très nombreuses PME et TPE.**

C'est dans cette articulation entre les grandes entreprises de la BITD et la myriade d'entreprises intermédiaires ou de petite taille qu'un besoin d'ordonnancement semble le plus patent.

Toutefois, sur certains segments de la GE comme la défense anti-missiles, seul Thales serait en mesure de répondre aux menaces du fait de son expertise inégalée en la matière.

#### b. *Commandes et passage à l'échelle*

**Au sein de cet écosystème foisonnant, il importe de réussir le défi du passage à l'échelle, en faisant en sorte que l'innovation résiste à l'innovateur.**

Dans le domaine organisationnel, plusieurs initiatives matérialisent l'engagement de la DGA à accélérer, amplifier et simplifier des projets, notamment pour prendre en compte les cycles courts d'innovation à l'instar de la GE. Cette stratégie de changement s'appuie notamment sur :

- **La force d'acquisition réactive (FAR) :** créée dans le cadre de transformation de la DGA initiée en 2023, cette équipe privilégie le respect d'un calendrier resserré entre l'expression du besoin et la mise en service ce qui nécessite une certaine flexibilité dans les fonctions ou performances attendues et dans la

gestion des risques. La démarche repose en particulier sur une priorisation commune EMA-DGA pour dégager des ressources (humaine et financière) pour des acquisitions rapides, au détriment d'autres opérations. Une trentaine de projets sont en cours au profit de toutes les armées. Déjà citée, l'acquisition de brouilleurs MAJES sur les frégates déployées en Mer Rouge a notamment été menée dans ce cadre.

- **La facilitation du passage à l'échelle :** la DGA a précisé à vos rapporteurs que sur une base annuelle, des fonds sont réservés pour permettre de transformer une innovation réalisée au sein des armées en une première capacité. Dans l'ensemble des domaines, une quinzaine de projets par an en auraient déjà bénéficié.

- **La révolution des affaires capacitaires (RAC) :** mise en place en 2025, cette démarche vise à amplifier l'élan donné par les projets de transformation de la DGA et post-combustion de l'EMA en exploitant les travaux du mandat « opérations agiles » et le bilan de la force d'acquisition réactive**.** Elle cherche en particulier à faciliter l'injection des différentes formes d'innovation dans les programmes d'armement, mais aussi à tirer parti des savoir-faire internes du ministère.

**Ces trois initiatives exploitent et favorisent les propositions d'industriels proactifs et réactifs, souvent PME et ETI avec des développements courts et / ou des achats sur étagère, et un passage à l'échelle d'innovations développées parfois sur un cycle très court.**

### c. *Renforcer la souveraineté et la résilience des chaînes de valeur*

#### i. Renforcer la souveraineté des chaînes de valeur

La majorité des équipements de GE utilisés par les armées françaises proviennent d'entreprises nationales. **La souveraineté de la chaîne de valeur est indispensable en raison de la manipulation de données permettant de caractériser les capacités GE des armées françaises.**

**La majorité des équipements de GE (brouilleurs, moyens de détection et de leurrage) sont en effet protégés tandis que les bibliothèques de GE programmées par les armées sont classifiées au niveau TRÈS SECRET-SPÉCIAL France, ainsi que l'ensemble du domaine « radar ».**

Ainsi que l'a résumé l'AAE, « *Domaine extrêmement sensible,* ***détenir des matériels « nationaux » est indispensable pour les avions de combat pour éviter toute compromission de notre savoir-faire et assurer notre autonomie.***

*Cette indépendance est aussi à rechercher autant que possible pour les avions de transport tactiques et les hélicoptères afin d'être en capacité d'assurer le meilleur niveau de protection à nos équipages et de succès de la mission* (…). ***Portant la mission de dissuasion, une chaîne 100 % française est indispensable***

***pour ne pas divulguer les capacités opérationnelles de l'AAE, notamment pour la mission de dissuasion ».***

**Les rares matériels étrangers composant les équipements de GE français imposent des restrictions d'emploi spécifiques en cas de panne.** Ainsi, lors d'un envoi de matériel en réparation à l'étranger, il faut s'assurer que les données « spécial France » ont été purgées (au risque d'une compromission). Il s'agit encore de mettre en place en place une filière de réparation nationale des équipements étrangers afin d'éviter tout transfert d'information involontaire.

**Ces restrictions concernent notamment les aéronefs acquis sur étagère à l'étranger,** à l'instar des avions de transport tactiques C-130J dotés d'un SAP entièrement américain. Dans ce cadre, les bibliothèques de GE sont réalisées par les USA.

Par ailleurs, vos rapporteurs regrettent qu'à la suite d'un accord de coopération relatif aux frégates FDA et FREMM entre Thales et l'entreprise italienne ELETTRONICA, Thales ne fabrique plus de brouilleurs navals, ces derniers étant conçus et développés par cette société pour les besoins de la Marine française.

**Vos rapporteurs plaident également pour la conception et le développement en France ou dans l'UE des composants critiques spécifiques intégrés et adaptés dans nos systèmes de GE, souvent d'origine américaine, afin de renforcer notre autonomie stratégique**.

Nous savons en effet exploiter, intégrer et parfois adapter des composants critiques d'origine étrangère, souvent américaine, mais non les concevoir et les développer, ce qui fragilise *de facto* notre autonomie stratégique.

**En outre, il existe une problématique en termes de matières premières critiques**. Ainsi que l'a résumé Thales devant vos rapporteurs : « *Nous souhaitons aussi rappeler que* ***les systèmes de guerre électronique et plus généralement les systèmes utilisés dans la défense font appel à l'utilisation de métaux et terres rares.*** *Un exercice de cartographie sur l'ensemble de nos solutions de défense a permis d'identifier les matières premières critiques dans nos produits au travers de composants achetés en direct ou via nos fournisseurs (rang 1, rang 2, rang 3).*

*Compte tenu des tensions géopolitiques, les risques liés à leur approvisionnement existent. Une des réponses destinées* ***à atténuer ces risques passera par la mise en place de filières de recyclage souveraines (nationale ou UE), au bénéfice de toute la BITD.*** *En tout état de cause, Thales reste particulièrement vigilant sur ces risques et demande un même niveau de vigilance à ses fournisseurs.* ***Les filières au sein de la BITD doivent donc constamment faire l'objet d'un suivi particulier pour assurer la pérennité de la France*** *en matière de systèmes de guerre électronique, et Thales est particulièrement attentif à leur développement durable*. »

ii. Renforcer la résilience des chaînes de valeur

**Principale grande entreprise historique positionnée sur le segment GE, Thales travaille avec une centaine de fournisseurs de rang 1. La résilience durable de la chaîne de valeur est une préoccupation légitime** : « *La combinaison « technicité et souveraineté » associée à des faibles séries au regard d'autres industries comme l'automobile, amène à devoir veiller très étroitement sur la solidité et la résilience de la BITD, en particulier sur des filières essentielles à la guerre électronique comme :*

- *La microélectronique ;*
- *Les circuits imprimés (CI) à très haute complexité (combinant électronique de puissance, hyperfréquence et électronique numérique de très haute densité) ;*
- *La filière des EMS (Electronic Manufacturing Services), fournissant des services de fabrication en sous-traitance de cartes électronique câblées à partir de CI nus ;*
- *La mécanique de précision et l'intégration mécanique-électronique.*

***Dans un contexte de forte croissance de la demande mais aussi d'attaques cyber ou de piratage de nos actifs industriels, ces filières, indispensables à la production de systèmes de guerre électronique, sont parfois fragiles et nécessitent un accompagnement important. »***

## C. LE DÉFI ESSENTIEL DE LA RESSOURCE HUMAINE

### 1. Le besoin en recherche et développement

#### a. *Maths et sciences, une base qui s'effrite*

Si la France peut s'enorgueillir d'une recherche en mathématiques de grande valeur, ses succès masquent **un déclin manifeste de sa base universitaire**. Si la question est complexe dans les facteurs qui la commandent, il est évident que **la baisse du niveau des candidats dans les études supérieures y joue un rôle manifeste.**

Cette évolution se confirme à travers les enquêtes PISA[20] qui mesurent chaque année le niveau scolaire des élèves. **Devant ce constat inquiétant, plusieurs dirigeants des grandes entreprises nationales – notamment celui de**

[20] *Programme international pour le suivi des acquis des élèves*

**Safran[21] - ont alerté sur les possibles effets de cette « *bombe à retardement* » pour l'économie française.**

**Les mathématiques sont au cœur de l'innovation technologique dans des domaines stratégiques** comme le nucléaire, l'aérospatiale ou l'électronique. Selon plusieurs chefs d'entreprises entendus par vos rapporteurs, la perte de cette compétence aura donc des conséquences importantes en termes de recrutement de spécialistes issus des filières scientifiques.

**Le déficit chronique de formation « d'ingénieurs RF », spécialistes des technologies de radiofréquence, est accentué par la concurrence de secteurs davantage porteurs comme le numérique mais aussi par des offres d'emploi plus attractives à l'étranger.**

**Cette concurrence joue un rôle non négligeable dans le maintien à niveau des spécialistes de guerre électronique et plus généralement dans la gestion des ressources humaines des personnels qui y sont rattachés.**

b. *L'excellence en R&D encore insuffisante à couvrir tous les besoins*

**Un niveau soutenu de R&D est nécessaire afin de permettre la souveraineté et la pérennité de la chaîne de valeur nationale de GE.**

D'après les auditions conduites par vos rapporteurs, la BITD française peut se prévaloir d'un bon niveau de R&D grâce notamment à Thales ainsi qu'à tout l'écosystème de PME/ETI spécialisées.

Il est notamment possible de citer MC2 Technologies et CERBAIR dans le domaine de la lutte anti-drones et du brouillage des communications, ATDI dans le domaine de la propagation des ondes ou encore SERPICOM dans les mesures de soutien électronique (ESM). À titre d'exemple, MC2 Technologies a précisé à vos rapporteurs réinvestir près de 20 % de ses résultats dans la R&D.

**En outre, les armées et les industriels français ont la chance de pouvoir disposer du centre d'essais SOLANGE de la DGA-MI permettant notamment d'orienter et de sécuriser techniquement les choix des industriels pendant la phase de développement des équipements.**

---

[21] *https://www.lefigaro.fr/conjoncture/une-bombe-a-retardement-le-directeur-general-de-safran-alerte-sur-la-chute-du-niveau-en-mathematiques-en-france-20260115*

SOLANGE, pépite de la DGA-MI

SOLANGE est un moyen d'essais essentiel de DGA-MI permettant de mesurer des signatures électromagnétiques radar (SER) d'aéronefs ou missiles à l'échelle 1. Il appartient à un complexe de trois bases de mesures pour **évaluer et qualifier la furtivité radar des systèmes d'armes nationaux dans le but à la fois d'assurer la maîtrise de leur détectabilité par les radars ennemis et d'alimenter les études de performances de leurs systèmes GE d'autoprotection actuels et futurs** (RAFALE, MIRAGE 2000, A400M, SCAF, FREMM, HORIZON, FDI, TIGRE, NH 90 *etc*).

Ces bases de mesures sont également utilisées pour évaluer les performances des systèmes antennaires des moyens de GE (détecteur et brouilleur) y compris dans le domaine NAVWAR (Guerre de la Navigation).

**Enfin, ces moyens permettent de mesurer les signatures radar de matériels étrangers récupérés sur les théâtres (drones, roquettes, missiles) afin de fournir aux forces l'information sur les capacités des radars nationaux à les détecter ou les reconnaitre.**

Selon les cas examinés, cette analyse alimente à la fois :

- une réaction temps court par la reprogrammation de nos systèmes GE nationaux qui permet de traiter la menace ;

- sinon, et une réaction temps long lorsque cette analyse identifie la nécessité d'identification des évolutions nécessaires importantes du matériel national pour le traitement de traiter la menace considérée.

**Les chambres anéchoïques et cages de Faraday de la DGA-MI abritent des simulateurs permettant de tester les systèmes de GE et des équipements radiofréquences en ambiance de GE.** Ils permettent de tester des équipements réels (matériel et logiciel) dans un environnement confiné pour la protection du secret (intérêt des cages de Faraday/chambres anéchoïques), sur un grand nombre de scénarios (de l'ordre de plusieurs milliers par campagne de test) face à des menaces simulées existantes ou à venir, en ambiance de GE de haute intensité, le tout pour un coût raisonnable et maitrisé.

Ces capacités techniques génèrent des plus-values tout le long du cycle de vie des armements testés :

• En phase amont des programmes, le test de démonstrateurs alimente le dossier de choix des nouvelles capacités à acquérir pour la phase de développement.

• au cours du développement d'un programme, des tests permettent de lever des risques techniques à corriger d'ici la phase de qualification.

• en fin de développement, ces moyens permettent à la fois de vérifier la conformité des équipements à leurs spécifications (qualification DGA) et de caractériser au profit des forces leur domaine complet de performances.

| |
|---|
| • en phase d'utilisation par les forces, ces moyens peuvent être également utilisés pour évaluer une évolution d'un concept d'emploi du matériel, sa performance vis-à-vis d'une nouvelle menace.<br><br>• ces capacités participent aussi aux actions DGA de soutien à l'Export. |

Malgré la qualité technique et l'intensité de la recherche et développement conduite, **l'écosystème de BITD français ne couvre pas l'ensemble des besoins exprimés** ce qui oblige ponctuellement les forces à s'équiper auprès de fournisseurs étrangers.

**Par ailleurs, certaines PME ont souligné devant vos rapporteurs les difficultés récurrentes qu'elles éprouvent au moment du dépôt des demandes de crédit impôt recherche.**

Ces difficultés résultent notamment de **la nécessité de justifier des activités de R&D dans le domaine de la défense,** alors que les activités en question, dès lors qu'elles ressortent de la GE, sont extrêmement sensibles. Le support expert vérifiant les dossiers n'est en effet pas spécifiquement habilité pour ce faire.

**Un organisme vérificateur « *marqué* » défense serait vraisemblablement plus pertinent (DGA, AID, par exemple).**

### c. *Les partenariats laboratoires/BITD*

Vos rapporteurs plaident en faveur d'**un rapprochement plus fréquent des laboratoires de recherche et de l'écosystème de la BITD spécialisée en GE**, dans le but de favoriser des synergies en R&D et créer un réel vivier de talents français susceptible de concevoir les innovations de demain.

Les secteurs de l'intelligence artificielle, des communications satellitaires, ou encore de la production de matériaux magnétiques peuvent retirer de nombreux avantages d'une recherche publique et cela d'autant plus qu'ils peuvent alimenter l'innovation de défense.

**Il apparait stratégique d'encourager le développement de ces nouvelles technologies sur notre territoire, notamment par des dispositifs de financement et d'accompagnement, dès lors qu'il s'agit d'un enjeu de souveraineté nationale**.

Christophe Gaquière, fondateur et directeur général de MC2 Technologies, entreprise du Nord visitée par vos rapporteurs, a évoqué **la puissance du substrat scientifique et technologique français qui devrait de fait permettre un meilleur échange entre les mondes académiques et industriels.**

Ces transferts fonctionnent d'ailleurs dans les deux sens pour l'industrie de défense, capable de détecter en amont le potentiel d'une technologie, d'aider ensuite à son développement puis de favoriser *in fine* l'application concrète de ces innovations.

**Pour toutes ces raisons, ces partenariats recherche-industrie (« *clusters* ») doivent être favorisés.**

### 2. Le défi du recrutement et de l'attractivité

#### a. *Le défi du recrutement*

**Le sujet de la ressource humaine et de la formation dans le champ de la GE est incontournable pour les armées**. Les enjeux sont multiples : recruter et former le vivier nécessaire pour renforcer les unités et enfin développer les compétences nécessaires à l'accompagnement des avancées technologiques.

Aujourd'hui, comme perçu par les rapporteurs tout au long des auditions, les armées déplorent la rareté de la RH compétente et experte dans le champ de la GE au sein des forces armées.

**Dans l'armée de Terre, les trois unités spécialisées dans la GE affichent un effectif théorique de 1 700 personnels**. Or, le « référentiel des effectifs en organisation » (REO) n'est pas honoré, singulièrement pour la catégorie des sous- officiers qui constitue le cœur du vivier d'experts de la GE, alors même que la remontée en puissance sur ce segment imposerait de densifier fortement les effectifs, en augmentant le REO à près de 2 000 personnels *a minima*.

**Les autres armées et unités militaires spécialisées dans la GE connaissent les mêmes difficultés à armer leurs effectifs théoriques de guerriers électroniciens**. Les métiers sont en effet nombreux et se diversifient en raison du besoin de traiter en masse les données (*data scientists, data analysts*). Ces profils doivent donc évoluer afin de s'adapter aux changements de traitement et la multiplicité des cibles (hybridité, données de masse, accès au contenu, prolifération). Il est à noter que le recours à du personnel civil permet d'atténuer ce déficit.

Plusieurs raisons peuvent expliquer la non-atteinte des cibles de REO :

- Un manque de connaissances de ces métiers très techniques lors du processus de recrutement, et notamment dans les centres d'information et de recrutement des forces armées (CIRFA).

- La faible proportion d'équipements modernes de GE dans les unités rend moins attractive cette spécialisation.

- Une « *aspiration* » substantielle des volontaires vers le domaine voisin du cyber.

- L'extrême spécialisation et la durée de la formation. Face à l'étroitesse du vivier d'experts militaires, les armées peuvent faire occuper ces postes par des civils, faute de ressources.

**Ces insuffisances RH engendrent plusieurs problèmes collatéraux. Le COMCYBER a ainsi expliqué « *se nourrir* » des compétences des armées pour « *porter* » la montée en puissance de la GE sur les niveaux opératifs et stratégiques.**

L'enjeu de génération des compétences est donc majeur au niveau interarmées : « *Une vraie reconquête mérite donc d'être entreprise par les armées, en termes de flux/capacités de formation et d'entraînement/prépa-opérationnelle, ce qui impose d'innover dans la manière de recruter, former et fidéliser.*

*L'expérience du cyber, domaine aux compétences rares également, sera très utile : le bureau d'appui au recrutement cyber (BARC) est un succès qui doit nourrir la réflexion pour la GCEM.*

***Au sein du COMCYBER plus particulièrement, la création envisagée d'un véritable bureau dédié exclusivement à la GCEM doit offrir la possibilité de démultiplier les effets, au-delà des possibilités actuelles, reposant sur des ressources propres limitées et d'opportunité.*** *La réalisation d'une ambition forte reposera sur l'affectation de ressource experte en complément.* »

### b. *Le défi de la formation*

**Le défi de la formation est double**.

**Concernant la formation initiale, comme développé *supra* sur le déficit de formations scientifiques, le domaine « Télécom », exigeant qualitativement pour les compétences à développer, souffre d'un déficit d'image et peine à attirer les étudiants français en nombre suffisant.** Par ailleurs, en raison de sa sensibilité, les spécificités de la GE sont très peu connues du grand public, ce qui augmente la difficulté d'attirer de bons profils sachant que ses apprentissages relèvent du temps long.

Au sein des spécialités de GE, une formation de trois ans est nécessaire pour devenir linguiste. Pour intégrer la division « renseignement » de l'escadron de programmation et d'instruction de guerre électronique (EPIGE) de l'armée de l'air et de l'espace, une formation de deux à trois ans est également nécessaire pour les sous-officiers concernés.

La capacité à programmer une bibliothèque de guerre électronique sur Rafale requiert six ans de formation pour atteindre le grade de contrôleur de niveau 2.

**Les spécialités ne sont donc pas occupées par des sorties d'école mais par des sous-officiers en général expérimentés voire très expérimentés.** La problématique du long « tunnel de formation » a été abordée à de nombreuses reprises lors des auditions. Les armées essaient de prolonger les contrats des sous-officiers, de 5/6 ans initialement à 8/9 ans voire 12 ans pour certains sous-officiers, tant les spécialités sont complexes et requièrent de l'expertise.

**L'enjeu pour les armées est également de constituer et d'organiser un vivier dès les niveaux scolaires du secondaire (lycée) qui alimenterait une filière sur plusieurs décennies**.

**Plusieurs projets peuvent être imaginés** afin de construire ce vivier dans le temps : **formations spécialisées à construire ou à adapter avec l'Éducation nationale, découverte de la GE dès la fin du lycée par la réserve** (pour les élèves majeurs) ou par des périodes de découverte (à développer encore plus) *etc*. **Plusieurs personnes auditionnées par vos rapporteurs ont d'ailleurs proposé de créer un BTS « *guerre électronique* » sur le modèle du BTS « Cyber » devenu un véritable succès de recrutement**.

**Par ailleurs, la guerre électronique est un domaine technique particulièrement complexe requérant une formation continue tout au long de la carrière**. Le métier de guerrier électronicien demande à celles et ceux qui l'épousent une triple exigence : être un soldat, avec des compétences techniques, mais aussi une aptitude à faire évoluer ces compétences techniques au gré des évolutions technologiques de plus en plus rapides.

Ainsi, **au sein de la Marine nationale, les analystes** qui servent dans des centres à Terre en tant que responsables de la programmation des senseurs des unités et de l'exploitation froide des enregistrements, **suivent un cursus très qualifiant tout au long de leur carrière.**

### c. *La diffusion d'une culture GE au défi des armées*

**Sous-investie budgétairement depuis la fin de la guerre froide, la culture de la GE s'est érodée dans les armées**, tant et si bien qu'il semble souvent exister un écart entre le besoin opérationnel constaté sur le terrain par les unités et le besoin capacitaire perçu par les chefs militaires en matière de GCEM.

**Il importe par conséquent de combler ce fossé entre monde tactique et monde stratégique.** Sans sacrifier trop profondément aux développements théoriques, il reste évident que **la culture de la guerre électronique, par sa spécificité, relève d'un objet singulier.**

Soumise à de nombreuses et rapides évolutions technologiques, sa transmission, comme le veulent toutes les cultures professionnelles, par socialisation, de génération en génération au fur et à mesure du renouvellement des effectifs, n'en est pas facilitée.

Pour autant, **le statut professionnel des personnels militaires depuis la suspension du service national pourrait néanmoins aider au renforcement d'un « *esprit guerre électronique* »**, mais cet objectif ne pourra prospérer qu'au prix d'une meilleure communication dans et hors des forces armées sur l'intérêt de domaine de guerre.

**Au-delà du recrutement, se pose également la question de la fidélisation des personnels**, qui ne pourra probablement être résolue que par une approche innovante et éventuellement dérogatoire, compte tenu de l'importance vitale de la guerre électronique dans nos capacités de défense.

### 3. Le défi de la fidélisation

#### a. *Une évaporation importante*

**Les trois armées peinent *de facto* à conserver les profils recrutés en GE en raison d'une forte concurrence au sein et à l'extérieur du ministère des Armées, qui génère une « *évaporation* » de sous-officiers expérimentés dont le profil est recherché**.

En outre, la sous-dotation qualitative et quantitative en équipements des unités spécialisées contribue à la difficulté de fidélisation d'une population attirée par les nouvelles technologies et souvent déçue de ce qu'elle peut « trouver » en unités.

**Beaucoup de sous-officiers et d'officiers spécialisés dans la GE ont naturellement vocation à servir en interarmées et dans les trois services de renseignement du ministère, les unités spécialisées des armées servant souvent de « *pépinières* » pour les services.**

Toutefois, afin que l'évaporation soit moins douloureuse, la base disponible doit être considérablement élargie avec un effort substantiel mené sur le recrutement et la fidélisation.

**En outre, en milieu de carrière, les techniciens experts en guerre électronique développent nécessairement des profils d'intérêt pour la BITD qui offre à ces professionnels de haute volée une deuxième carrière aux conditions de rémunération supérieures.**

### b. *Reconnaître l'expertise et la payer*

**Fidéliser une population impose de reconnaître son expertise et de la payer.** Sans qu'il ne soit possible pour les armées de concurrencer les entreprises de la BITD, des outils de revalorisation des soldes pourraient être imaginés.

**Une prime de compétences spécifiques de guerrier électronicien pourrait être créée, dans les mêmes conditions que la prime de compétences spécifiques déjà existante pour les combattants parachutistes et parachutistes spécialisés.**

En outre, l'un des ressorts de la fidélisation au ministère des armées est indéniablement le sens de la mission qui renvoie aux déterminants exposés *supra* concernant la culture de guerre électronique et sa souhaitable attractivité. **Permettre aux opérateurs spécialisés de GE de partir en soutien des opérationnels sur le terrain peut contribuer à renforcer ce sens.**

**Surtout, l'arrivée espérée de nouveaux systèmes de GE modernes et performants serait un excellent vecteur de fidélisation.** Ainsi que l'a résumé l'AAE : « *L'arrivée prévue de nouveaux capteurs (SOLAR, ARCHANGE, systèmes satellitaires) va permettre de développer l'attractivité de ces spécialités et faciliter le recrutement. En outre le développement des compétences nouvelles (GE, IA, BIG DATA, développement) offre des options variées et davantage de perspectives à ces spécialistes.* »

### c. *Le découplage des grades et statuts*

**Sur le plan RH, la GE numérique complexifie les systèmes de GE mis en œuvre par des sous-officiers au risque d'atteindre les limites de leurs compétences.**

Ainsi, dans le cas du système de programmation et d'exploitation de guerre électronique du Rafale, la limite de ce que l'on peut demander à une population non constituée d'ingénieurs serait en passe d'être atteinte. Comme vos rapporteurs l'ont constaté lors de leurs visites de terrain au sein des régiments spécialisés de l'armée de Terre, les sous-officiers ont *de facto* une formation de sous-officier supérieur alors qu'ils demeurent statutairement des sous-officiers subalternes.

**Outre les contraintes d'effectifs et de niveau de la ressource, un enjeu majeur consiste à développer des automatismes soulageant la charge de travail des opérateurs et des analystes programmeurs.** Si l'intelligence artificielle génère de grandes attentes, elle obligera certainement la création de nouvelles spécialités d'experts destinées à l'exploitation et la modification de ce type d'outils afin que les armées conservent une autonomie opérationnelle.

**Afin de donner du sens à l'engagement, le développement de parcours RH cohérents en GE/cyber au sein des armées pourrait être renforcé.**

## D. LE DÉFI DE LA PREPARATION OPÉRATIONNELLE

### 1. Un cadre juridique national très contraignant pour les armées…

**L'utilisation du spectre radioélectrique par le ministère des Armées s'effectue dans le respect d'un cadre juridique et d'une règlementation nationale et internationale.**

**En temps de paix, ceci impose une gestion et un emploi rigoureux du spectre radioélectrique, en particulier pour l'entraînement à la mise en œuvre des systèmes de brouillage.**

**En l'absence de contrôle et de surveillance adaptés du spectre, ils peuvent compromettre la sécurité aérienne,** perturber les moyens de secours, comme le guidage des pompiers, ou provoquer des brouillages sur les bandes de fréquences des opérateurs téléphoniques, affectant ainsi les numéros d'urgence.

**Sur les théâtres d'opération militaire, les forces armées assument un contrôle accru du spectre tout en maintenant une coordination et une maîtrise des actions de brouillage pour limiter les effets collatéraux** sur les forces alliées et les infrastructures vitales.

**Si les contraintes à la pleine utilisation des moyens de GE sur le territoire national en temps de paix sont compréhensibles, il semblerait néanmoins que leur application très scrupuleuse constitue un frein majeur à l'innovation des industriels et la préparation opérationnelle des forces.**

La préparation opérationnelle en matière de GE est pourtant plus que jamais essentielle, dans un contexte où les forces armées françaises doivent se réapproprier des savoir- faire délaissés et s'approprier des nouvelles technologies toujours plus complexes.

**Le cadre réglementaire ne leur permettrait pas aujourd'hui de mettre en œuvre certains moyens sur le territoire national, notamment concernant l'attaque électronique (leurrage, brouillage).**

De ce fait, la manœuvre en « ambiance » GE pour les forces est complexifiée, notamment pour l'armée de Terre qui ne peut mettre en œuvre ses moyens de GE dans les eaux internationales (à l'instar de la Marine nationale) ou en surplomb de ces dernières (à l'instar de l'AAE).

D'après des éléments transmis en audition à vos rapporteurs, ***« Le processus mis en place pour obtenir les autorisations d'émettre,*** *depuis la constitution des dossiers, la gestion des fréquences et jusqu'à l'obtention des autorisations vis-à-vis des autorités (ANFR, DGAC)* ***pâtissent d'une lourdeur administrative et un protectionnisme sécuritaire certains****. La position très conservative systématique de la DGAC qui s'appuie principalement sur la réglementation de l'emploi du spectre « temps de paix » est une contrainte lourde pour l'entraînement de nos forces. »*

La capacité à mettre en œuvre du brouillage-leurrage sur le territoire national serait en cours de traitement sous pilotage SGDSN. Par ailleurs, la réflexion sur le cadre réglementaire relatif aux armes à énergie dirigée est actuellement analysée par la direction des affaires juridiques (DAJ) du ministère des Armées à la demande de l'EMA.

Il convient cependant de relever que plusieurs expérimentations ont déjà été menées en haute mer sur des navires de la Marine Nationale, l'EMMN communiquant régulièrement sur les créneaux d'embarquement possibles (notamment dans le cadre des TF LAD et GCEM). En outre, des expérimentations de brouillage avec la DGAC ont eu lieu à Captieux en juin 2025 pour étudier les effets des systèmes sur l'aviation civile.

### 2. …ainsi que pour les industriels

**Les difficultés à tester les matériels de GE sur le territoire national sont également éprouvées par les industriels de la défense.**

Ainsi, Safran a précisé à vos rapporteurs qu'« *en ce qui concerne le SKYJACKER (leurrage GNSS), des difficultés réglementaires pour les essais en France freinent notre capacité à innover ou évoluer dans ce domaine majeur. Des discussions sont en cours au niveau SGDSN pour assouplir ces règles (…).* »

**Moins contraignant juridiquement, le test de matériels de GE à l'étranger est possible, sous réserve d'avoir obtenu de la DGA une licence d'exportation des matériels concernés.**

### 3. De grands exercices pour pallier ces contraintes

**Toutefois, les armées profitent généralement de grands exercices dont le cadre règlementaire a été sécurisé des mois à l'avance pour pouvoir s'exercer à la GE sur le territoire national.**

Dans l'armée de Terre, les unités de GE spécialisée participent aux exercices d'ampleur (DIODORE, WARFIGHTER, *etc*.) qui leur permettent de consolider les savoir-faire détenus, d'affiner leur doctrine et d'exprimer leurs besoins capacitaires.

**L'armée de Terre expérimente par ailleurs des outils afin de mieux maitriser l'empreinte électromagnétique (EM) des structures les plus importantes, comme les postes de commandement (PC).**

En outre, après avoir mené une opération réactive qui a permis de doter les forces terrestres de capacités d'hybridation des réseaux de communication (HYDRE), elle envisage de systématiser la mise sous stress électromagnétique de ses unités pendant les exercices majeurs, notamment lors d'ORION 26, dans la mesure du possible selon les possibilités permises par le cadre réglementaire.

**L'AAE a évoqué devant vos rapporteurs une capacité d'entraînement GE aujourd'hui réduite (CCPGE) depuis la dissolution de l'escadron de guerre électronique (EGE).**

Le polygone de guerre électronique

**En 1979, les ministres de la défense américain, allemand et français décident de créer une structure d'entraînement en GE afin d'entraîner les pilotes à déjouer les menaces sol-air soviétiques**. Un protocole d'accord est signé en 1979, qui acte la naissance du polygone de guerre électronique. L'escadron de guerre électronique 48.530 est créé et divisé en plusieurs sites. Trois de ces sites sont situés en France (Jeuxey (88) Chenevières (54) et Grostenquin (57) et quatre sont situés en Allemagne dont la grande base aérienne américaine de Spangdahlem.

**L'EGE 48.530 était chargé, depuis 1990, de la simulation des menaces sol-air lors d'exercices interalliés et interarmées, notamment grâce à son système antiaérien mobile à courte portée SA8 « GECKO » (ou 9K33 OSA) conçu pour détruire des avions et des hélicoptères de combat d'origine soviétique.**

Dans le contexte des dividendes de la paix, l'EGE a été dissout en 2014. L'ordre du jour de la dissolution de l'EGE 48.530 précisait cependant que les « *missions d'entraînement à la guerre électronique continueront à être assurées par le polygone de guerre électronique en cours de modernisation pour l'adapter aux besoins actuels et futurs (…).*

*Les autres unités du PGE prendront le relais pour assurer les missions menées par les 23 aviateurs de l'escadron, en utilisant les moyens radars de Grostenquin, Jeuxey et Chenevières et des moyens mobiles.*

*La BA 133 de Nancy-Ochey sera quant à elle chargée de la gestion de l'espace aérien dédié au PGE. Enfin, au sein de ce dernier, l'armée de l'Air sera représentée par « les aviateurs intégrés au sein du centre de coordination du PGE, implanté en Allemagne, à Bann, à quelques kilomètres de la base aérienne de Ramstein ».*

L'AAE a évoqué le développement conjoint de moyens de simulation travaillant en réseau (SMR) avec des moyens réels déployables sur un terrain de manœuvre afin de reproduire les menaces actuelles de la manière la plus réaliste et pédagogique possible.

**La DGA a ainsi acquis trois systèmes mobiles ARPEGE dont la mise en service opérationnelle a été prononcée par l'AAE.** Selon la DGA, ARPEGE est le moyen de remplacement du polygone de guerre électronique : « *Cette capacité de simulation de la menace sol-air a été employée très tôt, dès sa phase d'expérimentation menée par le CEAM. Les forces ont mesuré rapidement l'apport opérationnel d'ARPEGE dans l'entrainement des équipages :* ***son emploi est devenu ainsi systématique lors de la préparation opérationnelle des forces en France*** *(opération POKER des FAS, exercice VOLFA de l'AAE, exercice GE BLACK CROW) et à l'étranger (mission TLP en Espagne).* »

Si cette capacité développée en 2017 par le CEAM constitue probablement la « *meilleure simulation de menaces en Europe* », le nombre de véhicules blancs légers constituant la capacité ARPEGE (3) devrait *a minima* être doublé et la puissance des simulateurs augmentée afin de répondre aux besoins de simulation des menaces sol-air longue portée actuelles.

L'AAE s'entraîne à opérer en environnement EM contesté ou en recherchant une « sobriété électromagnétique » (discrétion électromagnétique), enjeux majeurs intégrés aux tactiques lors d'exercices comme VOLFA.

**Les forces aériennes stratégiques (FAS) planifient et exécutent régulièrement des opérations de grande ampleur, telles que l'opération POKER, intégrant l'ensemble des menaces envisageables dans le champ électronique** (brouillage radio et GPS, multiples systèmes sol-air adverses,

manœuvre de déception électronique, etc.). Ces opérations démontrent et entretiennent la compétence des FAS à conduire des raids aériens en milieu hostile.

**L'un des enjeux de la préparation opérationnelle consiste donc à maintenir des moyens humains et techniques nécessaires pour assurer un niveau d'entraînement suffisant et en phase avec les évolutions capacitaires.**

L'exercice Black Crow de l'AAE

**BLACK CROW (BC) est une activité d'entraînement à la guerre EM de niveau tactique et de type LIVEX qui a eu lieu en France, en zone Centre, en 2024 et en 2025.** « BC25 » a offert une trentaine de créneaux d'environ 1 h 30 aux forces et 55 missions, leur permettant d'opérer en environnement brouillé (radio, GNSS22, L1623) face à une quarantaine de systèmes sol-air représentatifs, réels ou simulés du Polygone de Guerre Électronique (PGE), de l'EDSA d'Istres et du 54ème RA de Hyères (armée de Terre). « BC25 » a nécessité le déploiement sur le terrain d'environ 300 hommes et 340 tonnes de matériel.

**L'édition 2025 de BC a ainsi considérablement augmenté les moyens mis en œuvre par rapport à la première édition, en 2024, avec une situation tactique générale conçue par les experts tactiques de la *Weapons School* du CEAM, une quarantaine de moyens répartis sur le terrain, assurant densité, représentativité et incertitude des menaces ainsi que la mise en place pour la première fois d'une instance de coordination de l'ensemble de la manœuvre GE (C2 GE qui coordonne à plusieurs niveaux, brouillage et défense sol-air au profit de la manœuvre adverse).**

Au-delà de l'entraînement l'édition 2025 a, comme en 2024, contribué au développement capacitaire, avec une activité importante au profit des expérimentations du CEAM (RAFALE F4.1 et A400M), de la DGA et, pour la première fois, la participation de l'industrie (Dassault Aviation). La DGA et l'industrie soulignent l'intérêt majeur à bénéficier d'une telle concentration de moyens au profit de la préparation de l'avenir.

**Sur le plan de la préparation opérationnelle, l'exercice a souligné la nécessité pour les escadrons de se réhabituer au traitement de la menace GE et à évoluer dans des environnements contestés (brouillage).** Les scenarii joués renforcent le caractère crucial du savoir-faire en TTBA[24] pour l'AAE. Les enseignements sont également nombreux pour les opérateurs de défense sol-air confrontés à la réalité d'un déploiement avec mobilité, interconnexion et coordination (déploiement réseaux, connections L16).

Sur le plan capacitaire, l'A400M et le RAFALE à son dernier standard ont pu éprouver leurs nouvelles fonctionnalités, notamment, d'autoprotection.

---

[22] *Global Navigation Satellite System dont fait partie le GPS par exemple.*

[23] *Liaison 16 : liaison de données tactique permettant la mise en réseau des systèmes de combat tels que les aéronefs les sol-air et les centre de commandement par exemple.*

[24] *Très très basse altitude : hauteurs de vol < 500ft permettant de se soustraire à l'intervisibilité, en se mettant hors de portée optique et exploitation des masques terrains. Cela empêche la détection par les radars adverses et place hors de portée des brouilleurs. ;*

**Sur le plan réglementaire, des progrès sont à réaliser pour être en mesure de mettre en œuvre du brouillage GPS de niveau suffisant sur le territoire national (le système expérimenté sous l'égide de l'EES a été très efficace sur le brouillage radio et L16).**

**Sur le plan de l'organisation de l'exercice, la structure de C2 GE mise en œuvre lors de BC25 est apparue indispensable au réalisme de la réplication de la menace d'un *IADS*[25] ennemi, au profit des équipages et opérateurs.** Cette fonction de coordination, notamment des systèmes sol-air, doit être pérennisée. BC25 fut l'occasion de former trois personnels à cette fonction, de manière à bénéficier de cette expertise lors des futurs exercices majeurs.

Dans le domaine de la préparation opérationnelle, **l'AAE a exprimé devant vos rapporteurs le besoin de restaurer un polygone de GE pour entraîner les forces grâce à des simulateurs de menace EM, des systèmes d'armes réels, des leurres de systèmes sol-air (perception visuelle et IR réaliste), des systèmes de simulation de départ missile (fumée – smokey SAM) ainsi que des simulateurs de la menace infrarouge (RAMAGE développé par CEAM).** La dotation en outils de « *débriefing* » de la menace sol-air avec modélisation des trajectoires missiles serait également très opportune.

Les unités de **la Marine nationale s'entraînent également spécifiquement chaque année, à l'occasion des exercices de grande ampleur de type POLARIS ou ORION, à prendre l'ascendant opérationnel**, conditionné par la supériorité informationnelle et la maîtrise de la signature électromagnétique.

Par ailleurs, le programme AGORA vise à produire un démonstrateur à l'horizon 2027 présentant l'empreinte électromagnétique des unités, en vue de mieux la contrôler.

**En 2026, ORION26, exercice « incubateur » interarmées majeur des capacités françaises, fournira une opportunité unique d'expérimenter des options et constituera un jalon majeur de la montée en puissance de la capacité interarmées de GCEM.**

## E. LE DÉFI ORGANISATIONNEL

### 1. Une meilleure coordination de la GE au sein du ministère des armées

Le COMCYBER a été récemment désigné coordonnateur de « *l'aptitude interarmées GE* ».

---

[25] *Integrated Air Defense System : système de défense aérienne intégrée, ensemble de moyens de détection de commandement de control et de communication permettant une mise en réseau des défenses sol-air*

Compte tenu des cultures d'armées différentes et de besoins technico-opérationnels différenciés entre les armées (COMINT pour l'AdT *versus* ELINT et autoprotection des plateformes pour la MN et l'AAE), il devenait *in fine* difficile de faire émerger, sur une base budgétaire réduite, une vision commune et cohérente de la GE aux niveaux opératif et stratégique, selon une approche M2MC[26] aujourd'hui indispensable à la combinaison des effets.

**Le COMCYBER a donc été désigné l'an dernier par le Major général des armées (MGA) pour prendre la présidence unique du comité exécutif (COEX) GCEM,** toujours subordonné à un comité directeur piloté par la division emploi des forces de l'EMA. **Cette présidence unique met fin à la présidente tournante du COEX entre les armées.**

**Le COMCYBER ne dispose actuellement d'aucune responsabilité opérationnelle en matière de GCEM. Il agit en stratège du domaine, coordonnateur des efforts et des travaux en la matière (doctrine, organisation, RH, équipement, soutien, entraînement) menés par les entités habituellement en charge de ces questions au sein du ministère.**

Domaine éminemment transverse dans ses besoins comme dans ses effets, la GE doit en effet pouvoir s'appuyer sur de nombreuses fonctions concourant à son efficacité et à sa parfaite intégration dans la manœuvre.

La construction capacitaire implique des relations étroites avec les armées comme avec l'ensemble des organismes détenant des responsabilités dans ce domaine.

**Ces éléments ont justifié la rédaction en 2025 par le COMCYBER d'une stratégie d'opérationnalisation fournissant à chacun des acteurs le cadre général de l'action.** L'ensemble des acteurs concernés ont participé aux groupes de travail organisés par le COMCYBER.

**Le COMCYBER incarne aujourd'hui le niveau opératif et stratégique de la guerre électronique.** Il permettra en cas d'engagement majeur dans un contexte de haute intensité de garantir une bonne coordination de l'emploi des moyens de ce domaine entre les armées, ce qui manquait jusqu'à présent.

Sur le plan purement capacitaire, la division « cohérence capacitaire » de l'EMA et la DGA co-pilotent une « Task Force » « Attaque EM ». Le COMCYBER travaille étroitement avec cette dernière afin d'assurer « *la cohérence de ses travaux avec le besoin des armées qui se nourrit du RETEX des conflits en cours, avec le besoin de niveau opératif (effort majeur au vu des conflits en cours) et ceux du niveau stratégique, portés par le COMCYBER* ».

---

[26] *Multi-milieux multi-champs.*

**Cette nouvelle organisation apparaît équilibrée entre les armées. Le champ électromagnétique étant un champ de bataille essentiel, dont la maîtrise conditionne celle des autres milieux et champs, il était dès lors nécessaire qu'il soit incarné au niveau stratégique**.

À défaut de véritable commandement de la GE, vos rapporteurs saluent la mise en place par les armées d'une gouvernance permettant d'animer la fonction GE et de coordonner les différents travaux au niveau interarmées.

Si cette aptitude a été attribuée au COMCYBER, vos rapporteurs souhaitent rappeler que **la fusion des deux champs GE et Cyber, qui demeurent dans les faits deux espaces de batailles distincts, est à proscrire.** Notamment, l'appellation de l'aptitude « guerre EM » mérite d'être préservée afin de maintenir de façon distincte les deux aptitudes interarmées.

### 2. La nécessaire mise en place d'une chaîne C2 dédiée à la GE

#### a. *Une meilleure maîtrise du spectre EM*

**Des travaux capacitaires actuellement menés par le COMCYBER devraient notamment permettre de développer des outils d'hypervision du spectre électromagnétique.** L'objectif est de mettre en œuvre une organisation de guerre électronique « donnée-centrée » permettant le traitement des informations d'un plus grand nombre de capteurs, mis en réseau, favorisant une meilleure appréciation de situation dans le champ électromagnétique.

**La connaissance de la situation tactique électromagnétique sur le champ de bataille est en effet primordiale pour analyser le spectre et déterminer les forces en présence, dans le but de coordonner les actions de guerre électromagnétique.**

**On parle à cet égard de météo spectrale. Plus la connaissance de la situation tactique électromagnétique est précise, plus la gestion du spectre en réaction est fine (par exemple, réallocation de fréquences en temps réel).**

L'hypervision du spectre EM sera à même de réduire les tirs fratricides et les problèmes de compatibilité électromagnétique au sein d'une même force. Selon des informations partagées en audition, 43 % des actions de brouillage actuellement menées en Ukraine seraient fratricides.

#### b. *Élaborer une chaîne C2 dédiée à la GE*

Aujourd'hui en opération, il revient au poste de commandement (PC) interarmées de théâtre de réaliser la coordination / synchronisation des effets cinétiques et EM, mais sans chaîne de commandement et de contrôle (C2) dédiée.

Vue comme une capacité offensive, défensive ou comme un moyen de surveillance, la guerre dans le champ électromagnétique (GCEM) s'intègre dans la chaîne de commandement « C2 » générale, intégrée et unifiée en vigueur au sein des armées.

**Afin de permettre cette parfaite intégration de la GCEM au niveau opératif comme stratégique, une chaîne de commandement (C2) propre à la GCEM sera testée pendant l'exercice interarmées ORION26 avant d'être formalisée**.

À terme, la mise en œuvre pérenne d'une chaîne C2 dédiée à la GE permettrait de coordonner les effets cinétiques et électromagnétiques de théâtre. De cette façon, les forces seraient en mesure de perturber immédiatement l'appréciation de situation et la manœuvre de l'adversaire par des actions coordonnées entre composantes tactiques, en défense et en attaque, dans les domaines EM et cinétiques. **La manœuvre GE serait ainsi pleinement intégrée aux effets de la manœuvre interarmées.**

### 3. Une armée spécifique ?

**Vos rapporteurs se sont interrogés sur l'opportunité de créer une armée ou un commandement spécifique pour la GE, à l'exemple des forces armées russes, ce qui pourrait donner à cette forme de combat une lisibilité plus grande en termes budgétaires et stratégiques.**

**Interrogées par vos rapporteurs sur ce sujet, les armées ont globalement estimé qu'à ce stade, en l'absence de recul sur la désignation du COMCYBER en tant que « *coordinateur de l'aptitude interarmées guerre électronique* », il semblait prématuré de se positionner sur la nécessité de créer un commandement dédié à la guerre électronique.**

Par ailleurs, l'état-major de la Marine nationale a notamment rappelé que « *Les besoins propres aux armées diffèrent de manière importante : les problématiques liées à l'environnement maritime sont peu partagées avec les autres armées. Si des coordinations peuvent être requises ponctuellement (amphibie, dispositif de protection sur le territoire national), un commandement dédié n'apparait pas nécessaire.* »

Les besoins en GE étant très spécifiques à chaque milieu (aérospatial, mer, terre), le modèle actuel conserve l'expertise au plus près des forces qui l'emploient.

**En outre, la doctrine militaire française actuelle, telle que décrite dans le concept d'emploi des forces (CEF), met l'accent sur l'intégration plutôt que sur la création de nouvelles structures spécialisées qui pourraient devenir des**

**silos. L'approche française privilégie ainsi l'intégration multi-milieux et multi-champs (M2MC).**

La stratégie d'opérationnalisation de la GE vise à dépasser la simple coordination pour atteindre une « *culture de convergence de toutes les actions* ». L'objectif est une « *intégration aboutie des effets produits par l'ensemble des acteurs* ». Créer un commandement GE séparé pourrait aller à l'encontre de ce principe d'intégration native.

**Le modèle choisi, avec un coordinateur interarmées (COMCYBER) et des référents de haut niveau dans chaque armée (comme l'OG GCEM pour l'AAE), privilégie ainsi une intégration profonde de la GE dans la manœuvre de chaque armée**, plutôt que de la centraliser dans un commandement unique et potentiellement déconnecté des réalités de chaque milieu.

## EXAMEN EN COMMISSION

*La commission procède à l'examen du rapport de la mission d'information sur « la guerre électronique » le mercredi 18 février 2026.*

**M. le président Jean-Michel Jacques.** Messieurs les rapporteurs, chers collègues, nous commençons nos travaux par l'examen des conclusions de la mission d'information sur la guerre électronique, dont les rapporteurs sont MM. Didier Lemaire et Thierry Tesson.

Au préalable, je tiens à exprimer, au nom de notre commission, notre profonde tristesse après le décès accidentel de l'engagé volontaire sous-officier Titouan Langlet, survenu lors d'un entraînement pendant sa formation à l'École nationale des sous-officiers d'actives. De même, en notre nom à tous, je rends hommage au sergent-chef Thibaud Breteau, mort accidentellement en opération dans l'accomplissement de sa mission. Nous assurons leurs familles, leurs proches et leurs frères d'armes de notre solidarité.

Je reviens à présent à notre ordre du jour. Messieurs les rapporteurs, je tiens à vous remercier et à vous féliciter pour la qualité de votre travail sur cette mission d'information. À quelques semaines de l'actualisation de la loi de programmation militaire (LPM), vos conclusions sont attendues pour contribuer à un état des lieux de nos capacités de guerre électronique et leur développement. Lors de son discours à l'hôtel de Brienne le 13 juillet 2025, le président de la République, chef des armées, a évoqué nos moyens de guerre électronique en les incluant dans notre zone de fragilité, et a insisté sur la nécessité de les renforcer. Avec nos collègues Chenevard et Saint-Pasteur, nous l'avions également évoqué lors de notre rapport d'évaluation de la loi de programmation militaire que j'ai présidée.

La guerre électronique est un sujet technique, souvent méconnu, mais fondamental pour l'ensemble de nos armées. Au même titre que le génie que nous avons évoqué la semaine dernière, son usage massif est naturellement revenu au premier plan avec la guerre en Ukraine. De la même manière, l'an dernier, l'aviation israélienne a pénétré en profondeur dans le territoire iranien pour pouvoir porter des frappes précises.

C'est vous dire l'importance de votre travail ; dont nous vous remercions. Vous formulez ainsi plusieurs recommandations dans votre rapport pour assurer le bon dimensionnement de nos capacités de la guerre électronique dans ces différents volets, qu'il s'agisse du renseignement, de l'attaque ou de la défense électromagnétique. Enfin, afin de conduire votre mission, vous avez effectué plusieurs déplacements pour aller rencontrer nos unités spécialisées dans la guerre électronique. Vous avez également visité plusieurs petites entreprises de notre base industrielle et technologique de défense (BITD), qui disposent d'une expertise précise dans ce domaine.

Je vous cède sans plus tarder la parole.

**M. Thierry Tesson, rapporteur de la mission d'information sur la guerre électronique.** En préambule, je veux rappeler l'état d'esprit dans lequel nous avons conduit ces travaux. Deux idées directrices nous ont guidés. La première était de rendre intelligible un sujet qui, par nature, demeure complexe, technique et souvent méconnu. La seconde idée, toute aussi essentielle, consistait à apporter une contribution utile à nos forces armées. Ce travail devait leur servir, leur permettre de tirer parti d'une réflexion approfondie, menée durant plusieurs mois, appuyée sur de nombreux entretiens, et formalisée dans un rapport qui, je l'espère, trouvera une utilité opérationnelle.

La guerre électronique est un domaine sensible, technique et encore insuffisamment connu. Il n'avait plus fait l'objet d'une étude parlementaire d'ampleur depuis longtemps : le dernier rapport remonte à 2013, et l'un des précédents à 1980. Pourtant, aujourd'hui, ce champ est crucial pour les conflits de haute intensité et les formes contemporaines d'affrontement. Pour bien saisir son importance, il faut revenir brièvement à son origine.

En 1864, Maxwell établit théoriquement l'existence des ondes électromagnétiques, qu'il imagine voyager dans l'espace à la vitesse de la lumière. Il faudra toutefois attendre vingt ans pour qu'Heinrich Hertz, par une expérience décisive, démontre qu'il est effectivement possible d'émettre et de capter une onde à travers l'espace. Cette découverte, prodigieuse pour l'époque, a immédiatement suscité l'intérêt des civils, mais aussi des militaires. Très vite, les armées ont perçu son potentiel et les ondes sont devenues un moteur fondamental de l'innovation dans le domaine du spectre électromagnétique.

La guerre dans le champ électromagnétique est ainsi définie comme « *l'action militaire qui exploite l'énergie électromagnétique pour fournir une appréciation de situation opérationnelle et délivrer des effets offensifs et défensifs* ». Très tôt, dès la première guerre mondiale, l'usage militaire des ondes s'est structuré selon trois fonctions majeures, qui demeurent encore aujourd'hui les fondements de la guerre électronique. La première est le renseignement, l'écoute : il s'agit d'intercepter les communications ennemies, de localiser les émetteurs, de recueillir l'information tactique et stratégique qui circule sur le spectre. La deuxième fonction concerne l'action offensive, qui vise à brouiller, neutraliser ou détruire les capacités adverses, pour empêcher l'ennemi de communiquer. La troisième relève de la défense : protéger son propre spectre, chiffrer, changer de fréquence, détecter les tentatives de leurrage, ou encore détruire de manière cinétique les moyens adverses.

Au fil du XX$^{e}$ siècle, l'usage militaire du spectre n'a cessé de s'étendre à mesure que progressaient les technologies de communication. L'entre-deux-guerres a vu l'invention du radar, qui a jouté un rôle décisif durant la seconde guerre mondiale en permettant de détecter et de mesurer la position d'avions, de navires ou de phénomènes météorologiques. Les opérations alliées d'Overlord constituent

d'ailleurs un exemple remarquable de l'emploi combiné de tous les leviers de la guerre électronique : le brouillage massif, l'intoxication, le camouflage électromagnétique. Ces opérations ont été réalisées sans ordinateur à l'époque, ce qui rend la performance d'autant plus impressionnante.

La période de guerre froide a marqué une intensification majeure. Face à la détention simultanée d'armes nucléaires, les blocs ont cherché des moyens de domination indirecte, rendant la guerre électronique centrale. La situation a changé à la fin de la guerre froide. Les conflits asymétriques, les opérations extérieures et les opérations de gestion de crise ont relégué la guerre électronique à un rôle secondaire. L'effort a moins porté sur le radar ou sur les actions offensives, mais davantage sur les communications radio. La guerre électronique est alors devenue une variable d'ajustement budgétaire, parfois même la variable d'ajustement de la variable d'ajustement. En conséquence, un déficit capacitaire s'est progressivement installé.

Or, aujourd'hui, la guerre électronique est redevenue un facteur déterminant des conflits modernes. Certes, elle ne suffit pas à gagner une guerre, mais en être dépourvu revient à livrer à l'adversaire une supériorité opérationnelle décisive. Les conflits récents, surtout celui d'Ukraine, servent de révélateur. Le champ de bataille ukrainien est ainsi marqué par un environnement électromagnétique extrêmement dégradé, un brouillage massif, permanent et organisé, résultant des dispositifs multicouches déployés par les forces russes et ukrainiennes, héritières du système soviétique.

Les Russes et les Ukrainiens déploient un « mur de brouillage » qui sature l'ensemble du spectre. Cet environnement saturé ne constitue pas seulement un cadre général des opérations, mais produit des effets directs mesurables sur les capacités militaires engagées. Il s'agit notamment de la dégradation concrète des systèmes clés, en particulier ceux reposant sur les services spatiaux et les technologies de navigation et de guidage, au cœur des doctrines occidentales du combat de précision.

La guerre électronique s'impose également comme une composante centrale de la lutte anti-drones, en intervenant à toutes les étapes de la chaîne opérationnelle, aussi bien pour la détection, l'identification des vecteurs aériens que pour la neutralisation par brouillage, leurrage ou prise de contrôle.

D'après le droniste Cerbair que nous avons rencontré dans ses locaux à Montrouge, 80 % des pertes matérielles et humaines en Ukraine relèvent aujourd'hui de ces technologies. Les deux belligérants en Ukraine adoptent en permanence leurs méthodes, leurs logiciels et équipements, afin de prendre l'ascendant électromagnétique sur l'adversaire.

Cette logique d'adaptation et de contre-adaptation s'effectue très rapidement. Selon les éléments portés à notre connaissance, les évolutions logicielles interviendraient tous les un à deux mois, tandis que les évolutions matérielles seraient

passées à six mois, en réduction constante. Toute émission électromagnétique non maîtrisée expose immédiatement le système à une localisation précise, puis à une neutralisation rapide en l'absence de manœuvre ou de dispositif de protection adaptée.

Au-delà de la seule guerre en Ukraine, la guerre électronique massive conduite par Israël contre l'Iran lors de la guerre des douze jours a offert une supériorité évidente aux forces israéliennes. De même, lors de l'opération au Venezuela en janvier 2026, la guerre électronique menée par les Américains, notamment grâce aux fameux avions Growler, a permis aux forces spéciales américaines d'intervenir sans déplorer de pertes.

Toutefois, en décalage manifeste avec son rôle essentiel dans les conflits récents, la guerre électronique occupe une place faiblement lisible dans l'actuelle LPM. Ainsi, le terme « électromagnétique » n'intervient qu'à trois reprises dans l'ensemble du texte. Dans ce rapport, nous appelons par conséquent à une remontée en puissance rapide des armées françaises dans le champ de la guerre électronique.

**M. Didier Lemaire, rapporteur de la mission d'information sur la guerre électronique.** En tant que député élu en Alsace, je suis particulièrement honoré de vous parler de cette mission. En effet, l'Alsace est la terre d'implantation historique des deux régiments spécialisés dans la guerre électronique : le 54e régiment et le 44e régiment de transmissions.

Traditionnellement, la guerre électronique marine et air est davantage spécialisée dans le domaine radar, tandis que la guerre électronique terrestre relève davantage du domaine radio. La remontée en puissance capacitaire des armées dans ce domaine devra donc être adaptée à chaque armée.

Dans notre rapport, nous formulons un ensemble d'axes d'efforts et de recommandations, afin d'adapter la densification du segment guerre électronique aux besoins de chaque armée. Nous nous sommes notamment déplacés à Brest, à bord de la frégate Amiral Ronac'h. Il apparaît nécessaire que la Marine nationale continue de consolider son socle en matière de maîtrise du spectre électromagnétique. Avant d'attaquer et afin de se défendre, il faut être en mesure de comprendre l'environnement. En matière de défense électromagnétique, l'objectif consiste à équiper les grandes unités de brouillage antimissiles et de brouillage antidrones. Toutes les frégates de premier rang devront être équipées tandis que l'autoprotection des frégates de second rang devra être renforcée. Si la Marine conserve une compétence reconnue dans la protection antimissiles et antinavires, cette capacité s'est développée dans un contexte marqué par un sous-investissement dans la guerre électronique.

Les bâtiments sont ainsi dotés d'équipements performants, mais ils apparaissent en nombre insuffisant, conséquence de choix capacitaires contraints. Cette situation aboutit à un constat préoccupant : l'ensemble des navires n'est pas

aujourd'hui équipé de manière homogène et complète en moyens de guerre électronique, fragilisant la cohérence globale des dispositifs de protection.

Ensuite, l'armée de l'air et de l'espace (AAE) souhaite assurer une continuité de la surveillance dans les domaines radio et radar, à travers la complémentarité de moyens d'écoute au sol et aéroportés. Dans le domaine défensif, un effort substantiel doit être mené pour l'autoprotection électromagnétique des flottes d'avions, de transports et d'hélicoptères. L'AAE dispose d'aéronefs équipés de systèmes d'autoprotection aux performances hétérogènes, induisant des différences d'employabilité élevées en fonction du théâtre. Ainsi, face à certains types de menaces, les équipements offrent des niveaux de protection assez disparates sur l'ensemble de la flotte.

Pour ne pas seulement subir la guerre électronique adverse, l'AAE doit se doter à nouveau d'une capacité offensive de suppression des défenses aériennes ennemies. L'objectif consiste à neutraliser les systèmes de défense, notamment les radars, pour permettre aux aéronefs de pénétrer un espace aérien contesté. La capacité à entrer en premier dans le cadre d'une opération conventionnelle impose de se doter de moyens de brouillage offensifs, aéroportés et de missiles antiradars de destruction des radars, de systèmes sol-air longue portée.

L'acquisition d'une capacité de brouillage électromagnétique au sol permettra en particulier la défense des bases aériennes de l'AAE et de points sensibles, notamment contre tous les types de menaces de drones de moyenne altitude ou de longue endurance, de munitions téléopérées ou guidées par GPS, d'aéronefs habités. Des capacités de brouillage et de leurrage devront également être développées depuis la très haute altitude (THA) et l'espace, la guerre électronique se jouant également dans ces nouveaux milieux opérationnels. Ces milieux constituent en quelque sorte la nouvelle frontière du champ électromagnétique. Certains de nos compétiteurs stratégiques investissent toujours plus sur ces segments.

Concernant l'armée de Terre, les unités spécialisées sont confrontées à un besoin marqué de réinvestissement du champ offensif. En particulier, les capacités de brouillage à forte puissance ont été largement délaissées au cours des dernières décennies, en raison de l'engagement prioritaire dans des conflits asymétriques, dans lesquels la supériorité électromagnétique adverse était limitée.

Par ailleurs, si l'armée de Terre a acquis au fil des années une expertise solide dans le domaine de la guerre électronique radio, elle doit désormais renforcer de manière significative ses compétences en guerre électronique radar, en particulier dans sa fonction de renseignement. Cette montée en compétences est essentielle pour appuyer le ciblage dans le cadre de la boucle de reconnaissance-frappe, dont l'importance s'accroît dans le développement des tirs dans la profondeur. Des investissements budgétaires significatifs doivent être engagés, afin de permettre à l'armée de Terre de mettre en œuvre ses objectifs de guerre électronique.

Il sera notamment indispensable de densifier le segment spécialisé, en le dotant de capacités sous blindage de détection et de localisation des radars et d'attaque de communication et des réseaux adverses, pour être en mesure d'acquérir la supériorité dans le champ électromagnétique. Très concrètement, la capacité détenue par le 54e régiment de transmissions pourrait être doublée, en créant un second régiment tactique de guerre électronique, et ainsi répondre à l'objectif de l'armée de Terre de constituer un corps d'armée pleinement opérationnel à l'échéance 2030.

En outre, nous insistons dans le rapport sur le nécessaire renforcement de la lutte anti-drones aux abords de nos bases militaires nationales. La France a été confrontée depuis l'automne 2025 à plusieurs survols non autorisés des sites sensibles comme la base de l'île Longue, pilier de la dissuasion océanique, mais aussi les sites de Mourmelon, de Creil ou l'entreprise Eurenco à Bergerac. Seule une combinaison de surveillance permanente du spectre et de capacités électromagnétiques robustes permettra de sécuriser durablement les emprises stratégiques françaises. Par ailleurs, nous appelons à renforcer l'attractivité des métiers d'opérateurs spécialisés en guerre électronique, qui souffrent de difficultés de recrutement et de fidélisation des personnels.

Enfin, notre rapport formule de nombreuses recommandations concernant la production de matériel de guerre électronique par la BITD française. La guerre en Ukraine nous enseigne l'importance de ne pas se focaliser à l'excès sur les types d'équipements utilisés par les belligérants, compte tenu de la rapidité de leur caducité. *A contrario*, il s'agit en priorité de savoir produire rapidement et en flux continu les capacités innovantes pour garder une longueur d'avance sur l'adversaire. Les théâtres de conflit en Ukraine ou au Moyen-Orient nous démontrent à quel point cette réactivité est nécessaire.

Aussi, la priorité en matière de guerre électronique consiste aujourd'hui à mettre en place des conditions pour bâtir un écosystème industriel qui saura produire en masse, au moment où nous pourrions être engagés dans un conflit de haute intensité. La guerre électronique nécessite une adaptation quasi permanente des réponses en fonction de la menace, réaction souvent en décalage avec les grands programmes d'armement, comme les programmes à effet majeur (PEM). Les PEM conçus de manière conventionnelle s'avèrent peu pertinents dans un champ hyper technologique, où les besoins des trois armées sont uniformes.

Il importe donc d'adapter les PEM au rythme de la guerre électronique, en faisant prévaloir une logique de flux plutôt qu'une logique de stock. Ainsi, l'acquisition en une fois d'une masse de capacités fait courir le risque de disposer de moyens rapidement obsolètes. À l'inverse, l'achat de volumes limités de systèmes selon un cycle de rafraîchissement technologique régulier et constant semble plus indiqué.

Cette nouvelle organisation supposerait d'étendre les prérogatives et les crédits des forces en matière d'innovation, de mettre en œuvre des mécanismes de financement extrêmement réactifs ainsi que des mécanismes de certification allégés. En outre, les équipements de guerre électronique des armées françaises devront, autant que possible, bénéficier d'architectures modulaires, ouvertes et collaboratives, capables d'adaptation.

J'insiste sur cette adaptation précoce, sur le terrain d'une BITD de « l'avant », dans le cadre de cycles d'innovation accélérés. En outre, une coopération plus étroite entre industriels, services de renseignement et forces armées semble impérative. Les trois services des armées responsables d'innovations capacitaires ont exprimé le souhait de voir les industriels de la guerre électronique davantage associés aux grands exercices des armées, afin d'accélérer d'éventuelles contractualisations avec la direction générale de l'armement (DGA).

En outre, il semble nécessaire de renforcer la souveraineté et la résilience des chaînes de valeur. La majorité des équipements de guerre électronique utilisés par les armées françaises doit provenir d'entreprises nationales. La souveraineté de la chaîne de valeur est indispensable, en raison de la manipulation de données permettant de caractériser les capacités de guerre électronique de l'armée française.

Par ailleurs, les rares matériels étrangers composant les équipements de guerre électronique français imposent également des restrictions d'emplois spécifiques, en cas de panne ou dysfonctionnement des équipements. Il faut également mentionner une problématique en termes de matières premières critiques. Les systèmes de guerre électronique, et plus généralement des systèmes utilisés par la défense, utilisent des métaux et terres rares. Compte tenu des tensions géopolitiques, les risques liés à leur approvisionnement existent. Une des réponses pour atténuer ces risques passera par la mise en place de filières de recyclage souveraines nationales ou de l'Union européenne (UE), au bénéfice de l'ensemble de la BITD.

En conclusion, la prochaine actualisation de la LPM, dont notre commission sera bientôt saisie, devra renforcer de manière décisive l'enveloppe budgétaire consacrée à la guerre électronique, dans une optique de rattrapage et de remontée en puissance.

**M. le président Jean-Michel Jacques.** Je vous remercie et cède la parole aux orateurs de groupe.

**Mme Catherine Rimbert (RN).** Je vous remercie à mon tour pour vos travaux. Comme vous l'avez souligné, la guerre électronique constitue aujourd'hui une dimension essentielle des conflits modernes, dans la mesure où le spectre électromagnétique est devenu un véritable champ de confrontation : drones, capteurs, systèmes de liaison de données et brouillages s'y affrontent sans relâche.

En conséquence, celui qui parvient à dominer ce spectre électronique dispose d'un avantage décisif sur l'adversaire. Si la guerre électronique ne suffit pas à elle seule à remporter un conflit, perdre le contrôle du champ électromagnétique expose directement à la défaite. Les récents événements l'illustrent sans ambiguïté. Dans certaines opérations, les forces américaines ont utilisé des avions spécialisés dotés de capacités de brouillage pour neutraliser rapidement radars et liaisons adverses, désorganisant ainsi les défenses avant toute action cinétique. Parallèlement, les forces ukrainiennes ont fait de la domination du spectre une réalité quotidienne, grâce à des systèmes de brouillage continus qui perturbent drones, communications et guidages de munitions sur le front.

Ce contexte stratégique a conduit la France à renforcer ses capacités dans ce domaine. Si nous n'avons jamais complètement abandonné ces savoir-faire, notamment en soutien aux opérations contre les engins explosifs improvisés (IED), une part des moyens utilisés par le passé s'est érodée avec le recentrage sur des théâtres de basse intensité.

Dès lors, deux questions se posent. Depuis la fin de la guerre froide, dans quel domaine avons-nous le plus perdu de substances capacitaires ? Aujourd'hui, quelles sont les priorités absolues pour recouvrer et assurer une véritable supériorité dans le domaine électromagnétique ?

**M. Thierry Tesson, rapporteur.** Comme nous l'avons indiqué dans notre propos liminaire, nous avons aujourd'hui le sentiment que certaines composantes de nos forces armées demeurent à un niveau d'excellence, en particulier dans tout ce qui relève de la dissuasion. En revanche, d'autres secteurs apparaissent affaiblis, non par négligence, mais parce que les conflits asymétriques de ces dernières décennies ont conduit nos armées à concentrer leurs efforts ailleurs.

Cependant, trois besoins majeurs se retrouvent aujourd'hui dans toutes les armées : une remontée en puissance offensive indispensable, un renforcement du renseignement d'origine électromagnétique, et une modernisation des outils.

S'agissant de l'armée de Terre, il est évident qu'il faut réinvestir le champ offensif et rapprocher les moyens de guerre électronique des forces de mêlée. L'expérience ukrainienne l'illustre : les soldats utilisent eux-mêmes des équipements de brouillage et de détection. La modernisation des matériels vieillissants est nécessaire, tout comme le développement d'une véritable « guerre électronique du combattant », rendue plus accessible par l'innovation rapide.

Pour la Marine, la question des frégates et de l'installation de brouilleurs antimissiles constitue un enjeu majeur. Pour l'armée de l'air et de l'espace, il s'agit de retrouver une capacité complète de maîtrise de l'espace électromagnétique, du sol jusqu'aux couches les plus hautes, en définissant notamment des zones de déni d'accès capables de neutraliser drones et vecteurs adverses, comme l'ont montré

l'opération américaine au Venezuela ou l'opération Toile d'araignée des forces ukrainiennes.

Enfin, le spatial devient un champ essentiel. Le brouillage y apparaît particulièrement adapté, car non cinétique, et donc mieux ajusté aux enjeux spécifiques de ce milieu.

**M. Didier Lemaire, rapporteur.** Nos travaux nous ont effectivement permis de mesurer les nécessités pour la Marine, l'armée de Terre, l'armée de l'Air et de l'espace. Lors de nos débats sur l'actualisation de la LPM, il nous appartiendra de cibler plus clairement et plus explicitement les besoins des différentes forces armées.

**M. Arnaud Saint-Martin (LFI-NFP).** La guerre électronique est devenue un pilier structurant des conflits actuels. Si le rapport que vous présentez n'inclut pas de recommandations explicites, il est *a priori* utile de disposer d'un état des lieux à l'usage des parlementaires.

Dans la large gamme de capacités et de besoins pris dans le *continuum* multi-champs, multi-milieux de la guerre électronique, je me concentrerai sans surprise sur le milieu exo-atmosphérique théâtre d'une nouvelle frontière de la conflictualité, comme vous l'avez justement suggéré. Le rapport dresse le constat d'une augmentation du brouillage de la géolocalisation et navigation par un système de satellites (GNSS) en Ukraine ; mais également de l'avance dont disposent en la matière la Russie, la Chine et les États-Unis, surtout à travers le système Starshield. En matière de brouillage, de lasers leurrants ou de capacités cinétiques, nous sommes, malheureusement, en retard et sous-dimensionnés.

C'est pourquoi le développement soutenu de satellites et de capacités au sol dédiés à la guerre électronique est de plus en plus critique, de même que la mise au point des moyens permettant de les neutraliser, qu'il faut posséder également. Cependant, la surenchère capacitaire paraît inexorable, ce qui est en soi problématique.

Dans cette perspective, sommes-nous parvenus à un stade de spatialisation de la guerre électronique ? Le cas échéant, la France y consacre-t-elle suffisamment de moyens ? Si tel n'est pas le cas, quelle priorité faut-il fixer dans le cadre de l'actualisation prochaine de la LPM dont vous avez convenu qu'elle se référait peu à la guerre électronique ?

Par ailleurs, si nous nous projetons dans un conflit de haute intensité où le guidage satellitaire est systématiquement brouillé, comme en Ukraine, quelles conséquences opérationnelles et doctrinales la France devrait-elle en tirer ? De quelles capacités dispose-t-on pour neutraliser les satellites adverses en dehors des solutions aussi potentiellement ravageuses pour le trafic orbital que les missiles antisatellites ? Qu'en est-il des satellites de renseignement d'origine

électromagnétique, le système Ceres et son potentiel successeur Celeste, qui doit le remplacer à horizon 2030 ? Sont-ils suffisants pour répondre aux besoins de renseignement d'origine électromagnétique qui pourraient évoluer d'ici à 2030 et au-delà ? Les possibles consolidations parmi les industriels impliqués à travers le projet Bromo rebattent-elles les cartes ? Comment également combiner la défense de nos capacités en orbite et la stratégie encore à approfondir de la très haute altitude ?

Ensuite, avez-vous évoqué lors de vos auditions les enjeux liés à la dissuasion spatiale – dont la guerre électronique orbitale fait partie – sur lesquels la Russie, la Chine et les États-Unis sont bien plus avancés que la France ? Recommanderiez-vous d'investir dans le domaine de la défense spatiale hyperactive pour se prémunir d'adversaires malintentionnés qui visent à désorganiser les communications et les infrastructures de pays entiers depuis l'espace ?

**M. Thierry Tesson, rapporteur.** Il apparaît désormais clairement que l'espace n'est plus un sanctuaire. Le traité de 1967, qui encadre encore aujourd'hui l'usage de l'espace extra-atmosphérique, révèle ses limites. Sans être diplomates, nous voyons bien qu'il faudra tôt ou tard s'y intéresser de manière approfondie. Cet angle mort offre à certaines puissances la possibilité d'agir sans contrainte : elles affirment sans détour qu'en l'absence de règles, elles se considèrent libres de tout faire.

Les menaces sont identifiées : tirs antisatellites russes, brouillages chinois intentionnels, manœuvres d'espionnage. Le brouillage GPS en est l'illustration la plus immédiate. En Ukraine, les signaux sont si perturbés que la géolocalisation devient parfois impossible. Au cœur de Kiev, certains appareils indiquent par exemple une position située à plus de 200 kilomètres. La situation est similaire en Israël, où le GPS se dégrade fortement en zone sensible.

Lors des auditions que nous avons menées, les forces armées françaises ont manifesté une conscience très nette de ces enjeux. Le remplacement du système Ceres par le programme Celeste illustre cette nécessité d'adaptation. Au plus haut niveau de décision, la priorité est désormais reconnue : il faut aller vite, renforcer nos capacités et clarifier les bases d'une véritable dissuasion spatiale. Ces évolutions requièrent encore un effort doctrinal.

**M. Didier Lemaire, rapporteur.** Nos auditions ont confirmé que la priorité porte sur la reconquête de la capacité de suppression des défenses aériennes ennemies, qui nous permet de garantir l'entrée en premier et la crédibilité de la dissuasion. Enfin, l'espace et la très haute altitude, deviennent effectivement de nouveaux champs de confrontation.

**M. Guillaume Garot (SOC).** Je remercie à mon tour les deux rapporteurs pour la qualité et l'exhaustivité de leur travail. En premier lieu, je tiens à formuler une demande générale qui s'adresse à l'ensemble de la commission. Les prochains

rapports, notamment ceux des missions d'information, pourraient-ils faire l'objet d'une synthèse, et en particulier d'une présentation des propositions ?

Pour en revenir à votre rapport, vous listez les nombreuses initiatives en cours dans nos armées, et plus largement au sein de la base industrielle et technologique de défense, pour monter en gamme et en masse dans le domaine des capacités de guerre électronique. À l'horizon 2030, serons-nous prêts à mener ce volet de guerre électronique dans le cadre d'un conflit à haute intensité ?

Ensuite, établissez-vous un lien entre l'exigence de se prémunir d'attaques électroniques et nos capacités à accueillir des blessés dans le cadre d'un conflit de haute intensité ? Ce sujet est particulièrement sensible en Ukraine aujourd'hui, où les blessés ne peuvent plus être pris en charge de façon optimale.

**M. Thierry Tesson, rapporteur.** Lors de nos auditions, nous avons entendu parler de systèmes de drones sur roues capables de rechercher et transporter des blessés sur le champ de bataille. Sur le théâtre de guerre ukrainien, la guerre électronique est partout, la surveillance constante. Toute sortie non protégée et prolongée accroît les risques. À ce titre, le retrait des blessés du champ de bataille pour pouvoir leur prodiguer des soins constitue un aspect extrêmement critique de ce type de combat. Nous formulons le souhait que notre rapport puisse contribuer efficacement à une remontée en puissance budgétaire, afin d'augmenter nos capacités dans ce domaine.

**M. Didier Lemaire, rapporteur.** Je partage ces derniers propos. Nous espérons que ce rapport puisse être utile à la réflexion. Nos forces armées sont conscientes des enjeux et s'efforcent d'être préparées de manière permanente et professionnelle. Il nous revient, à nous parlementaires, de prendre conscience des enjeux, de manière collective. Le pire serait de ne pas être prêts.

**M. Jean-Louis Thiériot (DR).** Je vous remercie pour cet exposé très pédagogique sur une matière qu'il n'est pas aisé de maîtriser.

Tout d'abord, vous avez soulevé une analyse très juste, qui repose sur la nécessité de raisonner en logique de flux et non en logique de stock. Vous évoquiez ainsi le cycle d'un à deux mois pour le *software,* et de quatre à six mois pour le *hardware*. Il n'y aurait aucun sens de disposer de stocks de matériel qui seraient immédiatement périmés dans le cas d'un conflit de haute intensité.

Quelle adaptation de notre stratégie industrielle envisagez-vous, puisque l'enjeu essentiel a trait à la remontée en puissance dans ce domaine ? À ce titre, il apparaît impérieux de disposer de stocks d'un certain nombre de composants, de matériaux critiques absolument nécessaires. Quelle stratégie faut-il établir et comment la piloter pour être en mesure d'assurer cette remontée en puissance ?

Ensuite, vous évoquiez l'actualisation de la LPM, sur laquelle nous allons devoir travailler. À quel niveau évaluez-vous le surinvestissement que nous devrions réaliser pour être à la hauteur ? Je veux notamment revenir sur le sujet de la neutralisation des défenses aériennes adverses (Sead), à l'heure où les missiles Martel n'existent plus. MBDA a lancé un programme Stratus dans ce domaine, mais ne faudrait-il pas accélérer la cadence ?

Enfin, ma dernière question concerne l'organisation. Vous parlez de la nécessité probable de dédoubler les régiments, *a minima* d'en dédoubler un. Pensez-vous que les capacités de guerre électronique doivent rester, au niveau régimentaire, rattachées à une division, à un corps d'armée ou à une brigade ? Faut-il plutôt envisager des compagnies dédiées venant des régiments de transmission dans les différentes unités engagées au contact ?

**M. Thierry Tesson, rapporteur.** Nous sommes confrontés à une difficulté majeure, commune à de nombreux domaines militaires : dès lors que l'on acquiert des équipements, ils risquent d'être dépassés quelques mois plus tard. Ce décalage permanent crée une forme d'équilibre instable qu'il faut sans cesse ajuster et qui demeure extrêmement difficile à maîtriser. Les échelles d'investissement sont multiples, la course technologique est permanente.

Au fil de nos auditions, nous avons échangé avec de nombreuses entreprises ainsi qu'un grand nombre de PME particulièrement innovantes, dont la vitalité est frappante. Elles témoignent de la capacité de l'industrie française à proposer des solutions de pointe. Certaines, comme MC2 Technologies à Villeneuve-d'Ascq, témoignent d'une agilité remarquable. La question qui se pose alors concerne la manière dont la DGA et les grands groupes de notre BITD – Thales, Safran, Dassault – articulent leur action avec ces PME.

S'agissant des investissements, davantage sera forcément nécessaire. Il est difficile de parler en milliards, mais l'essentiel consiste à faire en sorte que la LPM consacre une place claire, identifiée et consolidée à la guerre électronique, avec un financement associé.

Cela nous conduit à la question d'une éventuelle armée dédiée. L'exemple russe est connu : leur armée dispose d'une branche entièrement consacrée à la guerre électronique. Nous avons posé cette question à nos chefs d'état-major. Tous se sont montrés réservés, ce qui peut se comprendre, dans la mesure où notre culture opérationnelle diffère de celle des forces russes. De plus, l'empilement de structures n'est pas toujours un gage d'efficacité. En revanche, la nécessité d'une meilleure identification de cette capacité fait consensus : il faut rendre cette fonction plus visible et plus cohérente dans l'organisation du combat, dans la BITD, dans les investissements, comme dans la doctrine.

**M. Didier Lemaire, rapporteur.** Nos visites aux 54e et au 44e régiments nous ont permis de mesurer leur expertise tactique. Il est nécessaire de leur attribuer des moyens de transformation, et regagner le terrain perdu depuis la fin de la guerre froide.

**M. le président Jean-Michel Jacques.** Je me permets de vous soumettre une réflexion concernant les boucles technologiques rapides. Naturellement, il convient de veiller aux achats de nouveautés dont l'obsolescence s'accélère compte tenu des innovations. Cependant, cela ne doit pas devenir une excuse pour ne rien acheter sous prétexte que les évolutions sont trop rapides. Nos armées ont besoin d'équipements renouvelés. Lors de l'actualisation de la LPM, nous veillerons à faire en sorte que chaque régiment puisse obtenir un minimum de ces objets innovants, même s'ils seront sans doute technologiquement dépassés demain. L'ingéniosité de nos techniciens et de leurs *labs* dans les régiments n'est plus à prouver, ils savent comment « customiser », apporter des spécifications décisives à ces matériels, pour améliorer leur opérationnalité.

**Mme Josy Poueyto (Dem).** Au nom du groupe Les Démocrates, je vous remercie pour cet excellent travail, qui nous permet de disposer d'une vision claire des enjeux liés à la guerre électronique, notion particulièrement complexe, tant elle doit s'adapter aux besoins des différents corps d'armée ou aux évolutions technologiques exponentielles.

Vous nous présentez la combinaison des éléments susceptibles de caractériser une forme de supériorité informationnelle. Il s'agit de mieux appréhender l'environnement des adversaires, mais aussi d'obtenir une meilleure connaissance de nos propres forces et celles de nos alliés. Un autre enjeu concerne la capacité à comprendre, à communiquer, à agir à un moment où les univers électroniques et électromagnétiques rejoignent le cyber ; à un moment où l'activité militaire et l'activité civile semblent parfois se chevaucher.

Cette dimension, qui mêle activités civiles et militaires, m'interroge. Je pense d'abord à l'espace, devenu un milieu stratégique sans frontières, mais où s'expriment de nouvelles menaces. En la matière, le cadre juridique est insuffisant, puisqu'il repose sur un traité international de 1967. À l'évidence, il est urgent de l'adapter. Où en est ce chantier ?

Ensuite, alors que l'analogique laisse presque toute sa place au numérique, je me demande comment nos entreprises et nos services publics fonctionneraient en cas d'attaque ou de panne générale des systèmes. Quelles sont les alternatives ? Allons-nous regretter le démantèlement en cours du réseau cuivre, par exemple ? Enfin, le dernier colombier militaire de France et ses 200 pigeons voyageurs restent-ils d'actualité ?

**M. Thierry Tesson, rapporteur.** Certains spécialistes font valoir qu'en 1940, la France n'avait pas suffisamment utilisé les pigeons voyageurs.

Au-delà, il est nécessaire que notre doctrine éclaire les situations où la France ferait face à un brouillage massif et généralisé. Il faut se durcir et trouver la possibilité de mettre en place des moyens alternatifs. C'est ainsi que les Ukrainiens se sont adaptés en utilisant des drones filaires, face à un environnement extrêmement dégradé par les brouillages. Enfin, la révision du traité de 1967 constitue effectivement un enjeu majeur. Il m'apparaît nécessaire de progresser dans cette voie, mais cet aspect n'a pas été traité dans le cadre de notre rapport.

**M. Didier Lemaire, rapporteur.** Nos armées ont pleinement conscience de l'évolution accélérée des matériaux et des techniques, portée par les conflits actuels où la guerre électronique progresse à vive allure. Elles doivent désormais être capables de répondre, y compris en situation de panne, en conservant des prérogatives plus élémentaires. L'exemple des drones filaires l'illustre.

**M. Matthieu Bloch (UDR).** Je vous remercie pour la qualité de votre rapport sur ce sujet essentiel pour les guerres modernes, comme en témoigne le théâtre ukrainien. Ma question concerne notre BITD et la souveraineté. Or 80 % des composants électroniques et microprocesseurs présents dans nos systèmes de brouillage ou nos systèmes de protection viennent de Chine. Avez-vous pu étudier la capacité de notre BITD à absorber un conflit de haute intensité et à remplacer des matériels de brouillage pour nos armées ?

**M. Thierry Tesson, rapporteur.** Nous avons effectivement abordé ces sujets. Je pense notamment à la question des fonderies et la capacité, pour la France, à produire ses propres puces. L'idée est séduisante, mais elle suppose des investissements colossaux, difficilement soutenables pour répondre aux besoins de notre BITD. De fait, notre dépendance à des systèmes étrangers demeure.

Les restrictions liées aux normes américaines ITAR compliquent également l'usage de certains matériels, tandis que de nombreux composants proviennent d'Italie ou des États-Unis. Certes, des accords industriels existent et nous protègent partiellement, mais la dépendance est réelle et ne doit pas être occultée. Elle touche aussi les matières premières critiques, comme plusieurs auditions nous l'ont rappelé. Enfin, notre chaîne de production nationale, depuis les premières étapes de fabrication jusqu'aux dernières, révèle encore des fragilités. La maîtrise complète de cette filière constitue donc un enjeu stratégique majeur.

**M. Didier Lemaire, rapporteur.** La sécurisation de la chaîne de valeur est effectivement essentielle pour assurer notre souveraineté. Nous évoquions les composants, qui peuvent être chinois comme américains. À ce sujet, nous devons absolument pouvoir garantir une filière 100 % française, notamment pour sécuriser un enjeu clef, que nous n'avons pas encore abordé. Je pense ici aux bibliothèques de

la guerre électronique, ces références qui doivent impérativement être maîtrisées de bout en bout par notre pays, si nous voulons demeurer souverains.

**M. le président Jean-Michel Jacques.** Nous passons maintenant à une séquence de quatre questions individuelles complémentaires, en commençant par une première série de deux questions.

**M. Antoine Valentin (UDR).** Ma question porte sur la protection des bases militaires face à la menace drone. L'opération ukrainienne Toile d'araignée a démontré que les drones pouvaient désormais frapper des emprises stratégiques à plusieurs milliers de kilomètres du front. Je rappelle qu'en France, nous avons connu plusieurs survols de sites sensibles, notamment liés à notre dissuasion.

Or la protection de nos bases est cruciale. Notre modèle d'armée repose sur un nombre limité d'équipements à très haute valeur ajoutée. La neutralisation d'une dizaine de Rafale ou d'un ravitailleur entraînerait ainsi des conséquences disproportionnées. Or, la lutte anti-drones ne peut reposer uniquement sur des moyens cinétiques. Elle suppose une défense multi-couches intégrant pleinement la guerre électronique.

Estimez-vous que le niveau actuel de protection électromagnétique de nos bases soit à la hauteur ? Quelles mesures convient-il de prendre pour éviter un scénario comparable à celui rencontré en Ukraine ?

**Mme Florence Goulet (RN).** La guerre électronique constitue désormais un pilier des conflits de haute intensité et impose une remontée en puissance rapide de nos capacités. Pourtant, à la lecture de vos travaux, il apparaît clairement que la ressource humaine constitue aujourd'hui l'un des principaux points de fragilité. Les unités spécialisées ne parviennent pas à atteindre leurs effectifs théoriques, alors même que les besoins augmentent.

Cette tension est d'autant plus préoccupante que la formation est longue et exigeante. Il faut par exemple près de six années pour former un programmeur de bibliothèque de guerre électronique sur Rafale. À cette contrainte s'ajoute un enjeu majeur de fidélisation : les profils formés sont rares, hautement qualifiés et fortement concurrencés, notamment par le secteur cyber et par l'industrie.

Chaque départ représente donc une perte capacitaire significative, difficilement compensable à court terme. Dans ce contexte, quelles mesures concrètes préconisez-vous pour renforcer le recrutement, raccourcir ou optimiser les parcours de formation et surtout fidéliser durablement ces compétences critiques au sein des armées ?

**M. Thierry Tesson, rapporteur.** Vous nous avez interrogés sur la protection de nos bases, devenue un enjeu central. De fait, l'opération Toile d'araignée menée par l'Ukraine en juin 2025 a clairement démontré qu'il était

désormais possible de projeter des drones en profondeur sur un territoire ennemi, même si les dommages réels restent mal documentés. Ce simple fait nous renvoie immédiatement aux vulnérabilités de nos propres implantations militaires. La protection de ces bases ne peut plus être considérée comme un paramètre secondaire : elle constitue, au contraire, une priorité stratégique absolue.

La réponse ne peut évidemment pas être uniquement cinétique. On ne peut plus se contenter de tirer sur un drone lorsqu'il apparaît. La défense doit être multicouches, articulant une surveillance permanente, une détection fiable, une identification rapide et, lorsque c'est possible, une neutralisation des liaisons radio ou GPS. Le leurrage et la perturbation des vecteurs hostiles doivent également être intégrés. L'opération Toile d'araignée l'a montré : si l'ennemi parvient à détruire certains de nos aéronefs, l'ensemble de notre dispositif peut vaciller.

Vient ensuite la question des ressources humaines, sujet que j'ai examiné avec une attention particulière. Nous avons entendu à maintes reprises qu'il existe en France une fragilité croissante dans les formations scientifiques, notamment en mathématiques. Certes, nous disposons de chercheurs de très haut niveau, mais la base se rétracte, ce qui pose un problème majeur à moyen terme.

Les enjeux de formation sont également patents. Nous avons par exemple rencontré des industriels qui nous ont confié ne plus trouver d'ingénieurs radio, cette spécialité ayant quasiment disparu au profit de formations centrées exclusivement sur le numérique.

Enfin, le maintien dans les armées des compétences les plus pointues constitue un défi considérable. En Alsace, nous avons rencontré des caporaux-chefs disposant d'une expertise technique largement supérieure à celle des officiers qui les commandaient. Leur fidélisation doit devenir une priorité. Nous proposons donc d'envisager un système de primes spécifique, afin d'éviter leur départ vers le secteur privé, où les rémunérations sont bien supérieures. Mais il faut aller plus loin : il serait souhaitable d'examiner la possibilité de leur offrir un statut mieux reconnu dans la chaîne hiérarchique, à la hauteur de leurs compétences.

**M. Didier Lemaire, rapporteur.** Je partage entièrement les propos de mon corapporteur, notamment concernant la protection des bases et le défi des ressources humaines. Nos échanges ont permis de souligner un manque d'experts, d'autant plus que les formations sont particulièrement longues, à l'image de l'exemple que vous avez mentionné, ces six années pour former un programmeur de bibliothèque de guerre électronique sur Rafale.

À ce titre, nous proposons de créer un BTS « guerre électronique » associé à une prime de compétences, dans la mesure où nos armées souffrent aussi de la concurrence du secteur privé. La rémunération des spécialistes de nos armées constitue un point de vigilance très important de notre rapport, concernant le volet des ressources humaines.

**M. Thibault Monnier (RN).** Ma question porte sur un enjeu de souveraineté qui me paraît particulièrement préoccupant : la préparation opérationnelle en guerre électronique. À la lecture de votre rapport, il apparaît que le cadre juridique actuel reste très contraignant. Les règles applicables en temps de paix limitent fortement les entraînements, soumis à des autorisations longues à obtenir. Cela réduit la possibilité de s'entraîner en conditions réelles.

Or, sans entraînement, il est illusoire d'espérer retrouver des savoir-faire délaissés depuis la fin de la guerre froide. Plus préoccupant encore, les industriels rencontrent des obstacles similaires, voire supérieurs, pour tester leurs équipements. Faute de souplesse réglementaire, certains sont contraints d'effectuer leurs essais à l'étranger.

Dans un domaine aussi sensible que la guerre électronique, cette externalisation comporte un risque évident en matière de protection du secret. Dès lors, quelles évolutions recommandez-vous pour concilier sécurité des usages civils, souveraineté technologique et préparation opérationnelle crédible en guerre électronique sur le territoire national ?

**M. Jean-Louis Thiériot (DR).** Ma question est davantage d'ordre stratégique que tactique et opérationnel. Avez-vous été conduits à travailler sur les conséquences de bombes nucléaires à effet d'impulsion électromagnétique (IEM) ? En effet, certains de nos compétiteurs stratégiques disposent de stratégies d'emploi du nucléaire, quand la France s'inscrit dans une doctrine de dissuasion très claire. Quels effets pourraient-elles engendrer ?

**M. Thierry Tesson, rapporteur.** Le cadre juridique dans lequel nous évoluons découle du fait que la France n'est pas en guerre. Ce que nous observons en Ukraine relève, lui, du réel le plus concret, où chaque action est testée, affrontée, éprouvée. Sur notre territoire, heureusement en paix, les exercices demeurent strictement encadrés par des règles qui limitent nécessairement l'emploi de la guerre électronique et rendent son expérimentation plus complexe.

Parmi les pistes évoquées, la création de zones d'expérimentation permanentes et sécurisées pourrait offrir un espace de manœuvre. Une évolution de l'arsenal légal, visant à simplifier certaines procédures sous pilotage interministériel, mériterait d'être étudiée. Le cadre réglementaire pourrait également être revu, même si chacun comprend qu'un brouillage massif risquerait d'affecter le trafic aérien civil et d'entraîner des conséquences graves. C'est précisément pour éviter ces risques que les restrictions actuelles existent. Une modernisation d'un véritable polygone dédié à la guerre électronique pourrait être envisagée.

Quant à la dissuasion, elle a bien été abordée dans nos travaux, mais sa grande sensibilité explique la – légitime – grande réserve de nos interlocuteurs.

**M. Didier Lemaire, rapporteur.** Notre rapport constitue une base de travail, une amorce, qu'il convient d'approfondir en étant conscients que ces enjeux sont particulièrement sensibles. Des modifications réglementaires s'avèrent également essentielles pour permettre à nos armées de pouvoir s'entraîner, aux entreprises privées et publiques de mettre en œuvre leurs capacités et de les tester. En matière aérienne, un travail interministériel s'impose.

*Conformément à l'article 145 du Règlement de l'Assemblée nationale, à l'issue des échanges, la commission* ***autorise*** *la publication du rapport d'information qui lui a été présenté.*

**M. Thierry Tesson, rapporteur.** Je vous remercie pour votre consensus, qui témoigne de notre soutien commun à nos forces armées.

**M. Didier Lemaire, rapporteur.** Je me joins à ces remerciements, tant il est vrai que ces enjeux sont essentiels. Nos forces armées attendent notre action, mais également les Françaises et les Français, afin que notre pays soit protégé.

**M. le président Jean-Michel Jacques.** Je vous remercie.

# ANNEXE I : AUDITIONS ET DÉPLACEMENTS DES RAPPORTEURS

*(Par ordre chronologique)*

## 1. Auditions

• **Fondation pour la recherche stratégique - M. Philippe Gros**, maître de recherche ;

• **Agence nationale des fréquences - M. Gilles Brégant**, directeur général de l'ANFR, **M. Christophe Digne**, directeur général adjoint de l'ANFR, **Mme Corinne Le Ny-Gigon**, cheffe du service communication et relations institutionnelles ;

• **ONERA - M. Jacques Lafaye**, conseiller du président Sainjon, président-directeur général de l'ONERA**, M. Philippe Dreuillet**, directeur du département Électromagnétisme et Radar de l'ONERA ;

• **M. Alain Lardet**, sous-chef plans-programmes de l'armée de Terre ;

• **M. le général de corps d'armée Aymeric Bonnemaison**, commandant de la cyberdéfense (COMCYBER) ;

• **Audition commune : M. le Général de division Thierry Naville**, directeur général du numérique (DGNUM) par intérim au ministère des armées, **Général de brigade Alain Musy**, officier général en charge des fréquences du Ministère (OGF) et **Colonel Rodolphe Quemerais,** chef du bureau de la gouvernance des fréquences et des positions orbitales ;

• **Général Chusseau,** sous-chef plans-programmes de l'armée de l'Air et de l'espace ;

• **M. le général de corps d'armée aérienne Philippe Adam**, commandant de l'Espace (CDE) au ministère des armées ;

• **Commandant Anthony Namor**, officier dans l'Armée de Terre ayant servi dans des régiments de transmissions et chercheur associé au CREC de Saint-Cyr Coëtquidan ;

• **Capitaine de Vaisseau Rémi Thomas**, futur sous-chef d'état-major « plans programmes » de la Marine nationale à compter du 1er août 2025 ;

• **M. le général Stéphane Dossé,** co-auteur avec le COMCYBER d'« Attention Cyber : vers le combat cyber-électronique ! » ;

• **Direction générale de l'armement (DGA) - M. Frédéric Bouyer**, directeur de DGA maîtrise de l'information, **M. Christophe Vaucouleur**, sous-

directeur de DGA maîtrise de l'information, et **M Olivier Mary**, architecte de programme de défense aéro-mobilité, surveillance et protection**, Mme Jeanne Mailler ;**

● **SAFRAN - Mme Suzanne Kucharekova**, directrice des affaires institutionnelles de Safran et **M. le général Gilles Perrone**, directeur des relations institutionnelles de Safran Electronics & Defense (SED) ;

● **Table-ronde du GICAT sur le sujet de la guerre électronique :**

**- GICAT - M. Jean-Marc Duquesne**, délégué général du GICAT ; **M. Vincent Quintana**, directeur des affaires publiques France du GICAT ;

**- CERBAIR - M. Lucas Le Bel**, cofondateur et directeur général de Cerbair ;

**- HENSOLDT - M. Jérôme Galle**, *sales director Avionics and EW* de Hensoldt, **Mme Marion Vergès**, *political affairs manager* de Hensoldt

**- INEO DEFENSEM. Yves de Thomasson,** *directeur commercial et marketing d'Ineo Défense et* **M. Arnaud Lecca,** *directeur innovation d'Ineo Défense.*

● **Thales – M. Pascal Bourretère,** vice-président du secteur de guerre électronique des communications ; **M. Martin Defour,** vice-président Technique Thales Systèmes de Mission de Défense ; **M. Thierry Angel**, conseiller Défense (Air) du Groupe Thales ; **Mme Karine Broudeur**, directrice Stratégie Thales Système de Mission de Defense – Business Line ISR (Intelligence Surveillance et Reconnaissance) ; **Mme Isabelle Caputo**, directrice des relations parlementaires et politiques ;

● **M. l'ingénieur général de première classe de l'armement. Pierre Grandclément**, président de l'association GUERRELEC

● **ATDI - M. Philippe Missud,** président de l'ATDI ;

● **EVIDEN - M. Pierre-Yves Jolivet**, Directeur-Général de l'EVIDEN ;

● **ICA Frédéric Bal,** attaché d'armement en Ukraine ;

●**M. le général de brigade Jérôme Mallard,** attaché de défense près de l'Ambassade de France en Russie

● **M. le général de division aérienne Patrice Morand**, attaché de défense de la France près de l'ambassade de France **aux États-Unis ;**

2. **Déplacement en Alsace - BRCE, 54e RT et 44e régiments de transmissions (15 septembre 2025)**

3. **Déplacement à Mont-de-Marsan (AAE) (25 septembre 2025)**

4. **Déplacement à Brest (Marine) (3 octobre 2025)**

5. **Déplacement chez MC2 technologies (Lille) (24 novembre 2025)**

6. **Déplacement chez Cerbair (Montrouge) (4 décembre 2025)**