NOTE n°1

MAI 2018

Note n° 357/Consortium CONFLITS-2035
du 18 mai 2018

Marché n° 2017 1050 162 263
EJ court 180 004 69 93
notifié le 17 janvier 2018
réunion de lancement : 13 février 2018

Les opérations en environnement électromagnétique dégradé

PHILIPPE GROS

En partenariat avec

SOMMAIRE

LISTE DES ABREVIATIONS 5

RESUME 6

INTRODUCTION 7

MENACES, CONTRAINTES ET EVOLUTIONS TECHNIQUES DANS LE DOMAINE ELECTROMAGNETIQUE 9

1. UN ENVIRONNEMENT TECHNOLOGIQUE EN MUTATION RAPIDE 9

1.1 Rappel de quelques bases de l'attaque électronique 9

1.1.1 Les catégories basiques de CME 9

1.1.2 L'attaque des radars 9

1.1.3 L'attaque des télécommunications 9

1.1.4 L'attaque des services de navigation par satellite (GNSS) 10

1.2 Les risques permanents et accrus d'interférences 11

1.3 Des opérations dans le domaine EM en pleine mutation technique 12

1.3.1 Des mutations déjà à l'œuvre 12

1.3.2 L'émergence du « combat cyber-électronique » 13

1.3.3 Quelques ruptures technologiques accentuant ces évolutions à court terme… 13

1.3.4 …avant la révolution quantique à plus long terme… 14

2. LA GUERRE ELECTRONIQUE, UNE DES PIERRES ANGULAIRES DES CAPACITES D'INTERDICTION RUSSES ET CHINOISES 14

2.1 Radioelektronnaya bor'ba 14

2.1.1 La doctrine 15

2.1.2 L'organisation 15

2.1.3 Les équipements 16

2.1.4 L'entraînement et les retours d'expérience 17

2.2 Un modèle chinois résolument tourné vers la guerre cyber-électronique 17

3. UNE PROLIFERATION ENCORE LIMITEE MAIS QUI DEVRAIT LOGIQUEMENT SE RENFORCER 18

3.1 Une prolifération encore assez réduite 18

3.1.1 Quelques capacités affichées 18

3.1.2 Des prévisions anticipant une croissance limitée du marché 19

3.2 Plusieurs facteurs crédibilisent un renforcement de la menace 19
3.2.1 Un « effet Krasukha » analogue à « l'effet Predator » ? 19
3.2.2 Des configurations stratégiques et des capacités non-traditionnelles qui augmentent le risque 19
3.2.3 Conclusion : vers un étalement du spectre capacitaire 20

VULNERABILITES POTENTIELLES DE NOS SYSTEMES DE FORCE ET IMPLICATIONS CAPACITAIRES 21

1. CARACTERISATION DE LA PROBLEMATIQUE DE LA DEGRADATION DE L'ENVIRONNEMENT ELECTROMAGNETIQUE POUR NOS FORCES 21
1.1 Le niveau interarmées 21
1.1.1 Les communications 21
1.1.2 WLAN des bases et équipements des personnels 22
1.2 Les forces terrestres 22
1.2.1 Les réseaux de communications 22
1.2.1.1 Le réseau de théâtre 22
1.2.1.2 Les réseaux de capillarité 22
1.2.2 Les capteurs 23
1.2.3 Navigation et positionnement 23
1.2.4 Conclusions 23
1.3 La composante aérienne 23
1.3.1 Les communications 23
1.3.2 Les capteurs 24
1.3.3 Navigation et positionnement 24
1.3.4 Conclusions 24
1.4 La composante navale 24
1.4.1 Les communications 24
1.4.2 Les capteurs 25
1.4.3 Navigation et positionnement 25
1.4.4 Conclusions 25
1.5 Le cas des opérations spéciales 25

2. LES IMPLICATIONS CAPACITAIRES DORESE 26
2.1 Doctrine 26
2.2 Organisation 27
2.3 Recrutement 27
2.4 Équipements 27
2.5 Soutien 27

2.6 Entraînement 27

ANNEXE 1
LE SPECTRE ÉLECTROMAGNETIQUE 29

ANNEXE 2
SYSTÈMES DE GUERRE ÉLECTRONIQUE DES FORCES RUSSES 30

ANNEXE 3
LA REMISE À PLAT DE L'ARCHITECTURE DE TRANSMISSION DE L'US ARMY .. 31

ANNEXE 4
AXES DE RECHERCHE AMÉRICAINS SUR LA RÉSILIENCE DU PNT..... 32

ANNEXE 5
LES KNOWLEDGE MAP 34

RÉFÉRENCES 38

Liste des abréviations

APL	Armée populaire de libération
BFT	*Blue Force Tracking*
CME	Contre-mesures électroniques
CNE	*Computer Network Exploitation*
CNO	*Computer Network Operations*
COMINT	*Communications intelligence*
COMSATCOM	*Commercial Satellite Communications*
CUGE	*Charge utile de guerre électronique*
DORESE	*Doctrine, organisation, recrutement, équipement, soutien, entraînement*
EHF	*Extreme High Frequency*
EM	électromagnétique
EMCON	*Emission control*
EME	*Electromagnetic Environment*
EMSO	*Electromagnetic Spectrum Operations*
FO	Forme d'onde
GE	Guerre électronique
GNSS	*Global Navigation Satellite System*
GPS	*Global Positioning System*
GSM	*Global System for Mobile*
HF	*High Frequency*
INS	*Inertial Navigation System*
ISR	*Intelligence, surveillance, reconnaissance*
LDT	Liaison de données tactique
MILSATCOM	*Military Satellite Communications*
MPE	Mesures de protection électronique
MSE	Mesures de soutien électronique
PNT	Positionnement, navigation, timing
RDIFF	*Réseau de diffusion*
REB	*Radioelektronnaya bor'ba*
REMO	Réseau de mobiles
ROEM	Renseignement d'origine électromagnétique
RTRAN	Réseau de transit
SATCOM	*Satellite communications*
SHF	*Super High Frequency*
SIA	Système d'information des armées
SICS	Système d'information du combat SCORPION
SIGINT	*Signals Intelligence*
SWAP	*Size, Weight and Power*
UHF	*Ultra-High Frequency*
VHF	*Very High Frequency*
VLF	*Very Low Frequency*
WLAN	*Wireless Local Area Network*

Résumé

Les opérations dans le spectre électromagnétique, c'est-à-dire l'exploitation de ce spectre à des fins de télécommunications, de télédétection et de positionnement, navigation et timing (PNT), la guerre électronique et le renseignement d'origine électromagnétique, représentent le substrat de toutes les fonctions opérationnelles de notre système de force. Ces opérations sont transformées par des mutations technologiques rapides, particulièrement la numérisation. Elles se traduisent par des équipements « *software-defined* » permettant des opérations plus flexibles, l'émergence du « combat cyber-électronique » – laquelle ne va pas sans poser de sérieux défis cependant – et de la guerre électronique « non traditionnelle ». De nouvelles technologies comme l'Internet des objets ou à plus long terme les technologies quantiques, révolutionneront plus encore ces opérations, présentant des défis comme des opportunités.

Dans ce contexte, les forces occidentales font face à un étalement du spectre des menaces. En l'état, la Chine et la Russie sont les seules puissances au seuil du combat cyber-électronique et disposant d'un arsenal complet de moyens en mesure d'affecter le spectre électromagnétique dans l'ensemble des milieux, y compris spatial. Les capacités de la plupart des autres acteurs restent, au mieux, lacunaires : moyens rudimentaires de brouillage GPS ou des SATCOM, systèmes d'autoprotection, etc. Cependant, plusieurs facteurs sont susceptibles de renforcer cette menace. La guerre électronique est en effet un moyen idoine pour contrer les capacités de reconnaissance-frappe qui se développent et/ou pour exécuter des stratégies « ambiguës ». Les moyens, même limités, de guerre cyber-électronique non-traditionnelle pourraient proliférer y compris entre les mains d'un plus grand nombre d'acteurs étatiques comme non-étatiques.

Dans ce contexte, à court-moyen terme, l'interdiction de capacités comme les SATCOM semble devoir rester l'apanage des principales puissances. En revanche, les réseaux locaux mis en œuvre sur les bases de nos armées de même que les équipements individuels peuvent présenter des vulnérabilités plus étendues.

Les forces terrestres sont plus spécifiquement confrontées à la densification des capacités d'attaque électronique contre les échelons tactiques les plus bas, susceptibles d'entraver la conduite de la manœuvre au contact et de ses appuis. Certes, nos forces sont théoriquement en mesure de neutraliser cette menace mais sont contraintes par le volume compté, voire « échantillonnaire », de nos capacités et le nombre de missions qui leur seraient imparties. En outre, la congestion du spectre EM, notamment en zone urbaine, affecterait en premier lieu les forces terrestres. Notre composante aérienne fait surtout face au modèle russe et à sa prolifération éventuelle, consistant à intégrer une GE à longue portée dans la bulle d'interdiction aérienne adverse, susceptible d'entraver nos capacités ISR et de frappes de précision dans la profondeur. La dégradation de l'environnement EM naval semble elle se poser selon deux problématiques. La première est celle du combat naval hauturier et concerne le haut du spectre face aux plus grandes puissances, les seules à disposer des capacités aériennes et navales nécessaires. La seconde est celle des opérations en zone littorale, notamment des opérations amphibies. Nos forces navales pourraient y faire face, non seulement à l'ensemble des menaces de GE contre leurs moyens de transmission et de télédétection, mais également, elles-aussi, à la congestion du spectre EM.

Les recommandations, déclinées dans le spectre capacitaire DORESE, se structurent autour de quelques axes clés : la résilience de nos capacités, combinant des mesures visant à améliorer ou, au contraire, à réduire l'exploitation du spectre EM ; le développement des capacités de lutte contre les menaces d'attaque électronique et de combat cyber-électronique ; enfin le développement des méthodes et outils permettant une gestion du spectre plus dynamique.

Introduction

Les forces armées ont exploité les ondes électromagnétiques dès leur maîtrise par l'Homme à la fin du XIXème siècle (première liaison de Télégraphie Sans Fil transmanche effectuée par Guglielmo Marconi en 1899)[1]. Un siècle plus tard, l'environnement électromagnétique (EME)[2] est devenu, au moins *de facto*, un domaine de lutte à part entière.

Selon le corpus doctrinal français[3], les opérations dans cet environnement relèvent de trois domaines. **Le premier est celui de « l'exploitation du spectre** » (voir annexe 1 pour une frise du spectre EM). Cette exploitation se traduit par plusieurs capacités devenues des **« *enablers* » de toutes les fonctions opérationnelles** (commandement, renseignement, effecteurs, soutien, etc.) d'une force militaire :

- **les capacités de télécommunications** par voie hertzienne. Elles exploitent des bandes de fréquences de plus en plus élevées pour permettre les échanges de données toujours plus volumineuses et... trouver des ressources disponibles. Ces capacités de télécommunications représentent désormais une portion de la couche transport d'un autre domaine, le cyber ;
- **les capacités de télédétection**, passives ou actives, engerbant la détection radar, infrarouge, optique, et par extension les capacités de désignation d'objectifs et de guidage des systèmes d'arme ;
- **les capacités de positionnement, navigation, timing** (PNT) souvent indispensables aux deux autres capacités et contribuant à des degrés divers, à l'ensemble des fonctions opérationnelles.

Le second domaine est celui du combat dans cet environnement, c'est-à-dire de la **guerre électronique (GE)**. La GE naît presque en même temps que les télécommunications, en 1904, avec les premiers brouillages des communications TSF de la Marine nippone par les Russes[4]. L'État-major des armées la définit comme « *une action militaire qui exploite l'énergie électromagnétique pour fournir une appréciation de situation opérationnelle et délivrer des effets offensifs ou défensifs* [...et comme] *l'affrontement dans l'espace électromagnétique* »[5]. La GE comprend trois catégories d'actions :

- « *l'attaque électronique (EA) : l'usage de l'énergie électromagnétique à des fins offensives. Cela inclut les armes à effets dirigés, les micro-ondes à forte puissance, les ondes électromagnétiques et les appareils à fréquences radio ;*
- *la défense électronique (ED) : l'usage de l'énergie électromagnétique pour la protection et pour la maîtrise du spectre électromagnétique ;*
- *la surveillance électronique : l'utilisation de l'énergie électromagnétique pour fournir une appréciation de situation et du renseignement* »[6].

Pour réaliser ces actions, les systèmes d'arme délivrent à leurs niveaux trois types de mesures : les contre-mesures électroniques (CME), les mesures de protection électroniques (MPE) et les mesures de soutien électroniques (MSE).

Le dernier domaine est celui du **renseignement d'origine électromagnétique**, le ROEM, domaine connexe à celui de la surveillance électronique dont il exploite et capitalise les données en temps plus réfléchi.

La problématique **d'une dégradation de cet environnement EM** se pose au sein des forces occidentales depuis des années, pour deux raisons majeures :

- **la perception d'un retour de la menace dans le domaine de la guerre électronique** à laquelle nos armées sont d'autant plus vulnérables qu'elles sont « *network-enabled* » et qu'elles n'ont pas suffisamment investi dans ce domaine durant une décennie de contre-insurrection. Alan Shaffer, *Assistant Secretary of Defense for Research and Engineering* américain, résumait le sentiment général outre-Atlantique en septembre 2014 par cette formule « *We have lost the electromagnetic spectrum* »[7] ! Cette préoccupation s'inscrit dans l'analyse

plus large d'une remise en cause de la supériorité occidentale, par la (re)montée en puissance rapide des forces armées chinoises et russes. La GE serait ainsi un des instruments clés des capacités adverses de déni d'accès et d'interdiction de zone (A2/AD) ;

- **la congestion croissante de l'environnement électromagnétique** générée par la numérisation généralisée des échanges d'information et qui se caractérise par une croissance continue de l'usage des réseaux de communication sans fil, tout particulièrement en zone urbaine.

Pour traiter cette double problématique, la présente note expose :

1. **un panorama des menaces et risques**, lequel commence par un rappel des permanences et des évolutions techniques qui affectent et devraient affecter les capacités de la GE, mais aussi les risques d'interférence accidentelle. Il passe ensuite en revue les capacités de GE dont les différents acteurs stratégiques sont supposés disposer, en insistant sur l'un des modèles capacitaires les plus achevés, celui des forces russes. Enfin, il analyse les facteurs susceptibles d'affecter le développement de ce spectre de menaces à court-moyen terme ;
2. **un essai de caractérisation du problème que pose cette dégradation de l'EME pour notre système de force**. Cette partie se fonde sur une application partielle d'une méthode dite « d'analyse des dépendances et des vulnérabilité 'inter-domaines' », développée par l'auteur dans le cadre de l'expérimentation multinationale MNE7 en 2011-2012 (voir annexe 5). Cette analyse est menée au niveau interarmées puis pour chaque milieu. Cette estimation est suivie de **recommandations capacitaires** par domaines DORESE, proposées *in abstracto* des mesures prises par nos institutions et alimentées notamment par les pistes sur lesquelles communiquent les institutions américaines ou suggérées par leur think tanks.

Précisons cependant que cette note non protégée, élaborée à partir de sources ouvertes complétées d'entretiens, ne prétend aucunement proposer une analyse détaillée et exhaustive de vulnérabilité de nos systèmes.

Enfin la problématique qui nous intéresse ici nous amène à concentrer notre propos sur les effecteurs d'attaque électronique, tout particulièrement sur les contre-mesures électroniques. Les questions relatives aux armes à énergie dirigée et au cyber, abordées ici de façon périphérique, seront explorées plus avant dans les travaux ultérieurs. La note n'aborde pas non plus les capacités occidentales dans ce domaine, se concentrant surtout, en ce qui nous concerne, sur les cibles que constituent nos moyens d'exploitation du spectre électromagnétique, cœur de la dégradation de l'environnement électromagnétique de nos opérations.

Menaces, contraintes et évolutions techniques dans le domaine électromagnétique

1. Un environnement technologique en mutation rapide

1.1 Rappel de quelques bases de l'attaque électronique

L'attaque électronique recouvre l'emploi des **armes à énergie dirigée** qui seront traitées ultérieurement, des **missiles antiradiations,** comme l'AGM-88 américain, utilisés pour la destruction des radars adverses, enfin et surtout le vaste ensemble des **contre-mesures électroniques**. **L'efficacité de ces CME est indissociable des capacités de surveillance électronique et de la capitalisation du ROEM**.

1.1.1 Les catégories basiques de CME

La doctrine américaine retient plusieurs catégories de contre-mesures électroniques :

- **l'emploi de leurres**, pour l'autoprotection des plates-formes contre les systèmes de guidage optroniques, infrarouges ou électromagnétiques des systèmes d'arme ;
- **les émissions de brouillage actif (*jamming*)** des radars, des télécommunications ou d'autres émissions adverses ;
- **l'intrusion électromagnétique** au sein des systèmes adverses qui consiste en une « *intentional insertion of EM energy into transmission paths in any manner, with the objective of deceiving operators or causing confusion* ». Les canaux d'intrusion comprennent les moyens de télécommunication et les radars ;
- **la déception électromagnétique**, qui consiste à utiliser l'énergie électromagnétique « *de façon à tromper, distraire ou séduire l'ennemi ou ses systèmes électroniques* » selon l'OTAN.

Cela étant, pour mieux prendre la mesure de ces CME, il convient de les décliner plus précisément dans les trois domaines majeurs d'emploi du spectre EM, qui présente chacun des conditions technico-opérationnelles propres : radars, communications, signaux de PNT.

1.1.2 L'attaque des radars

La typologie proposée par la doctrine américaine s'applique tout particulièrement aux attaques des radars. Elles comprennent en premier lieu les techniques de brouillage noyant l'écho dans le « bruit EM » : brouillage de barrage couvrant l'ensemble d'une large bande de fréquences, brouillage par balayage (*sweep jamming*) au sein d'une large bande de fréquences ou brouillage sélectif (*spot jamming*) d'une bande ou d'une fréquence particulière. Elles incluent en second lieu les techniques de déception ou de séduction, comme le brouillage par répétition ou « vol de fenêtre », visant à faire « décrocher » le radar adverse de sa cible en manipulant le signal renvoyé. Ces techniques se répandent à partir des années 1970. Elles incluent également l'emploi de leurres actifs assez sophistiqués pour reproduire les signatures radars des plates-formes à protéger. Un autre paramètre concerne la position du brouillage qui peut être réalisé à distance de sécurité (*stand off*) ou dans la bulle des moyens de défense adverses (*stand in*) en escorte d'autres effecteurs.

1.1.3 L'attaque des télécommunications

L'attaque électronique des communications recouvre d'une part le brouillage relevant du déni de service, incluant les techniques de déception, d'autre part l'intrusion électromagnétique.

Un facteur important conditionnant le brouillage réside **dans les différences de vulnérabilités des bandes de fréquence** : alors que le brouillage est assez simple pour le spectre allant de la HF à l'UHF, il devient plus difficile à réaliser au fur et à mesure

que l'on monte en SHF compte tenu des puissances d'émission et de la directionnalité croissante qu'impliquent les transmissions sur ces bandes. Cependant, seules les transmissions en EHF restent, pour l'instant, immunes au brouillage.

Pour faire face à ces attaques, les **mesures de protection électronique** peuvent inclure :

- **la réduction de la signature électromagnétique,** de l'exposition des transmissions aux capteurs de surveillance adverses, par la directionalité des communications et/ou le contrôle des émissions (EMCON) ;
- **le chiffrement des données**, principal moyen de lutte contre l'intrusion EM, mais qui consomme beaucoup de bande passante ;
- **les techniques d'étalement du spectre** permettant de contourner le brouillage : le saut de fréquence consistant à séquencer le message sur plusieurs fréquences, mais aussi l'étalement du spectre par séquence direct qui remplace le bit de donnée transmis par une série de bits sur une largeur de spectre plus grande. Elles sont d'autant plus réalisables que la bande passante, donc la fréquence, est élevée.

Bien évidemment, dans la course sans fin entre le glaive et la cuirasse, les techniques d'attaque s'adaptent à ces évolutions et connaissent une large diversification. **Il est ainsi possible de distinguer une douzaine de modes d'action** en fonction de la nature proactive ou réactive (calés sur la transmission adverse) du brouillage, du caractère permanent ou intermittent de ce brouillage, de la largeur du spectre de fréquence et du nombre de canaux attaqués, du caractère ciblé ou aléatoire des fréquences attaquées, du nœud ciblé (récepteur, émetteur, système de gestion de la transmission), donc de l'importance du ROEM[8].

L'un des brouillages les plus répandus porte sur les communications par satellites (SATCOM) non chiffrées. Il va potentiellement affecter les émissions en UHF – particulièrement utiles aux opérateurs mobiles –, et en SHF – dont la bande Ku représente un pilier de la diffusion haut débit. Le brouillage peut être réalisé par deux techniques assez simples :

- **le brouillage de bruit ou l'usurpation de la liaison montante vers le satellite** qui n'est plus capable de relayer le signal vers ses destinataires ;
- **le brouillage de bruit de la liaison descendante,** s'exerçant sur les récepteurs. Il a une portée locale ou tactique estimée à quelques kilomètres en zone urbanisée et jusqu'à 20 km en espace découvert[9], mais il est possible d'utiliser un brouilleur aéroporté.

Par extension, ce type de brouillage peut affecter également les liaisons en ligne de vue entre éléments d'un système, particulièrement **les systèmes de drones**. En général, sur un système de drone ISR, si la liaison assurant le contrôle du drone est chiffrée, il n'en est pas de même pour la liaison de données ISR (même si le chiffrement de la vidéo ou de l'imagerie à la source est possible), car l'essentiel des données ISR sur une mission ne révèle aucun élément critique[10]. En revanche, dès lors que le drone est armé, le chiffrement de la liaison de données devient un impératif.

1.1.4 L'attaque des services de navigation par satellite (GNSS)

Le brouillage des émissions de PNT assurées par les systèmes de GNSS, GPS et Galileo pour nous, relève de la catégorie précédente car les canaux UHF utilisés sont proches de celles de plusieurs SATCOM. **On distingue le brouillage de la réception du signal par émission de bruit (*jamming*) de l'usurpation de ce signal (*spoofing*).** Techniquement, le brouillage est facile à réaliser à condition que l'attaquant soit, là encore, en ligne de vue des récepteurs. La puissance du signal GPS est en effet assez faible. A titre d'exemple, un brouilleur de 4 watt, de la taille d'un poste radio portable, comme celui vendu par la firme russe Aviaconversia depuis les années 1990, peut empêcher un récepteur d'acquérir le code militaire P(Y) à plus de 30 km et le faire décrocher à environ 10 km[11]. Le *spoofing*, qui aura pour effet de fausser le recalage du positionnement, est beaucoup plus difficile à détecter. En revanche, la nécessité de synchroniser l'attaque avec le signal rend la manœuvre plus compliquée. Il est possible d'envisager la combinaison des deux modes d'action, à savoir le brouillage pour faire décrocher le signal puis la réacquisition d'un signal usurpé. Un tel leurrage devant inscrire son action dans la durée pour être efficace, sa mise en œuvre apparaît plus logique contre les plates-formes à évolution lente[12].

La vulnérabilité du GPS étant un sujet de préoccupation depuis des années, de nombreuses mesures sont développées pour en atténuer les effets : renforcement du signal satellitaire, relais terrestres le complétant (voir annexe 4). Les ingénieurs notent cependant que cet accroissement du nombre d'émetteurs PNT est lui-même de nature à offrir de nouvelles sources de vulnérabilité… Concernant la navigation des plates-formes, les GNSS assurent le recalage de positionnement mais la navigation reste assurée par les centrales inertielles et autres solutions embarquées. **La fonction dont la perturbation est peut-être la plus problématique est celle du *Timing***, nécessaire à la synchronisation d'une large part des systèmes de télécommunications et des radars et dont l'interdiction peut provoquer rapidement l'interruption du service.

1.2 *Les risques permanents et accrus d'interférences*

A la différence des contre-mesures électroniques qui supposent une action intentionnelle, les interférences accidentelles représentent un risque permanent quelle que soit l'opération. Ces interférences sont souvent difficilement différentiables des contre-mesures.

Certains facteurs technologiques tendent à en réduire les risques, comme la généralisation des transmissions de signaux numériques, la quantité croissante de données transmises sur une fréquence donnée et les capacités de montée en fréquence des transmissions permettant de dégager de nouvelles ressources. En revanche, l'accroissement continu du nombre d'émetteurs tend à compenser ces gains.

Ces interférences peuvent tout d'abord se manifester **entre systèmes radars, de communications, de réception GNSS et bien sûr de CME au sein d'une force et relever ainsi des problèmes d'interopérabilité.** En général, elles seront ainsi moindres dans des opérations menées en national. Bien évidemment, ces risques se posent tout particulièrement dans un environnement de coalition où cohabite une forte concentration d'émetteurs, qui plus est opérant selon des sources de standardisation multiples. Le manque d'interopérabilité des outils censés assurer au sein des J6 la gestion du spectre EM contribue à entretenir le risque.

L'instrument militaire américain constitue un bon exemple d'environnement à fort risques d'interférences endogènes. Le Pentagone utilise pour ses seules communications, pas moins de 68 formes d'onde dont les trois quarts sont propriétaires[13]. Lors de l'opération Iraqi Freedom, sur une période de 16 mois, le DoD a enregistré environ 50 interférences sur ses émissions via des SATCOM commerciaux. Vingt-neuf cas relevaient du « *self-jamming* » par accident. Sur les 21 cas restants, seuls cinq ont été répertoriés comme des tentatives délibérées de brouillage[14]. Le général Hyten, à la tête du US Strategic Command, a révélé que les forces américaines avaient enregistré, en 2015, pas moins de 261 cas d'interférence de leur SATCOM, « *almost always self-jamming* »[15].

Ces interférences peuvent ensuite se poser avec l'environnement électromagnétique externe dans lequel intervient la force. Concrètement, la ressource fréquentielle est attribuée en France par le Tableau national de répartition des bandes de fréquences élaboré par l'Agence nationale des fréquences sous l'autorité du Premier ministre[16]. Au niveau international, les normes et ressources sont harmonisées par l'Union internationale des télécommunications de l'ONU. Chacun peut constater tous les jours le niveau de maîtrise atteint dans la gestion de nos environnements EM civils au sein d'une zone donnée. Cependant, le nombre d'utilisateurs augmentant de façon continue, la ressource fréquentielle apparaît de plus en plus contrainte pour l'institution militaire alors même que ses besoins sont eux-aussi en augmentation tendancielle. Le problème vient ensuite en opération extérieure. Réglementairement, la situation sera souvent plus simple mais les interférences peuvent provenir des éventuelles incompatibilités entre la répartition régionale adoptée sur le théâtre concerné et les bandes de fréquences utilisées par la force expéditionnaire.

Enfin, **les interférences peuvent provenir des conditions de propagation**. Les contraintes posées par les masques EM créés par les reliefs ou le bâtis, l'environnement météorologique mais aussi l'environnement géomagnétique affecté par les productions solaires, évoluent peu en soi. En revanche, le recours croissant aux émissions en SHF (comme les bandes Ku, X ou Ka) rend les opérations proportionnellement plus sensibles à ces conditions.

1.3 Des opérations dans le domaine EM en pleine mutation technique

1.3.1 Des mutations déjà à l'œuvre

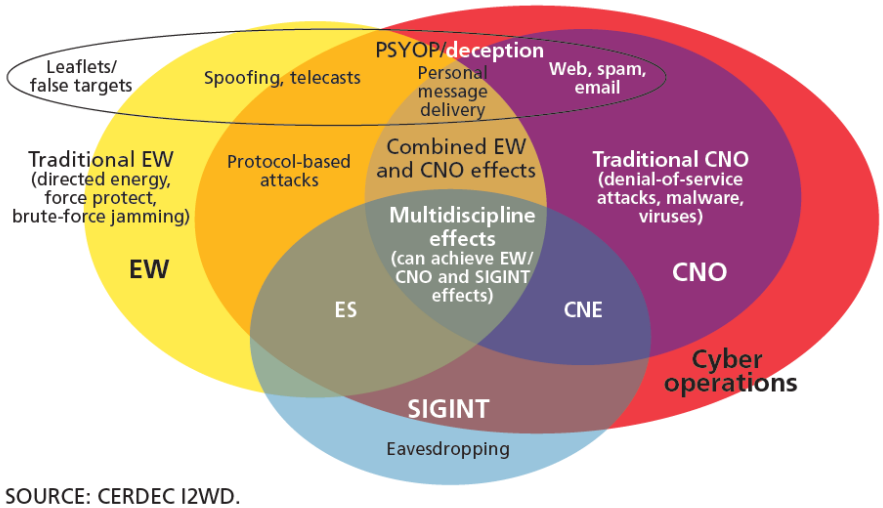
Les opérations dans le spectre EM évoluent à l'aune de mutations technologiques rapides. On en citera les principales : la mise en œuvre opérationnelle des semi-conducteurs à l'arséniure de gallium débouchant sur le développement d'antenne à balayage électronique, l'accroissement continu des capacités de calcul et de mémorisation ou encore la généralisation de la numérisation des signaux.

Ces mutations à l'œuvre depuis environ deux décennies assurent la transition :

- de systèmes mono-mission vers **des systèmes polyvalents**, modulaires et reconfigurables ;
- de systèmes aux modes d'action et données préprogrammés vers **des systèmes « *software-defined* », plus agiles**, c'est-à-dire « manœuvrant » dans le spectre EM en pouvant varier leur fréquences, leur puissance, leur positionnement, etc. ;
- de systèmes de télédétection mono-statique mais aussi opérant sur une bande de fréquence donnée vers des systèmes de **télédétection multistatique** avec un déport de certains capteurs, **des plates-formes de détection hyperspectrale** (combinant ondes radio et infrarouges par exemple) ;
- plus particulièrement, de systèmes radars mono-mission, à haute puissance vers des **radars polyvalents à ouverture synthétique, de basse puissance, à basse probabilité de détection et d'interception (LPD/LPI), voire passif ou multiplexant plusieurs émetteurs et récepteurs**, répliquant les normes les plus récentes en télécommunication WiFi (le « *Multiple Input Multiple Output*, MIMO » soit **« entrées multiples, sorties multiples »)** ;
- de plates-formes qui ont progressivement cédé la place à des systèmes de systèmes et maintenant à des **« familles de systèmes »** ;
- de systèmes lourds, dédiés vers **des systèmes plus légers, voire des microsystèmes à faible contrainte SWAP** opérant en réseau.

Ces mutations techniques, si elles sont correctement exploitées, permettent :

- de passer de modes d'action réactifs classiques (brouillage d'une émission existante ou inversement gestion du spectre répondant à un brouillage) vers **des modes d'action préemptifs,** c'est-à-dire détectant des comportements, des « *patterns* » de l'adversaire et anticipant ainsi ses émissions. Les Anglo-saxons évoquent ainsi la transition vers une « ***Adaptive Electronic Warfare*** »[17] ;
- d'une gestion statique avec allocation préétablie de la ressource fréquentielle vers une **gestion dynamique du spectre électromagnétique** que l'on peut qualifier d'*Electromagnetic Battle Management* (EMBM)[18].



SOURCE: CERDEC I2WD.
RAND *MG1113-5.2*

Vue fonctionnelle de la convergence entre *computer network operations*, *electronic warfare* et *signals Intelligence* selon l'U.S. Army Communications-Electronics Research, Development and Engineering Center
Source : Porche, et al., *Redefining Information Warfare Boundaries for an Army in a Wireless World*, Arroyo Center, Rand Corporation, 2013 p.51

1.3.2 *L'émergence du « combat cyber-électronique »*

La GE devient de plus en plus **indissociable de la guerre cyber** en raison des capacités émergentes d'intrusion électromagnétique permettant, en exploitant des failles dans les systèmes de transmission ou de télédétection, de surveiller, dégrader voire même détruire des éléments des couches logiques et applicatives des systèmes d'information. Il convient ainsi de parler, surtout aux horizons prospectifs, de **combat cyber-électronique** comme le font les officiers Aymeric Bonnemaison et Stéphane Dossé[19]**.** Le corpus doctrinal de l'US Army, en l'occurrence le concept de *Cyber Electromagnetic Activities* (CEMA) de 2014 puis le *Field Manual 3-12*, *Cyberspace and Electronic Warfare Operations* (CEWO) de 2017, a d'ores et déjà acté que le spectre électromagnétique constitue un « dénominateur commun » de la GE et de la guerre cyber, et qu'il était nécessaire de pleinement intégrer et synchroniser les deux domaines d'activité[20].

Cette guerre cyber-électronique ne pourra donner toute sa mesure qu'avec **la distribution de capacités de lutte informatique jusqu'au niveau tactique**. Cette transformation pose encore d'importantes contraintes doctrinales, humaines ou encore organisationnelles. En outre, si les **effets cyber-électroniques** peuvent être beaucoup plus importants que ceux des CME, ils sont aussi plus **compliqués à réaliser**. En effet, l'acquisition et l'analyse du renseignement d'intérêt cyber (empreintes numériques, connaissance de la topologie du réseau et des autres caractéristiques du système adverse, etc.) et la réalisation de l'attaque cyber sont des processus longs. Ils peuvent aboutir à la réalisation de malware affectant les systèmes adverses préalablement et susceptibles au moment opportun de dégrader leurs fonctionnalités. Ils s'accommodent cependant difficilement d'une exigence d'effets à la fois rapides ET significatifs sur une architecture SIC *ad hoc* rapidement déployée. En revanche, un dispositif est susceptible de révéler ses vulnérabilités dans des engagements de temps long l'exposant au renseignement adverse (menaces contiguës dans le cadre de dispositifs de dissuasion ou de contre-insurrection par exemple). En outre, les progrès dans le domaine informatique permettront probablement de raccourcir ces boucles d'action cyber à l'avenir. Cette évolution apparaît donc inexorable dans les années qui viennent.

1.3.3 *Quelques ruptures technologiques accentuant ces évolutions à court terme…*

L'attaque électronique, *a fortiori* cyber-électronique, sera de moins en moins affaire de moyens spécialisés, du moins pour les effets limités. Les évolutions technologiques débouchent en effet sur des équipements polyvalents (consacrés à l'exploitation du spectre et à la GE) et/ou duaux civils-militaires. Ils permettent de développer des **capacités d'attaque électronique que l'on peut qualifier de « non-traditionnelles »** :

- **les antennes à balayage électronique** confèrent aux radars des capacités d'attaque dans la bande de fréquence du capteur. Celle-ci est par exemple mise en avant sur le F-35 ;
- **les radios logicielles qui se diffusent dans le commerce** depuis quelques années apparaissent ainsi tout à fait **utilisables à des fins de combat cyber-électronique**. Elles démultiplient les capacités d'interception de l'ensemble des réseaux types GSM, Tetra ou Wifi dont les vulnérabilités au brouillage et/ou à l'intrusion sont démontrées par plusieurs études[21] ;
- l'usurpation des GNSS est elle aussi probablement amenée à évoluer à l'aune des innovations civiles. Ainsi, le projet de Pizza Hut de livrer ses repas par drone pourrait générer des « recherches accrues » de la part des hackers pour détourner la précieuse livraison[22].

La technologie de la « radio cognitive », permettant d'exploiter de façon dynamique des bandes de fréquence non utilisées, offre des perspectives intéressantes pour limiter ou contourner les contraintes de la congestion du spectre[23].

L'internet des objets connaît un développement fulgurant. Déjà plus de 60% des connexions à Internet sont le fait de mobiles (smartphones, tablettes, etc.). Le groupe de consulting Gartner Research estime que le nombre d'objets connectés autres dépassera les 25 milliards en 2021[24]. Cette évolution va avoir également un impact non négligeable sur le combat cyber-électronique : il implique la multiplication des liaisons électromagnétiques ce qui est de nature à congestionner plus encore le spectre EM. Il offre aussi des perspectives de développement progressif

des réseaux de capteurs abandonnés, n'émettant qu'en fonction des activités détectées. C'est par exemple l'objet du programme N-ZERO de la DARPA[25]. Ces réseaux constituent des opportunités pour notre fonction renseignement, mais aussi pour celle de l'adversaire.

1.3.4 …avant la révolution quantique à plus long terme…

Plusieurs autres technologies offriront des ruptures dans les 10 ans qui viennent, notamment le recours à **l'intelligence artificielle** dans la gestion du spectre ou la transmission par fibre optique du signal émis/reçu par l'antenne, permettant d'exploiter l'ensemble des fréquences jusqu'à plus de 100 GHz, évitant les contraintes actuelles des équipements électriques qui ne peuvent véhiculer un signal que sur une bande réduite de fréquences[26].

Les perspectives les plus fascinantes sont cependant offertes par les **technologies quantiques**. A moyen terme (5 à 10 ans), le Pentagone, engagé dans une course avec la Chine, envisage de parvenir à des **technologies matures pour les instruments de navigation et les horloges**. Si tel est le cas, **la capacité PNT pourrait être progressivement révolutionnée à l'horizon 2030** car cette technologie rendrait inutile le recours aux GNSS. **Les travaux sur les radars quantiques** (reposant sur le phénomène de l'intrication de deux photons au sein d'une paire) sont déjà lancés depuis plusieurs années, aux États-Unis, en Chine ou encore au Canada[27]. Cette technologie, si elle devient mature, **devrait minimiser l'apport de la furtivité, au moins contre les radars de veille**, ou encore, en théorie, **déjouer les CME de déception** (en jouant sur la signature que constitue la polarisation spécifique du champ électrique d'une émission radar)[28]. A plus long terme, les scientifiques rêvent du Saint Graal de l'ordinateur quantique permettant des ruptures majeures non seulement dans la vitesse de calcul – en accélérant les possibilités d'intelligence artificielle, mais également la nature des données prises en compte. Dans le domaine qui nous intéresse, **le calcul quantique révolutionnerait la dualité chiffrement / décryptage** des données. La puissance disposant d'une avance technologique en la matière s'adjugera ainsi un avantage capacitaire décisif[29].

Bien entendu, il convient de ne pas sous-estimer les difficultés classiques de cristallisation des besoins permettant à une technologie en cours de maturation de franchir la fameuse « vallée de la mort » entre R&D et programmes opérationnels.

2. La guerre électronique, une des pierres angulaires des capacités d'interdiction russes et chinoises

2.1 Radioelektronnaya bor'ba

La réémergence militaire russe se traduit dans la balance des potentiels par une compétition renouvelée avec les Occidentaux pour le contrôle du spectre électromagnétique. Ce dernier ne se limite pas à la guerre électronique : il comprend les nouveaux capteurs mis en œuvre par les forces russes, par exemple l'architecture de détection radar de son système intégré de défense antiaérienne, que nous aborderons dans une autre note.

La guerre électronique (*radioelektronnaya bor'ba*, REB) a toujours été un point fort des armées russes. Elle représente avec les défenses sol-air ou encore les missiles antinavires **l'une des pierres angulaires de cette réémergence impulsée par la réforme Serdioukov de 2008**. **La GE connaît donc depuis cette période une refonte touchant tous les domaines DORESE**. Il s'agissait en premier lieu de répondre aux nombreuses insuffisances constatées lors du conflit géorgien (manque de préparation ESM, de fiabilité et de soutien des équipements, d'intégration des moyens dans la manœuvre, de protection électronique face aux forces géorgiennes). En second lieu, la GE représente l'une des principales réponses « asymétriques » à la sophistication des moyens conventionnels occidentaux, comme l'explique le General Major Lastochkin[30].

Leur redoutable efficacité contre l'armée ukrainienne dans le Donbass en 2014-15 a agi comme un révélateur pour les Occidentaux. Les développements en sources ouvertes qui en ont découlé, exploitant les

nombreuses sources russes, permettent d'avoir une vue assez complète de ces capacités russes, au moins théoriques.

2.1.1 La doctrine

La REB fait l'objet de plusieurs définitions officielles. Certaines sont l'exacte reprise des définitions otaniennes[31]. La plus intéressante émane du dictionnaire encyclopédique militaire des armées russes. Elle y est présentée comme « *a type of armed struggle using electronic means against enemy C4ISR to "change the quality of information", or using electronic means against various assets to change the conditions of the operational environment. EW consists of suppression and protection. It aims to "reduce the effectiveness" of enemy forces, including command and control and their use of weapons systems, and targets enemy communications and reconnaissance by changing the "quality and speed" of information processes. In reverse, EW in defence protects such assets and those of friendly forces* »[32].

Le chercheur Roger McDermott explique ainsi que la REB représente un **« multiplicateur de force »** au cœur de la reprise par les Russes du concept de *Network-Centric Warfare*, « épicentre » de leur modernisation actuelle[33], en dépit d'un gap capacitaire en matière de SIC que les Russes ne cherchent manifestement pas à combler.

Les doctrines et retours d'expérience de l'Ukraine semblent montrer que les unités de guerre électronique emploient **leurs capacités d'attaque électronique** :

- comme un effecteur à part entière, de façon pleinement intégrée avec les capacités de manœuvre et les feux, y compris ceux de la défense sol-air... ;
- ... comme des relais d'opérations militaires d'influence via la transmission de messages sur les réseaux de communication adverses... ;
- ... comme des émetteurs de déception, amenant l'adversaire à dévoiler ses propres feux ou moyens d'attaque électroniques, créant ainsi une « maskirovka électronique » ;
- enfin, comme moyens défensifs pour neutraliser les feux de précision adverses (guidage, fusées de proximité, etc.).

Leurs capacités de surveillance électronique, outre la caractérisation des émissions, la goniométrie et l'alerte, représentent une source majeure de renseignement d'origine électromagnétique (ROEM)... ...et des capteurs de ciblage d'opportunité au profit des feux contre les cibles de surface. Enfin, **leur capacité de protection électronique suit** les axes classiques de la gestion du spectre, du durcissement EM et du contrôle des émissions.

Les unités de REB opèreraient en étroite coordination avec les unités de transmissions dans la gestion du spectre EM, afin de préserver les capacités de télécommunications des forces russes. En revanche, il semble que **les Russes présupposent que leur système de GE interdirait tout signal PNT (GPS/GLONASS) sur le champ de bataille, y compris pour leurs propres unités**[34].

Les penseurs russes envisagent un développement incrémental des aptitudes de la REB passant du « blocus de l'information électronique », actuellement recherché, à « l'usurpation et à la destruction des bases de données » ennemies. McDermott estime donc que les Russes vont également progresser dans la fusion cyber-électronique.

La REB est donc le pivot d'une doctrine intégratrice qui apparaît semblable, toute chose égale par ailleurs, **à celle des *information operations* américaines,** dont les Russes pousseraient la mise en œuvre bien au-delà des Occidentaux eux-mêmes ! En d'autres termes, **compte tenu de l'avance prise sur la GE occidentale**, la REB semble être **l'instrument privilégié du nivellement de la confrontation avec un système C4ISR adverse que les Russes ne peuvent émuler**. À cet égard, **la REB pourrait devenir une arme à part entière des forces russes** durant la prochaine décennie.

2.1.2 L'organisation

La réforme de 2008 s'est traduite par une intégration des moyens de guerre électronique au sein **d'un commandement fonctionnel unique**, commandé par le General Major Yuriy Lastochkin depuis 2014.

À l'inverse des forces américaines, en Russie, **ce sont les forces terrestres qui sont en pointe dans le domaine de la GE**. Ces forces alignent deux types d'unités de guerre électronique :

- **des brigades indépendantes** rattachées aux commandements interarmées de district (une

par district militaire, deux pour le district ouest), constituées de 2009 à 2015. Ces unités à quatre bataillons sont destinées à une GE de portée opérative voire stratégique, visant les capacités de communication en HF et les capacités ISTAR des puissances aérospatiales otaniennes (radars aéroportés et satellites, GPS, etc.) ;

- **des compagnies de guerre électronique**, une par brigade de combat, destinées à la GE tactique sur les zones de contact et d'appui adverses, soit sur une allonge de 50 km. Leur dotation comprend notamment une douzaine de stations de brouillage automatisées permettant de neutraliser les communications tactiques, les SATCOM, le GSM, le GPS ou encore les fusées de proximité adverses.

Ces unités peuvent détacher des modules en appui d'autres échelons, et opérer en groupements tactiques interarmes avec d'autres moyens, selon la pratique du groupement *ad hoc* bien établie dans l'armée russe.

Les « forces aérospatiales » (VKS), qui se voient accorder la priorité dans la stratégie capacitaire russe, disposent de moyens propres mais sont surtout massivement appuyées par les capacités des brigades de district. Ainsi, en cohérence avec leurs doctrines et concepts, **les forces russes des trois armées intègrent** organiquement, ou peuvent intégrer en détachement parfois interarmées, **des moyens de GE à tous leurs échelons**.

2.1.3 Les équipements

La modernisation de la GE s'appuie sur **la consolidation, de 2009 à 2012, d'une BITD auparavant très éclatée**. Les équipements sont désormais fournis par deux grandes entreprises : *Kontsern RadioelectronicTechnologies* (KRET) et *Kontsern 'Sozvezdiye'*.

La plupart des systèmes de GE russes, y compris les plus récents, sont hérités de programmes ou de concepts élaborés à la fin de la Guerre froide pour faire pièce à la « révolution technico-militaire » que les Russes voyaient poindre chez leurs adversaires de l'OTAN. Cependant, les efforts de réinvestissement dans ces programmes sont en pleine phase d'aboutissement. La GE connaît en effet depuis le début de la décennie **une modernisation impressionnante**. **L'objectif initial de la réforme Serdioukov visant le rééquipement des forces russes à 70% d'équipements modernes en 2020 sera largement atteint pour les unités de la REB**, contrairement à d'autres fonctions opérationnelles des forces russes.

Les équipements présentant les performances les plus ambitieuses, sont ceux dotant les brigades de GE : **les fameux brouilleurs Krasukha-2 et -4**, destinés à la neutralisation du dispositif C4ISR de la puissance aérienne adverse[35], **le Murmansk BN** de brouillage des communications HF**, le RB 341V Leer-3** de brouillage des réseaux GSM, pouvant reposer sur des drones tactiques Orlan-10[36], enfin l**e RB-109 Bilyna,** le nouveau système de contrôle de la brigade qui ferait appel à des techniques d'intelligence artificielle pour assurer un *battle management* largement automatisé et intégré avec les réseaux de la défense aérienne[37]. Ces moyens sont utilisés en pleine complémentarité avec les nombreux systèmes ROEM russes, à commencer par le récent **Moskva-1[38].**

Les compagnies de GE tactiques présentent également plusieurs équipements récents remarquables : le **RB 301B Borisoglebsk-2**, intégrant l'ensemble des contre-mesures HF/VHF[39], **le SPR-2 Rtut BM**, engin de neutralisation des fusées de proximité des roquettes et munitions de précision et **la famille des RP-377 en V/UHF portables ou déployables** sur véhicules légers. Déployées dans toutes les compagnies de GE, elles sont particulièrement utiles aux VDV (les troupes parachutistes, forces d'élite de l'armée russe).

Les VKS sont équipées de plusieurs systèmes récents. Les principaux visent à brouiller, en stand-off, des « *systèmes de C2 ainsi que les radars des missiles sol-air et air-air* » : le **Rychag-AV** embarqué sur hélicoptères Mi-8MTPR-1[40] et, à plus longue portée, quelques **Il-22PP Porubshchik** puis des **Tu-214PP** plus volumineux[41]. Les appareils d'interdiction SU-34 emportent des **nacelles Khibiny** en bout de voilure. Enfin, les appareils d'interdiction russes peuvent embarquer le Kh-31P, un missile antiradar d'une centaine de kilomètres de portée, équivalent de l'AGM-78 américain. Les capacités de la marine, pourtant réelles, sont en revanche assez peu documentées, hormis les systèmes de CME mis en œuvre par les corvettes les plus récentes[42].

2.1.4 *L'entraînement et les retours d'expérience*

Les unités de la REB bénéficieraient d'un niveau opérationnel croissant. En 2016, les seules unités du district centre ont participé à environ 50 exercices soit une augmentation de 50% par rapport à 2015[43]. Le niveau d'agrégation de ces exercices a été développé. L'armée russe a ainsi réalisé un vaste exercice interarmées, Elektron-2016, le premier de la sorte depuis 1979[44]. La REB a été pleinement intégrée dans Zapad-2017.

Les Russes déploient d'importantes capacités en Syrie. Elles sont employées à des fins de protection de force, pour assurer la couverture des autres systèmes d'interdiction de zone des VKS ainsi que, très probablement, pour appuyer la manœuvre syrienne et pour **recueillir un maximum de ROEM sur les forces occidentales**. Elles sont également depuis utilisées **pour gêner les opérations occidentales** comme le général Thomas, commandant les forces spéciales américaines, l'a expliqué récemment[45]. Les moyens déployés incluent au moins un Krasukha-4 et un Leer-3[46]. Il semble que les Russes aient intégré ces systèmes dans leurs arrangements de déconfliction avec les Israéliens et peut-être les Américains.

Cependant, le modèle d'emploi de la REB reste bien sûr **l'intervention dans le Donbass**. Elle a permis d'une part de **dégrader la cohérence de la manœuvre de l'armée ukrainienne, d'autre part d'améliorer drastiquement l'efficacité des feux des forces séparatistes et russes**.

Les capacités de GE russes dans le Donbass reposaient sur deux types d'unités. **Deux à cinq groupes de « contrôle technique intégré »** fournissaient des appuis rapprochés ou de contact, effectuant de la surveillance électronique, en l'occurrence du COMINT technique et de la goniométrie des moyens GSM et radio VHF ukrainiens, et secondairement du brouillage de protection. Ces groupes intégraient du personnel des unités REB et du GRU, mettant en œuvre des systèmes portables Lorandit et ELK 7077 de ROEM. **Au moins 2 groupes de manœuvre REB** fournissaient un appui de zone, à 30-40 km des lignes, exécutant là encore COMINT technique / goniométrie, mais aussi le gros des effets d'EA : actions d'interdiction des communications tactiques terrestres et aériennes, actions d'influence sur leurs adversaires ukrainiens via le réseau GSM. Chacun de ces groupes mettaient en œuvre pour ce faire des binômes de stations automatisées R-330 et R-934, un ou deux Infauna et deux systèmes Leer-3[47].

2.2 *Un modèle chinois résolument tourné vers la guerre cyber-électronique*

Au sein de l'armée populaire de libération (APL) chinoise, **la guerre électronique devient une des capacités majeures permettant d'interdire aux Américains l'accès au Pacifique ouest**, selon la stratégie développée depuis 20 ans.

Un premier concept dédié**,** l'***Integrated Network Electronic Warfare***, a été élaboré au début des années 2000. Déclinant le fameux concept de « guerre locale informatisée » visant à frapper de façon préemptive les points de vulnérabilité américains[48], il envisageait **un emploi intégré des attaques électroniques, informatiques et cinétiques contre les nœuds et flux de l'infrastructure C4ISR et l'obtention de la domination informationnelle**[49]. L'APL a récemment actualisé ses concepts, et les réformes récentes décidées par Xi Jinping ont refaçonné l'organisation de la guerre électronique. L'APL considère actuellement la guerre comme **une opposition entre « systèmes de systèmes »** : commandement, frappe, renseignement-reconnaissance, soutien et, en ce qui concerne la GE, le **système de confrontation informationnelle**. Ce dernier comprend les deux volets classiques défense et attaque, ce dernier incluant l'attaque électronique (brouillage), l'attaque des réseaux, l'attaque psychologique et la destruction des infrastructures informationnelles. Chaque engagement nécessite un système opérationnel spécifique intégrant ces sous-systèmes. La finalité, directement inspirée des concepts américains, est d'opérer dans la boucle décisionnelle de l'adversaire[50]. Sur le plan organisationnel, une **force d'appui stratégique (SSF) a été créée** afin de placer **sous une autorité unique l'ensemble des unités de guerre de l'information**, donc la GE, le cyber et les forces spatiales[51].

Les Américains estiment que l'APL dispose d'un spectre assez complet de capacités de GE terrestres, aéroportées et navales[52]. Le cas des forces aériennes semble le mieux documenté : elles aligneraient ainsi une flotte conséquente de dérivés des quadrimoteurs Y-8 et Y-9 : peut-être 11 appareils de ROEM et au moins 8 Y-8G et de nouveaux Y-9G de brouillage stand off[53] et plus récemment, une version GE du bombardier H-6[54]. Elles mettent également en œuvre le J-16D, une version de brouillage d'escorte et de SEAD du Su-30 indigène, un équivalent basé à terre de l'EA-18G Growler de l'US Navy,

avec CME et missiles antiradars YJ-91, version locale du Kh-31 russe[55].

Enfin, **l'interdiction des capacités spatiales américaines joue un rôle déterminant dans cette doctrine**. L'exégèse des écrits chinois rend compte de développements capacitaires de *counterspace* permettant d'atteindre l'ensemble des constellations américaines sur les différentes orbites. Les armes à énergie dirigée ou les missiles sont régulièrement mis en avant. Cependant, certains experts pointent les concepts chinois de brouillage des liaisons de télémesure et télécontrôle des satellites, et d'opérations co-orbitales d'attaque électronique des SATCOM américaines par des microsatellites. Ces modes d'action exploiteraient les progrès en matière de « *rendezvous and proximity operations* », dont une demi-douzaine a déjà été réalisée par Pékin depuis 2008[56].

3. Une prolifération encore limitée mais qui devrait logiquement se renforcer...

3.1 Une prolifération encore assez réduite

Autant les capacités des principaux pays occidentaux, des deux grandes puissances militaires émergentes et d'Israël (voir ci-contre) à façonner l'environnement EM à leur avantage sont évidentes, autant celles des autres acteurs restent très lacunaires, comptant surtout les moyens rudimentaires de brouillage GPS et, bien sûr, les nombreux systèmes d'autoprotection des plates-formes. Les puissances régionales commencent cependant à se doter de moyens d'attaque. Quant aux autres États et aux entités stratégiques non-étatiques tels que les proto-États djihadistes, leur capacité à perturber sérieusement les opérations EM adverses reste encore dans les limbes.

3.1.1 Quelques capacités affichées

Dans l'arc de crise, c'est sans surprise **Israël qui dispose, probablement de loin, des capacités les plus robustes**. L'état-major général des forces de défense de l'État hébreu dispose sous son commandement direct d'un bataillon de guerre électronique. L'unité a pour mission, outre la surveillance et le ROEM sur le Hezbollah et autres acteurs djihadistes en Syrie, de perturber les transmissions, de toutes natures, de contribuer à la manœuvre d'influence et d'interdire les détonations d'EEI, tâches largement accomplies contre le Hamas[57]. La force aérienne repose quant à elle sur l'escadron Sky Crows, d'attaque des communications et des radars adverses. L'unité met en œuvre des variantes de C-130 et de CH-53[58].

L'Égypte est l'autre pays de l'arc de crise disposant de capacités étendues. Outre ses importantes capacités ELNT, son armée de l'air dispose de deux à quatre hélicoptères commandos Mk2E dotés de brouilleurs Selenia IHS-6[59]. L'armée de Terre dispose des systèmes de CME GSY2210 fabriqués par l'industriel sud-africain GEW Technologies (ex-Grintek Ewation)[60]. Ces capacités sont employées contre Daech dans le Sinaï. L'interdiction des moyens GSM djihadistes a provoqué des perturbations EM dans l'État Hébreu et Gaza[61].

L'Iran dispose de capacités avérées de brouillage élémentaire des COMSATCOM, largement utilisées pour interdire la diffusion de certaines chaînes de télévision sur leur pays (telles la BBC Persian TV ou Voice of America)[62]. Pour le reste, en dépit d'une communication souvent fantaisiste, très peu d'éléments concrets sont spécifiés. Les Iraniens disposent sans doute de brouilleurs GPS importés d'Aviaconvertia selon les Américains, ou produits par leur industrie nationale[63]. Les Russes ont délivré des systèmes ELINT 1L222 Avtobaza en 2011. KRET s'est dit prêt en 2015 à exporter d'autres systèmes ELINT Moskva-1, des brouilleurs Rtut-BM mais rien n'a été confirmé depuis. À noter toutefois la présentation d'un « fusil de brouillage » anti-drone UHF, vraisemblablement destiné à interrompre le segment de liaison ISR.[64]

La fameuse capture du drone RQ-170 américain en décembre 2011 a donné lieu à bien des spéculations, dont l'une des principales est celle de l'usurpation de son signal GPS par les Iraniens. Certains ont émis l'hypothèse d'un emploi combiné de l'Avtobaza et de la station 1L125M APUR, mais il n'est fait

mention nulle part de l'acquisition par l'Iran de ce système[65]. Sept ans plus tard, ce qui est arrivé au RQ-170 reste un mystère (spoofing iranien ? brouillage GPS iranien suivi d'un crash ? Crash habilement exploité par la propagande de Téhéran ?).

Au final, il n'est pas prouvé que la GE fasse partie des quelques développements capacitaires prioritaires poursuivis, notamment par le Corps des gardiens de la révolution, à l'instar de la puissance de feu balistique, des capacités navales « asymétriques » ou des drones[66].

La Corée du Nord a pour sa part démontré sa capacité de brouillage GPS. Entre 2010 et 2016, les Nord-Coréens ont réalisé quatre actions de brouillage qui ont affecté les opérations aériennes de l'aéroport international d'Inchon à 40 km de la frontière. Pyongyang disposerait de brouilleurs vendus par la firme russe Aviaconversia portant à plus de 100 km et d'une version indigène qu'il proposerait à l'export au Moyen-Orient[67].

La **Turquie** commence à mettre en œuvre d'importants moyens de GE indigènes. Le plus connu est le Koral fabriqué par Aselsan, un système terrestre de brouillage/déception des radars portant à plus de 100 km, assez analogue au Krasukha-4. Le système est déployé dans le cadre de l'opération « Bouclier de l'Euphrate » en Syrie[68].

En Ukraine et en Biélorussie, les forces armées ont repris et modernisé les systèmes de GE tactique mis en œuvre par les forces soviétiques (systèmes R-330 Mandat-BE1 pour l'Ukraine[69] et Mandat-M pour la Biélorussie[70]).

3.1.2 *Des prévisions anticipant une croissance limitée du marché*

Les analyses les plus récentes envisagent un accroissement du marché de la GE de 13 Mds$ en 2017 à 17,5 Mds$ en 2027. Cependant, la protection électronique continue de dominer ce marché à 59%, suivi de la surveillance électronique pour 30%, l'attaque électronique ne comptant que pour 9% des transactions. De fait, la majeure partie des contrats portent sur les systèmes d'autoprotection des plates-formes. Les acquisitions devraient concerner l'Amérique de Nord, donc les forces américaines pour 45%, la zone Asie-Pacifique pour 27% et l'Europe pour 20%[71]. Le développement anticipé des capacités d'attaque électronique susceptibles de nous être opposées dans notre « arc de crise » AFN-PMO est donc réduit. Il convient cependant de prendre avec précaution ce type d'analyse de marché, comme l'ont montré celles portant sur les drones qui prédisaient régulièrement une explosion du marché civil, laquelle ne s'est en réalité pas produite.

3.2 *Plusieurs facteurs crédibilisent un renforcement de la menace*

Cependant, nos forces pourraient à l'avenir opérer dans des environnements électromagnétiques moins cléments pour plusieurs raisons.

3.2.1 *Un « effet Krasukha » analogue à « l'effet Predator » ?*

L'offre industrielle est en cours de diversification. Les entreprises russes, biélorusse (Kandar-RB), ukrainienne (Topaz puis NPK-Iskra), sud-africaine et turque (Aselsan) présentent des **offres éventuellement à la portée d'un plus grand nombre de budgets** que celles des grands industriels occidentaux. Parallèlement, la **prolifération des systèmes de reconnaissance-frappe à laquelle nous assistons au Moyen-Orient ou en Asie**, dont les moyens ISR et les missiles sont de plus en plus rentables, **est susceptible en retour de générer** chez l'opposant **un besoin accru de systèmes de guerre électronique** permettant d'en perturber l'emploi.

On pourrait en fait assister dans le domaine de la GE à un processus analogue à celui qui a marqué les drones armés depuis quelques années : une offre plus rentable met à la portée d'un plus grand nombre d'acteurs des solutions suffisantes, rencontrant des clients impressionnés par les retours sur l'efficacité des opérations russes en Ukraine (comme ils le furent par celle des frappes américaines de drones).

3.2.2 *Des configurations stratégiques et des capacités non-traditionnelles qui augmentent le risque*

L'éventuelle extension des acquisitions de moyens de GE par les États ne constitue pas la seule source de menace pour nos forces.

Pour les puissances globales ou régionales, l'heure est, par défaut, aux stratégies indirectes ou aux interventions à empreintes réduites. Le soutien aux *proxies* se traduit par des actions d'assistance militaire opérationnelle par les forces étatiques et/ou les entreprises de sécurité et de défense (ESSD), sur le modèle des stratégies de Moscou en Syrie et dans le Donbass et de celles de Téhéran. Dans cette configuration, **nos unités peuvent parfaitement se heurter**, non pas tant aux éléments d'une force nationale ayant importé des équipements de GE, mais **à des soutiens émanant de parrains de notre adversaire, se déployant avec des capacités sélectives de GE**. En effet, **l'utilisation des CME,** aux effets par nature disruptifs et non destructeurs sauf à courte portée, **se prête parfaitement aux confrontations stratégiques « ambiguës »** entre puissances.

courte portée en se dotant de brouilleurs GPS civils, de radios logicielles, voire à l'avenir de systèmes de spoofing de signal GPS civil et d'intrusion de réseaux locaux de base ou des équipements de nos personnels.

3.2.3 *Conclusion : vers un étalement du spectre capacitaire*

À titre de conclusion, le tableau ci-dessous présente empiriquement les types de capacité dont pourraient disposer les différents acteurs stratégiques d'ici une dizaine d'années. Il met en exergue un étalement plausible du spectre des menaces combinant :

- le renforcement des capacités des grandes puissances, déjà largement dotées ;
- la montée en gamme possible des puissances régionales ;

	Entités non-étatiques type Daech	Puissances locales	Puissances régionales	Russie / Chine
Brouillage GNSS courte portée	Probable	Probable	OUI	OUI
Brouillage GNSS de portée opérative	Peu probable	Possible	OUI	OUI
Usurpation GNSS civil	Possible	Probable	Probable	OUI
Brouillage simple COMSATCOM	Possible	Probable	OUI	OUI
Brouillage / intrusion MILSATCOM non durcis	Peu probable	Peu probable	Possible	OUI
Brouillage / intrusion COMM radio dans la profondeur	Peu probable	Peu probable	Possible	Probable
Brouillage / intrusion réseaux tactiques	Peu probable	Peu probable	Possible	Probable
Brouillage/intrusion réseaux locaux	Possible	Possible	Possible	Probable
Brouillage liaisons RPAS	Peu probable	Peu probable	Possible	OUI
Brouillage MGP	Peu probable	Peu probable	Possible	OUI
Brouillage radars dans la profondeur	Peu probable	Peu probable	Possible	OUI

Enfin, la menace est susceptible de s'accroître en raison de la **prolifération probable des capacités de guerre cyber-électronique « non-traditionnelle »** évoquée supra. Un État aux ressources réduites ou un adversaire non-étatique pourra parfaitement se constituer de réelles capacités tactiques de

- l'acquisition tout aussi envisageable de moyens de guerre cyber-électronique « de poche » par un nombre croissant d'acteurs.

Vulnérabilités potentielles de nos systèmes de force et implications capacitaires

1. Caractérisation de la problématique de la dégradation de l'environnement électromagnétique pour nos forces

Comme rappelé en introduction, cette section n'a pas pour objectif de réaliser une analyse précise de vulnérabilité de notre système de force aux menaces exposées en première partie, laquelle ne peut relever que de la fonction renseignement et des études technico-opérationnelles.

En revanche, pour formuler des recommandations DORESE susceptibles d'intéresser l'institution, elle doit préalablement s'essayer à caractériser les vulnérabilités potentielles et leur criticité. Pour ce faire, elle identifie les principales capacités d'exploitation du spectre (COMM, PNT et télédétection) à l'égard desquelles nos forces sont dépendantes, estime les types d'attaque envisageables et la criticité de leurs effets. Elle s'appuie sur des « *knowledge map* » illustrant les relations d'« enabling » / « enhancing » entre les systèmes (voir annexe 5).

1.1 Le niveau interarmées

1.1.1 Les communications

Le premier domaine de vulnérabilités potentielles concerne les communications par satellites :

- les MILSATCOM Syracuse III/IV. Syracuse III, relayant en EHF et SHF, assure d'une part un réseau de transmission sécurisé (RTRAN) entre les principaux états-majors, prolongé par un réseau de mobiles (REMO) bas débit avec les échelons tactiques les plus bas, d'autre part un réseau de diffusion IP haut débit non durci (RDIFF) ;
- les systèmes franco-italiens Sicral et Athéna-Fidus COMCEPT, non durcis, permettant de délester Syracuse pour les échanges haut débit niveau DR (Intradef, vidéo, imagerie) ;
- les COMSATCOM variés, en large bande Ku, tel EUTELSAT, ou UHF tel INMARSAT pour les échanges non protégés ;
- des SATCOM UHF complémentaires pour les liaisons spécialisées (opérations spéciales et contrôleurs aériens avancés)[72].

Au moins quatre types d'attaque potentiels sont envisageables :

- l'attaque du segment satellitaire comme évoqué en première partie : opérations co-orbitales apanage des grandes puissances ;
- le brouillage des liaisons montantes, plus répandu, envisageable contre Sicral, Athéna-Fidus, les COMSATCOM et peut-être contre le RDIFF ;
- l'attaque directe du segment utilisateur par le brouillage de la liaison descendante, contre les mêmes composantes ;
- l'attaque indirecte du segment utilisateur par le brouillage des signaux GNSS perturbant la synchronisation des transmissions.

Ces attaques du segment utilisateur nécessitent avant tout des capacités spatiales sophistiquées ou au moins des brouilleurs en ligne de vue. Pour ce qui concerne les transmissions stratégiques ou opératives, elles ne semblent donc à la portée que des quelques puissances disposant de brouilleurs aéroportés stand-off. Cependant, à l'heure du combat cyber-électronique, la société IOActive a démontré que plusieurs terminaux de COMSATCOM UHF, comme Thurraya, Inmarsat-C ou encore Iridium, souffraient de vulnérabilités cyber[73].

L'autre domaine est bien sûr celui des **capteurs de la fonction interarmées du renseignement** : satellites de reconnaissance (Hélios II et Pléiades, plus tard composante satellite optique, recours aux satellites radar alliés et acquisition d'imagerie commerciale pour le ROIM, CERES pour le ROEM) ; C-160 Gabriel puis Falcon Epicure dotés de la charge utile de guerre électronique (CUGE), futurs ALSR ; composante terrestre ROEM du 44ème RT et SCRIBE de l'armée de l'Air ; Dupuy de Lôme et charges ROEM des bâtiments de la marine.

Les menaces antisatellites par missiles ou armes à énergie dirigée sont régulièrement mises en avant. Au-delà, les sources ouvertes ne permettent pas d'objectiver une analyse de vulnérabilité potentielle de ces moyens, par les contre-mesures électroniques. Quant aux autres systèmes, leur vulnérabilité ne diffère guère de celle des autres plates-formes.

1.1.2 *WLAN des bases et équipements des personnels*

Les réseaux locaux WIFI déployés dans les bases interarmées, terrestres, aériennes ou navales situées en zone urbaine ou péri-urbaine sont potentiellement à la portée d'équipes adverses opérant à faible distance, par exemple mettant en œuvre un réseau de capteurs dispersés, piloté par radio logicielle et disposant des compétences pour décrypter les transmissions surtout si elles incluent des normes civiles comme le 802.11 de nos WIFI. Le degré de criticité de ces vulnérabilités potentielles dépend bien entendu des informations transitant sur ces WLAN. Même si l'usage de ces réseaux est restreint aux informations générales, non-opérationnelles, il peut potentiellement prêter le flanc à des manœuvres d'influence visant les personnels.

Les équipements individuels peuvent constituer une autre source de vulnérabilité. Les efforts importants accomplis dans la dotation de matériels sécurisés, tel le smartphone Auxylium, réduisent mais n'annulent pas les failles potentielles découlant de l'usage d'équipements personnels. En témoignent les efforts de SECOPS entrepris au sein des unités déployées dans les pays baltes qui tendent à montrer que les risques continuent de se poser sur le plan des équipements.

Contrairement aux capacités d'attaque évoquées précédemment, celles de ces WLAN et équipements individuels peuvent tout à fait être détenues par de multiples acteurs stratégiques, y compris non-étatiques, non seulement en OPEX mais aussi sur le territoire national.

1.2 Les forces terrestres

1.2.1 *Les réseaux de communications*

1.2.1.1 Le réseau de théâtre

La dorsale de transmission large bande permettant les échanges d'information entre niveaux 1 (LCC) à 4 (GTIA) reste assurée par la combinaison du réseau de zone RITA 2G et des MILSATCOM, principalement via les stations ASTRIDE jusqu'au PC de GTIA et secondairement via les stations Venus-OTM (*on the Move*) étendant la connexion jusqu'au sous-GTIA. Ce dispositif serait potentiellement vulnérable au brouillage des services GNSS interdisant la synchronisation des transmissions, à condition que celui-ci soit exercé par des stations adverses aéroportées ou postées sur des zones surélevées, rayonnant des puissances de plusieurs KW portant sur plusieurs dizaines de kilomètres. Un R-330 Zhitel pourrait tout à fait entreprendre ce type d'action.

Le réseau radio bas débit en HF Melchior, aux élongations stratégiques, offre une solution de complément, laquelle est cependant vulnérable, plus encore, aux capacités de GE comme celles alignées par les Russes, allant du Mourmansk BN jusqu'au Borisoglebsk-2 au niveau tactique.

1.2.1.2 Les réseaux de capillarité

Le réseau de capillarité des niveaux 4 à 7 repose sur le PR4G-VS4 qui doit être incrémentalement remplacé par CONTACT destiné à devenir l'unique moyen de communication V/UHF sol-sol, sol-air et air-air des forces tactiques à l'horizon 2025-2030.

Le brouillage de ce réseau sur la zone de contact briserait non seulement toute cohérence du GTIA Scorpion en privant SICS de sa couche COM, mais également les chaînes fonctionnelles intervenant en appui (ATLAS, SITALAT, etc.). Même un brouillage partiel peut obtenir des effets disruptifs. L'un des défis de SICS et de l'agrégation de la SITAC sur SIA au niveau brigade réside dans la bande passante, insuffisante pour faire remonter en temps réel tous les éléments de cette situation. Des attaques en réseau visant à ralentir les échanges pourraient donc avoir

un effet de congestion disruptive sur le plan opérationnel. Cela étant, il est possible que cette contrainte soit levée avec les capacités de gestion du spectre proposées par CONTACT. Une autre action consisterait à exercer un **« harcèlement électronique »** poussant les systèmes à utiliser en permanence leur technique de contre-contre-mesures, gourmande en énergie, épuisant par ce biais rapidement les batteries.

À court/moyen terme, seuls les Russes avec un système comme le Borigoglebsk-2 seraient potentiellement en mesure de mener ce type de mode d'action si l'on se fie aux bandes de fréquences concernées. Quant à la potentialité de vulnérabilité à ces capacités, il est intéressant de se référer à l'exemple américain, bien documenté (voir annexe 2).

1.2.2 Les capteurs

Les systèmes de drone tactique (SDT) peuvent être l'objet, potentiellement, d'attaques électroniques du signal GNSS ou de **la liaison en ligne de vue.** Cependant, cette dernière opère en bande Ku[74], assez directionnelle, ce qui complique l'attaque. Elle n'est potentiellement vulnérable qu'au petit nombre de systèmes russes Krasukha-4. Ces effets interdiraient potentiellement l'emploi des drones privant ainsi les échelons tactiques 2-3-4 de ROIM.

Les radars de surveillance comme le RASIT ou à l'avenir le MURIN, ainsi que les radars de mise en place des tirs d'artillerie RATAC pourraient être vulnérables à un brouillage aéroporté et au brouillage GNSS qui dégraderait leurs horlogeries.

1.2.3 Navigation et positionnement

Le brouillage des services GNSS, outre les effets sur le positionnement et la navigation, **ne permettrait plus le *Blue Force Tracking* (BFT)** augmentant le risque de tirs fratricides. Il perturberait les appuis comme par exemple le CAS dans des situations fortement imbriquées (nécessitant la transmission du BFT par serveur CID), surtout s'il est combiné avec un brouillage des communications radio entre le Joint Terminal Attack Controller et l'aéronef.

1.2.4 Conclusions

Le problème le plus critique pour le système de force terrestre pourrait résider dans la densification des capacités d'attaque électronique contre les transmissions des échelons tactiques les plus bas, susceptibles d'entraver la conduite de la manœuvre au contact et de ses appuis. Comme nous l'avons vu en première partie, ces capacités restent encore l'apanage des grandes puissances mais pourraient partiellement se diffuser à l'avenir dans les appareils militaires des puissances régionales. Bien entendu, avec les capacités de surveillance et d'attaque du 54ème RT qui seraient intégrées dans le bataillon multi-capteurs, ses feux dans la profondeur et l'aéro-combat, l'armée de Terre dispose théoriquement des moyens de neutraliser les brouilleurs adverses. Intervient cependant ici la question de la masse de moyens disponibles, dans la mesure où l'ensemble de ces capacités au volume compté, voire « échantillonnaire », devrait en même temps réaliser de multiples autres missions d'appui contre les éléments adverses.

En outre, la congestion du spectre EM notamment en zone urbaine affecterait en premier lieu les forces terrestres.

1.3 La composante aérienne

1.3.1 Les communications

Partant de l'idée que le système de commandement et de conduite des opérations aériennes sur le territoire national bénéficie de transmissions filaires ou hertziennes réglementées, on concentrera notre propos sur les réseaux de transmission tactiques sur le théâtre, principalement la liaison-16 et les radios.

La liaison 16 et son extension satellitaire JRE, principal réseau de liaison de données tactiques des opérations aériennes, **est présentée comme très résistante aux CME actuelles**, en raison de son chiffrement, de ses 77 000 sauts de fréquences/sec, et de la capacité du réseau à se synchroniser sur une base du temps relative (donc sans dépendance au GPS)[75]. De même, les liaisons radio V/UHF en phonie de l'ensemble des appareils bénéficient des **FO à sauts de fréquence Havequick II et SATURN**[76]. Le brouillage du GPS pourrait cependant interdire à une plate-forme la synchronisation de ces transmissions. Enfin, **la connectivité accrue dont vont bénéficier les Rafale standard F4** avec la liaison SATCOM chiffrée et les radios utilisant la nouvelle forme d'onde FO3D directionnelle semble aller dans

le sens des recommandations du *Defense Science Board* du Pentagone pour les forces américaines[77].

1.3.2 Les capteurs

Les MQ-9 Reaper constituent la principale capacité ISR aéroportée de l'armée de l'Air. Potentiellement, le système peut être affecté de plusieurs façons (hormis la liaison radio évoquée plus haut). Le brouillage des GNSS affecterait la navigation de l'appareil. L'attaque peut aussi porter sur la liaison par SATCOM en bande Ku ou celle en ligne de vue, en bande C, plus simple théoriquement. Cependant, l'armement des drones implique le chiffrement de ces liaisons, de nature à préserver d'une usurpation. Enfin, il est possible d'envisager le brouillage du radar de surveillance Lynx, là encore par des systèmes tels que le Krasukha-4. À noter cependant que le directeur des tests et évaluation du Pentagone, pourtant très critique à l'égard du MQ-9 Block 5, ne mentionne à aucun moment une quelconque vulnérabilité EM / cyber, un critère de test pourtant très présent dans ses évaluations[78].

Les radars des AWACS de l'armée de l'Air et des E-2 de l'aéronavale peuvent être quant à eux la cible des Krasukha-2 dont c'est la mission principale.

1.3.3 Navigation et positionnement

La plupart des plates-formes et des armements guidés de précision repose sur l'emploi de centrales inertielles garantissant la permanence de la navigation et le recalage du positionnement par GNSS. En la matière, il apparaît que le recours au signal Galileo en combinaison du GPS n'offrirait pas de précision ni de protection supplémentaires contre le brouillage. Il permet en revanche de limiter les risques d'usurpation du signal civil.

L'interdiction du recalage GPS aurait pour principal effet de dégrader la précision du tir sur coordonnées (*Bomb on Coordinates*, BOC) tout particulièrement pour les armements à longue portée comme le SCALP ou même les A2SM. Des tests du MIT ont ainsi montré qu'une arme de précision tirée à plus de 60 MN, dotée d'un système GPS/INS, voyait son cercle d'erreur probable se dégrader rapidement pour atteindre 100 m lorsque le brouillage atteint 10 watt[79]. L'usurpation du signal reste également une menace potentielle. Cependant, la vitesse et l'évolution des mobiles ne facilitent pas la mise en œuvre de cette tactique. **Le brouillage des GNSS est donc de nature soit à limiter la précision soit à restreindre les portées d'engagement pour conserver cette précision, donc à limiter les capacités de tir à distance de sécurité de notre puissance aérienne**.

Enfin, des systèmes comme le Rtut-BM, censés neutraliser les fusées de proximité de nos munitions, seraient en mesure de protéger des objectifs sensibles contre notre ciblage.

1.3.4 Conclusions

Pour notre composante aérienne, le problème central réside dans le modèle russe et sa prolifération éventuelle. Il consiste à intégrer une GE à longue portée dans la bulle d'interdiction aérienne adverse, susceptible de contrer nos systèmes ISR et de frappes de précision, entravant les opérations d'interdiction ou de suppression des défenses antiaériennes adverses. Cependant, dans les opérations OTAN ou en coalition sous lead américain, l'US Air Force fournirait un volume de moyens permettant de saturer ce type de menace qui reste, même chez les Russes, en quantité limitée.

1.4 La composante navale

1.4.1 Les communications

La force navale continuera de reposer sur des moyens de transmissions redondants :

- les SATCOM comme moyens premiers : Syracuse pour les principales plates-formes (PA, BPC, navires de premier rang, SNA), COMSATCOM SHF pour les autres bâtiments, COMSATCOM UHF (Iridium, Thurraya et Inmarsat) pour les échanges en phonie ;
- les réseaux de Transmission en l'Air à destinataires Multiples (TRAM) permettent des échanges phonie et messagerie ACP-127 en HF avec la terre ou entre bâtiments, ainsi que les réseaux tactiques de théâtre assurant les liaisons VHF entre bâtiments, essentiels pour assurer l'interopérabilité avec les navires alliés ;
- les liaisons VLF pour les sous-marins en plongée[80].

L'attaque des SATCOM, directe ou via brouillage GNSS, telle que décrite précédemment, aurait donc

pour effet de limiter les transmissions aux moyens bas débit n'autorisant que les échanges des éléments essentiels de commandement, interdisant par exemple la réception de données ISR volumineuses nécessaires à la projection de force. Là encore, l'exigence de l'action en ligne de vue ne rend ce type d'attaque envisageable, en haute mer, que par une puissance aérienne ou de surface que seules la Russie et la Chine peuvent aligner, au moins à court-moyen terme. L'environnement littoral apparaît, en revanche, nettement plus riche en menaces de dégradation de ces transmissions, non seulement SATCOM mais aussi VHF, qu'elles proviennent de bâtiments légers ou de sites côtiers. Enfin, la liaison-11, toujours en usage pour assurer l'interopérabilité avec les marines non dotées de LDT récentes, présente des vulnérabilités bien identifiées et sera avantageusement remplacée par la liaison-22 présentée comme aussi robuste que la L16[81].

1.4.2 Les capteurs

Les capteurs des bâtiments recouvrent principalement les radars, les moyens MSE et les baies COMINT qui viendront renforcer, au cours de la prochaine décennie, les Systèmes de Drone Aérien Marine. La problématique des distances d'attaque contre ces dispositifs se pose comme dans les cas précédents. L'attaque directe des radars semble compliquée étant donnée la sophistication des dispositifs récents à balayage électronique. Celle, indirecte, par brouillage GNSS est peut-être plus critique. Combiné à l'emploi de missiles hypervéloces (actuellement supersoniques et sans doute hypersoniques dans 10 ans), ces attaques pourraient parvenir à des résultats décisifs en combat naval. Elles auraient également pour effet de priver non seulement la force navale mais aussi potentiellement la force déployée d'une partie de sa couverture antiaérienne et antimissile.

1.4.3 Navigation et positionnement

Il n'est pas évident que le brouillage des signaux de GNSS présente un niveau de criticité pour la navigation des bâtiments, notamment pour les plus sophistiqués qui disposent de centrales inertielles comme la SIGMA 40D, extrêmement précises. La problématique de la navigation et du guidage des missiles de croisière naval face à des menaces de ce type, laquelle est en revanche bien réelle, se rapproche de celle des armements air-sol évoqués supra.

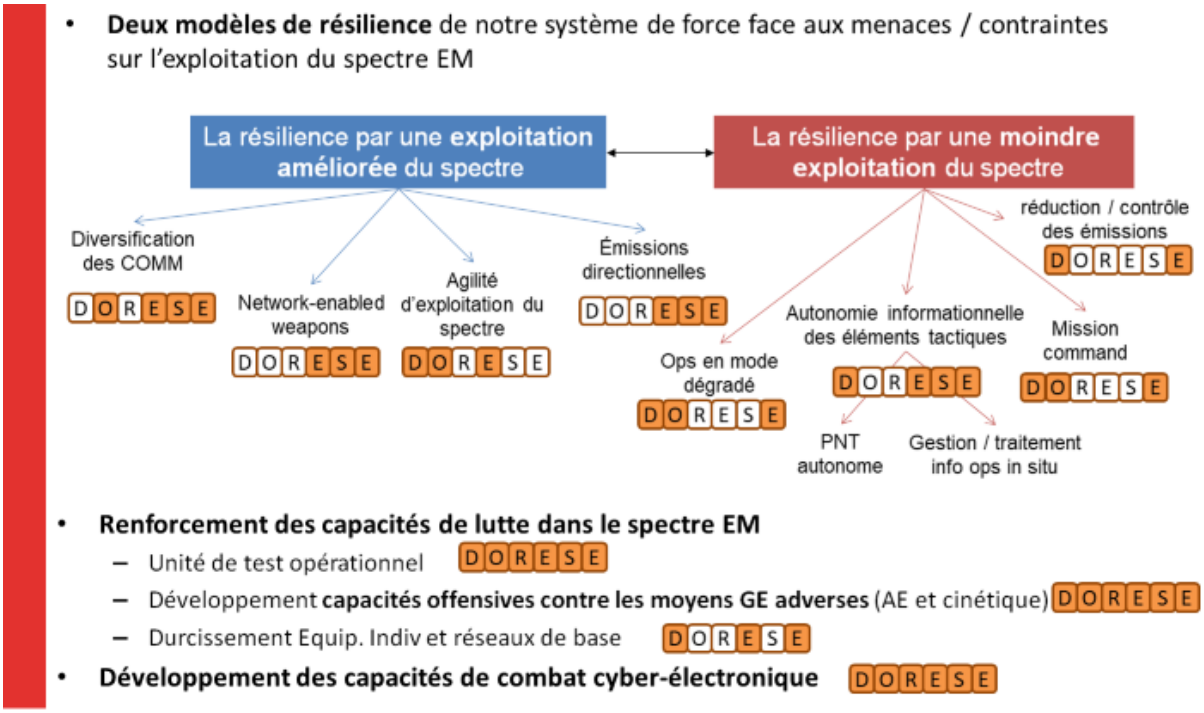
1.4.4 Conclusions

Pour la composante navale, la dégradation de l'environnement EM semble se poser selon deux problématiques différentes. La première est celle du combat naval hauturier et concerne le haut du spectre, face aux plus grandes puissances, les seules à disposer des capacités aériennes et navales nécessaires. La seconde est celle des opérations en zone littorale, notamment des opérations amphibies. Nos forces navales pourraient y faire face non seulement à l'ensemble des menaces de GE contre leurs moyens de transmission et de télédétection mais aussi aux effets de congestion du spectre EM qui affectent les forces terrestres.

1.5 Le cas des opérations spéciales

Les opérations spéciales bénéficient probablement du RTRAN de Syracuse. Cependant, les opérateurs utilisent également, par exemple dans les missions d'appui aérien rapproché, des moyens comme la radio par satellite PRC-117/BGAN, un système présentant lui aussi des vulnérabilités. L'implantation préalable d'un malware pourrait provoquer l'interruption du service lorsque l'opérateur pénètre dans une zone donnée[82]. Le brouillage GNSS serait plus problématique encore pour l'infiltration, l'exfiltration et les opérations débarquées des personnels qui manquent d'alternatives de P/N contrairement aux plates-formes[83].

2. Les implications capacitaires DORESE



Les recommandations capacitaires proposées ici sont présentées *in abstracto* des mesures prises par nos institutions.

2.1 Doctrine

Il est proposé de rajouter une aptitude à celles listées par la *Revue stratégique* de 2017. Elle pourrait être formulée ainsi **: « mener des actions dans le spectre électromagnétique »** ou **« obtenir et conserver la supériorité dans l'environnement électromagnétique »**.

Les doctrines prescrivant les modalités d'exploitation du spectre EM pourraient **préciser les axes permettant de réduire notre vulnérabilité aux efforts de guerre électronique adverses** tels que, par exemple, les pratiques de contrôle des émissions des SIC (EMCON) ou encore d'emploi « *low-to-no power* » de nos capteurs dans la détection et la contre-détection.

La doctrine pourrait également préciser les modalités de manœuvre interarmées, de **neutralisation non seulement électronique mais également cinétique** des capacités d'attaque électronique adverses.

La résilience à ces menaces plaide, notamment dans le milieu terrestre, pour un développement accru de **l'autonomie des échelons tactiques** selon le principe du *« mission command »*. Le travail doctrinal sera particulièrement critique pour assurer la cohérence entre cette autonomie et les mesures de coordination qu'impliquent nos approches visant la convergence des actions entre effecteurs.

Les opérations terrestres en mode dégradé peuvent également être envisagées selon une logique de **différenciation des unités au contact et en appui,** combinant des unités autonomes, exploitant moins le spectre, et des unités de décision, opérant selon la doctrine Scorpion, plus efficaces mais vulnérables[84].

La doctrine pourrait être complétée par **l'inclusion du cyber tactique**.

Les armées pourraient enfin étudier comment **combiner les exigences d'attribution fixe des fréquences qui leur sont imposées avec les possibilités de la gestion dynamique du spectre**.

2.2 Organisation

Le rapport de force équilibré avec une force adverse puissante dotée de nombreux appuis feu et électroniques plaide pour **une démultiplication des capacités d'attaque électronique actuellement mises en œuvre uniquement au sein du 54ème RT et secondairement de l'armée de l'Air**.

En complément des capacités de la DGA Maîtrise de l'information, la création d'une **petite unité** à vocation interarmées **type Red Team d'attaque cyber-électronique dédiée aux tests opérationnels de vulnérabilité** de nos capacités d'exploitation du spectre, pourrait être évaluée, à l'instar de ce que l'US Army a entrepris dans ses *Network Integrated Evaluation* (NIE) testant et validant ses nouvelles architectures de réseaux[85].

2.3 Recrutement

Cette unité interarmées de tests pourrait intégrer, en complément des militaires, des **personnels civils spécialistes** permettant d'améliorer l'analyse des menaces cyber-électroniques.

2.4 Équipements

La résilience contre les menaces de guerre électronique pourrait passer tout d'abord par des équipements permettant une **exploitation améliorée du spectre** :

- **la diversification des SATCOM par le recours aux nouvelles constellations** COMSATCOM en orbite moyenne, comme O3b, qui offrent d'ailleurs des performances très supérieures à celles des SATCOM en orbite géostationnaire ;
- **le développement d'émissions directionnelles** analogues aux solutions envisagées par General Dynamics pour réduire la vulnérabilité du WIN-T Inc.2[86] et la poursuite du **développement des capteurs et moyens de communication à basse probabilité de détection / d'interception ;**
- **Le développement des *Network Enabled Weapons* (NEW)** air-surface reposant sur la L16 permettant de contourner la dégradation de navigation générée par le brouillage des GNSS.

Les solutions peuvent en complément relever **d'une moindre exploitation du spectre**, afin de réduire la surface d'exposition à la menace. Au niveau des équipements, cette approche repose avant tour sur **le développement de l'autonomie informationnelle des éléments tactiques** incluant d'une part **la poursuite des recherches d'alternatives PNT aux GNSS** (voir annexe 4), d'autre part un recours au réseau de communication limité aux données « de recalage » les plus critiques, grâce aux progrès à coût constant de l'informatique embarquée (stockage des données, traitement de l'information, etc.) et, à l'avenir, de l'intelligence artificielle.

Qu'il s'agisse de l'exploitation du spectre ou de la GE, nos forces tireraient profits de **se doter de radios cognitives** permettant une gestion dynamique du spectre EM.

L'auteur comprend que la CUGE sera un instrument de surveillance électronique. Si tel est bien le cas, il serait nécessaire de la compléter par une **charge d'attaque cyber-électronique aéroportée** en mesure d'attaquer les réseaux adverses.

Il pourrait être intéressant de poursuivre **l'évaluation de l'apport des capteurs abandonnés à l'aune des nouvelles technologies de l'IOT**, notamment au profit des opérations spéciales.

Enfin, la protection contre les menaces cyber-électroniques pesant sur les WLAN des bases et équipements personnels, probablement la plus diffuse, **plaide pour l'emploi le plus systématique d'équipements durcis dédiés**, au-delà de la stricte application des mesures de SECOPS.

2.5 Soutien

Les recommandations de soutien s'inscrivent en complément de celles des autres domaines. À noter plus spécifiquement que la résilience du système de force dans un environnement EM contesté passe par un **soutien significatif en énergie (batteries, etc.) des éléments tactiques**.

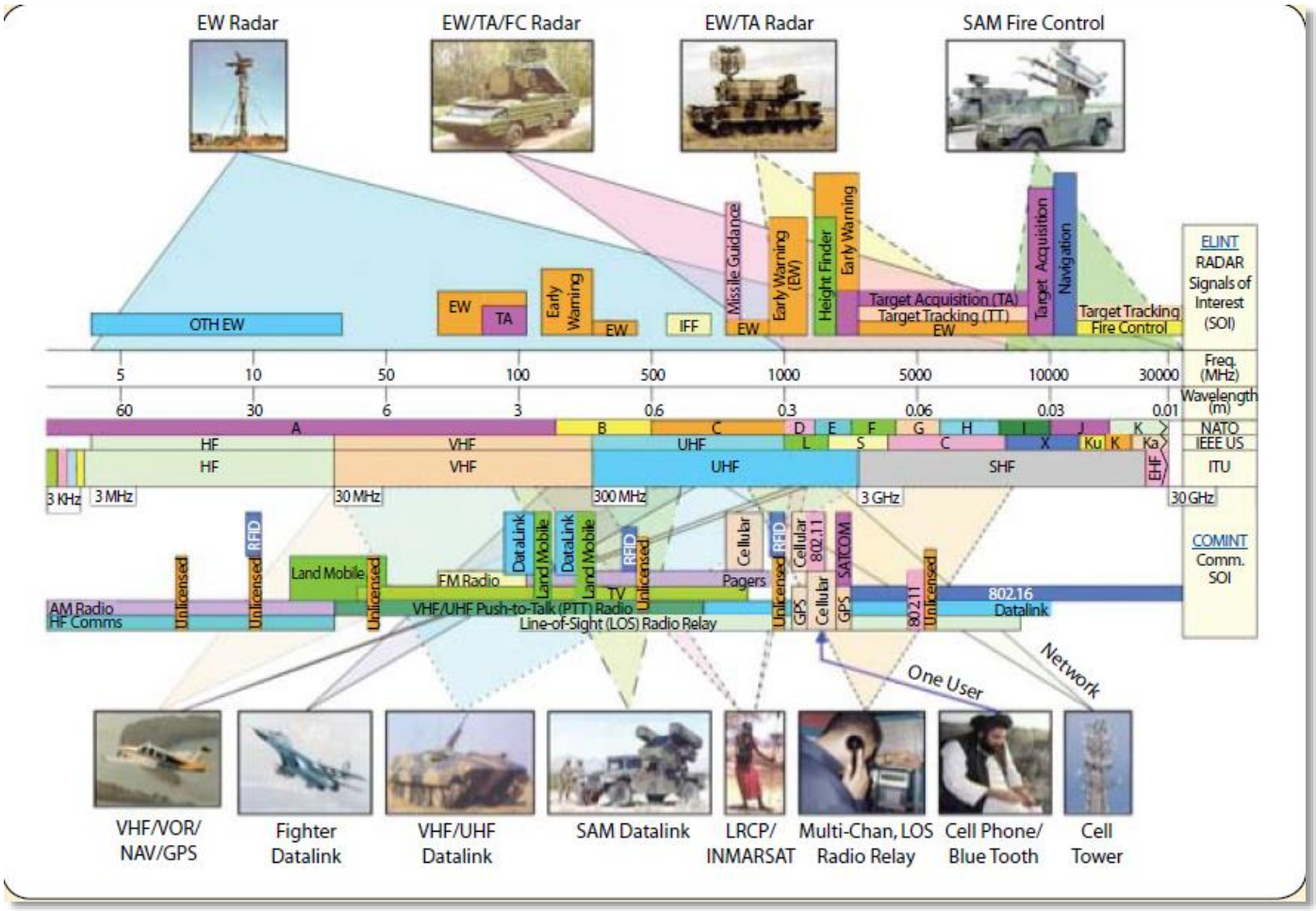
2.6 Entraînement

Nos forces pourraient **multiplier les exercices sans GNSS, sans SATCOM et en situation de EMCON**, à l'instar de ce que pratiquent de nouveau les forces américaines, notamment la Navy qui y voit une composante essentielle de sa vaste approche d'*Electromagnetic Maneuver Warfare*[87].

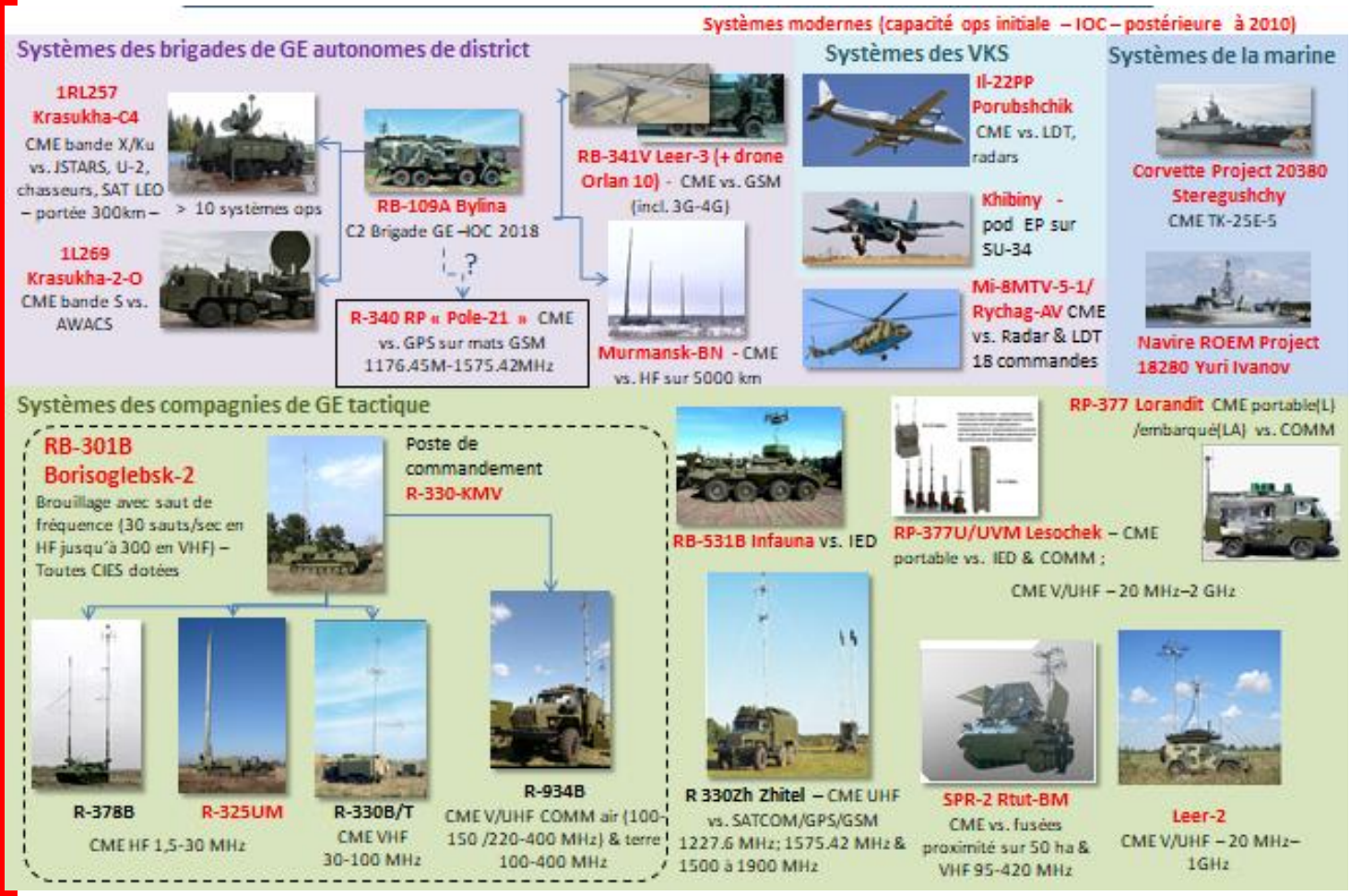
Les recommandations d'entraînement vont de pair avec celles concernant la doctrine : **manœuvre offensive de neutralisation des moyens d'attaque électronique, autonomie des échelons tactiques, éventuellement différenciation des unités selon leur degré de vulnérabilité**.

ANNEXE 1 – LE SPECTRE ÉLECTROMAGNETIQUE

Source : Loren Thompson, *Next Generation Jammer: Essential Protection in the Digital Age*, Lexington Institute, December 2010, p.2



ANNEXE 2 : SYSTÈMES DE GUERRE ÉLECTRONIQUE DES FORCES RUSSES



ANNEXE 3 : LA REMISE À PLAT DE L'ARCHITECTURE DE TRANSMISSION DE L'US ARMY

L'US Army vient de remettre à plat la stratégie de modernisation de ses réseaux tactiques.

Le WIN-T Inc. 2, la dorsale de communication des forces terrestres permettant le « *networking on the move* », selon une logique de réseau MANET, vient d'être mis en service dans plus de 20 brigades. Il donne certes satisfaction dans les opérations actuelles.

Cependant, entre autres problèmes, il est considéré comme potentiellement vulnérable aux moyens de GE russes par les hiérarques de l'Army, s'adossant à une évaluation de l'Institute for Defense Analyses[88] :

- Il est en effet nettement trop visible pour le ROEM adverse, offrant donc éventuellement des cibles de choix à l'artillerie russe. General Dynamics travaille ainsi fébrilement à trouver des solutions telles que des antennes calibrées pour des émissions plus directionnelles[89].
- En second lieu, au niveau du segment bas du WIN-T équivalent à CONTACT, les nouvelles formes d'onde censées assurer les échanges à haut débit (*Mid-Tier Networking Waveform* et *Soldier Radio Waveform*) affichent une portée effective de quelques kilomètres, trop faible pour assurer une connectivité entre le PC bataillon et ses compagnies et entre ces compagnies, pouvant être distants de plus de 10 km.

L'Army souhaite donc que les nouveaux postes radio puissent continuer à recourir à la FO SINCGARS « classique ». Or, il semble que l'intégrité de cette radio logicielle, considérée comme sûr depuis son introduction à la fin des années 1990, ne soit pas forcément garantie[90]. Le SINCGARS est ainsi donné à environ 100 sauts de fréquence/sec contre 300 pour le système de brouillage Borisoglebsk[91]. S'il en est ainsi du SINCGARS, il est possible qu'un réseau PR4G, contemporain de ce système américain, présente les mêmes vulnérabilités.

ANNEXE 4 : AXES DE RECHERCHE AMÉRICAINS SUR LA RÉSILIENCE DU PNT

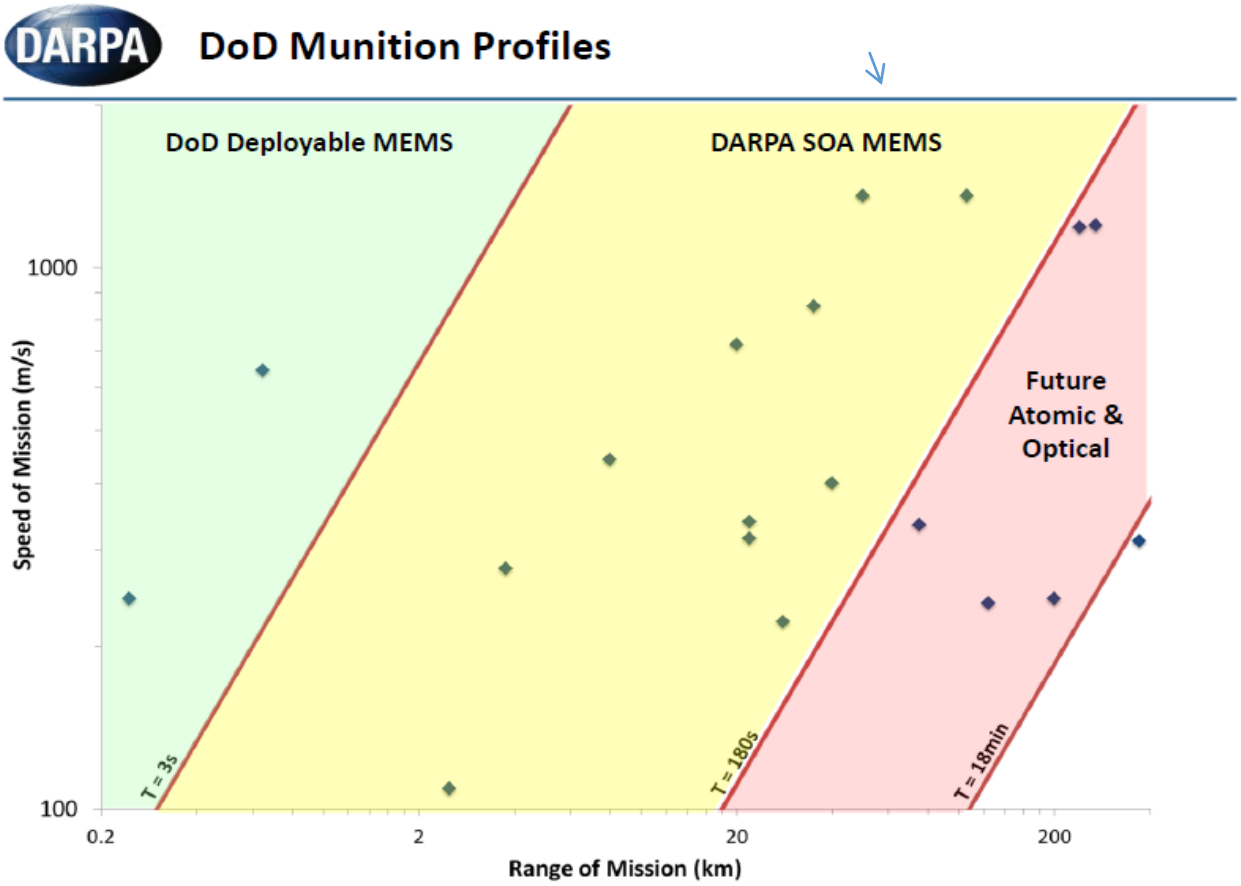
La stratégie américaine de résilience de la capacité PNT poursuit de multiples axes :

- Bien entendu, la **modernisation du GPS** avec l'arrivée du nouveau M Code (code militaire) sur les satellites Block II qui sera suivi du renforcement du signal sur les Block III.
- **La combinaison des sources de géolocalisation**, laquelle peut inclure de multiples signaux d'opportunité : SATCOM commerciaux, émissions radio voire même télévision, etc. Dans le cadre du programme *Adaptable Navigation Systems* (AND), la DARPA a ainsi testé de nouveaux algorithmes de fusion de données provenant de ces signaux et des centrales inertielles et de reconfiguration rapide du traitement de ces données[92].
- **La R&D sur les centrales INS**. Le programme de miniaturisation d'horloge atomique *Atomic Clocks with Enhanced Stability* (ACES) de la DARPA cherche à révolutionner les capacités de timing. En ce qui concerne les accéléromètres et les gyroscopes composant les unités de mesures inertielles (IMU) de ces centrales, les centres travaillent à améliorer les performances des technologies de microsystèmes électromécaniques (MEMS) qui n'atteignent pas encore le niveau des unités actuelles, et le facteur SWAP ainsi que le coût des technologies optiques classiques.
- **Dans le domaine des munitions air-sol,** le programme *Precise Robust Inertial Guidance for Munitions (PRIGM)/ Navigation-Grade Inertial Measurement Unit (NGIMU)* a pour objectif de parvenir en 2019 à une solution, expérimentable en vol, de micro-puce permettant à une munition air-sol planante (comme les *Small Diameter Bombs*) de conserver un CEP de 10 m sur un vol de trois minutes, couvrant ainsi l'essentiel des cas de figure tactique. **Pour les missiles balistiques ou hypersoniques**, la DARPA et des centres tels que l'AFRL travaillent en parallèle sur les technologies d'IMU nucléaires, telles que l'interférométrie atomique et la résonnance magnétique nucléaire. Elles offriraient les performances idéales pour ces systèmes, meilleures que le GPS. Cependant, les recherches en sont encore au stade du laboratoire, avec un facteur SWAP prohibitif. Les programmes menés par la DARPA en 2014 montrent que ces technologies ne pourraient aboutir à des solutions susceptibles d'être opérationnalisées que dans la décennie 2030[93].

On peut donc anticiper que les plates-formes comme le plus gros des munitions air-sol pourront progressivement s'affranchir du guidage GPS durant la prochaine décennie. Le CERDEC de l'Army, entre autres, poursuit de multiples pistes combinant ces axes technologiques pour assurer également le positionnement et la navigation des combattants débarqués[94]**.**

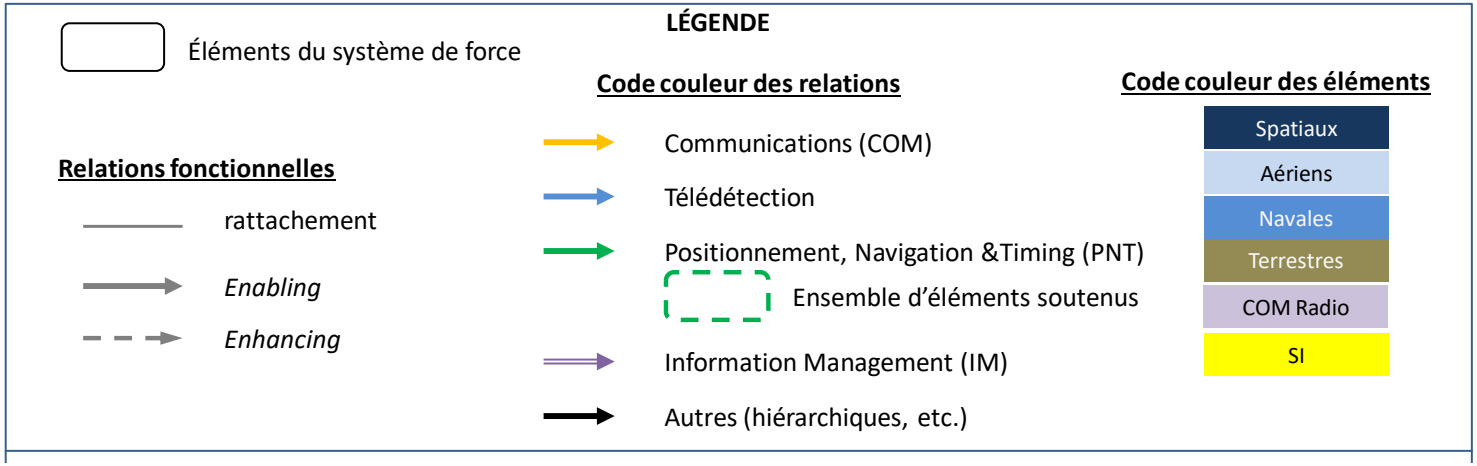
MATURITÉ DES TECHNOLOGIES DES CENTRALES DE MESURES INERTIELLES ET MUNITIONS HYPERSONQUES

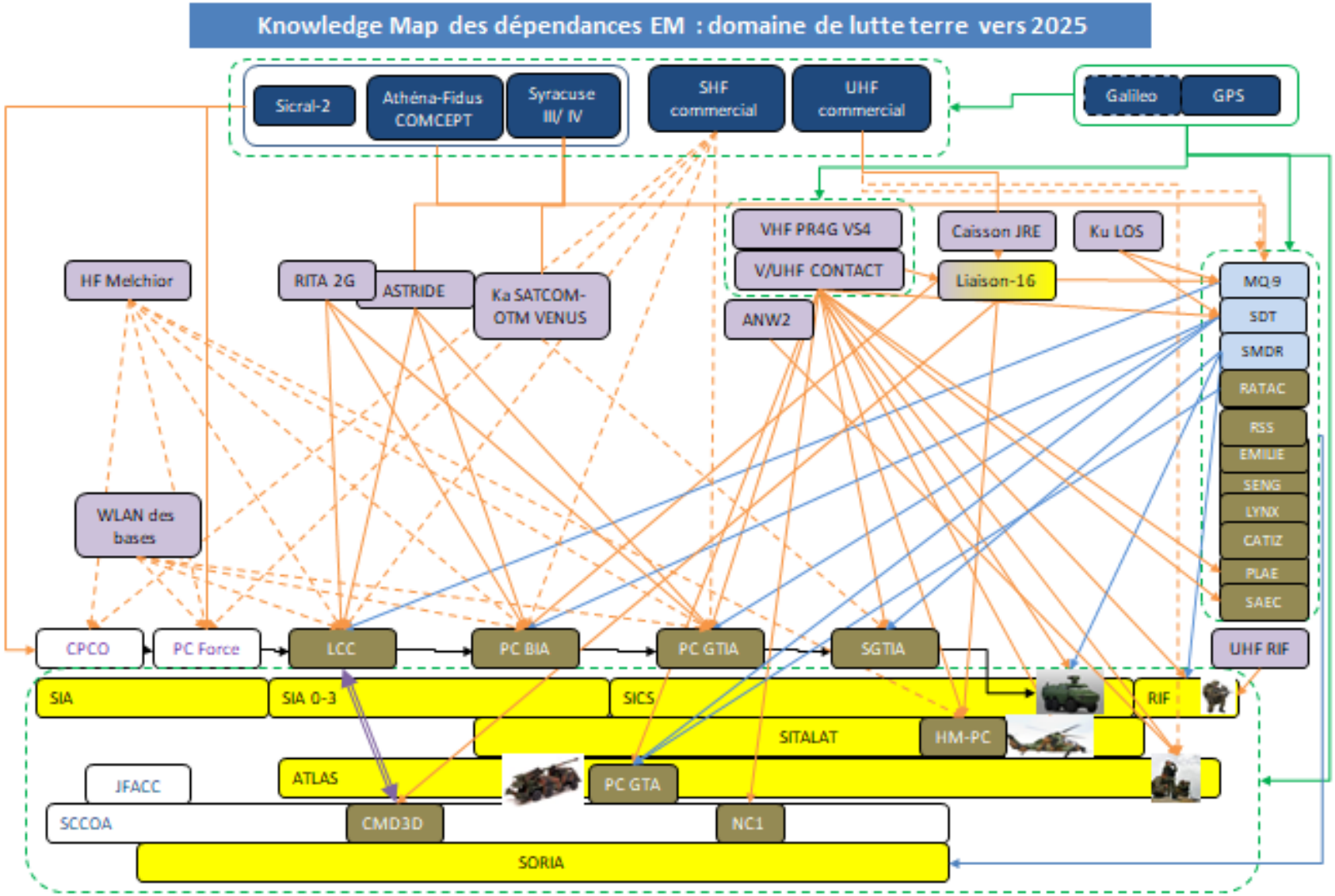
Adapté de Dr. Robert Lutwak, Program Manager, Microsystems Technology Office, DARPA, *Micro-Technology for Positioning, Navigation, and Timing Towards PNT Everywhere and Always*, présentation, Space-Based Positioning Navigation & Timing National Advisory Board, Fourteenth Meeting, Washington, DC, December 10, 2014

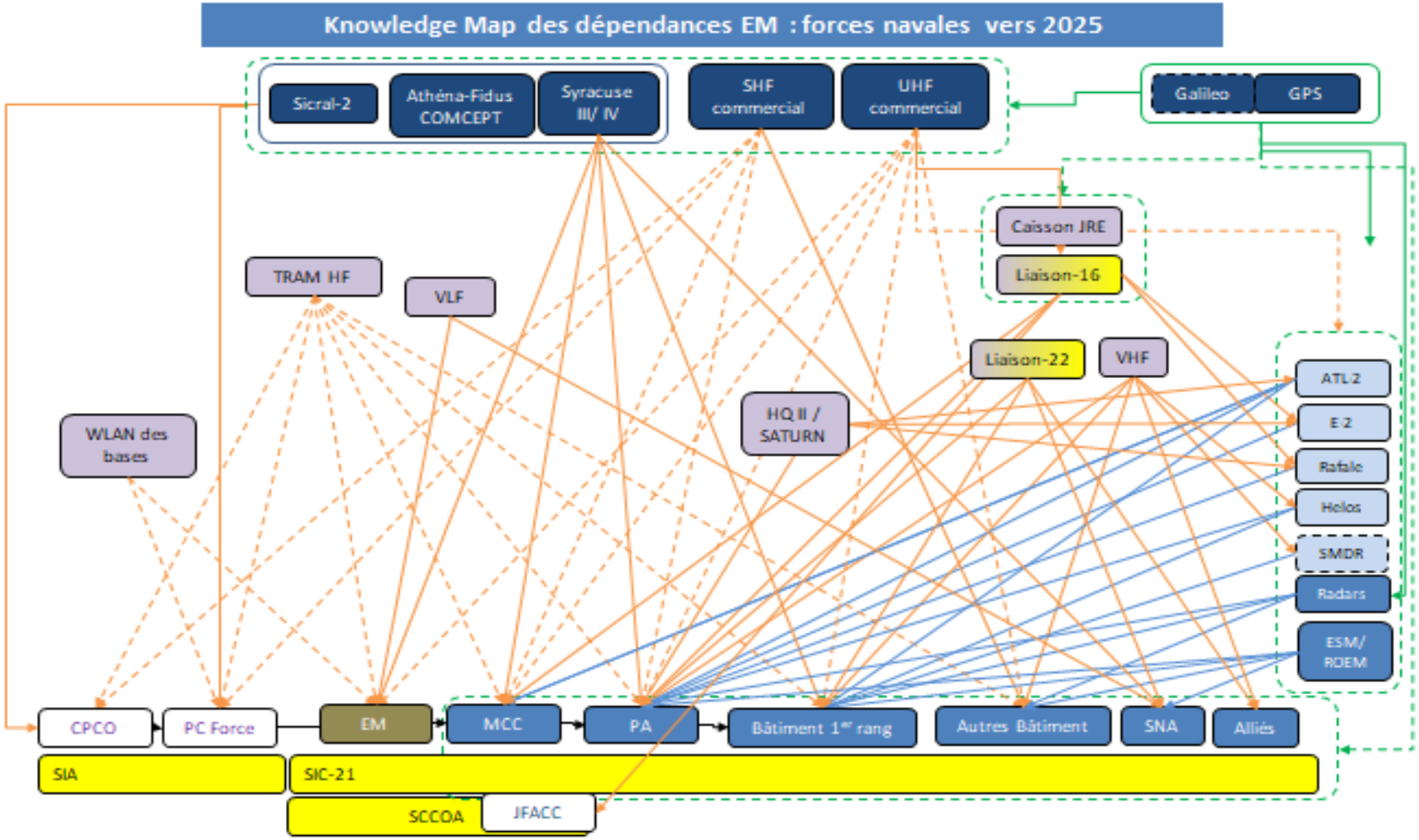


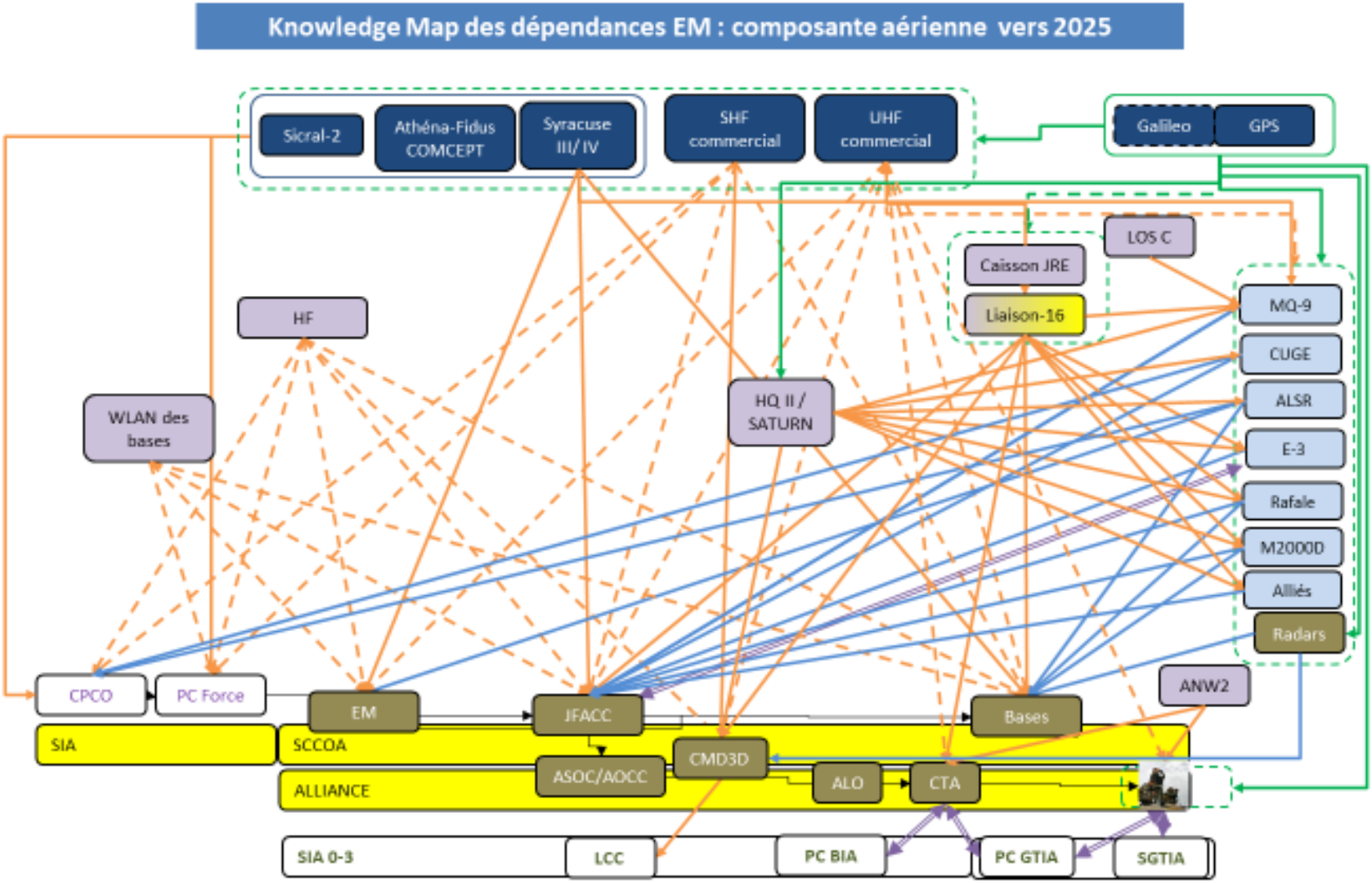
ANNEXE 5 : LES KNOWLEDGE MAP

L'analyse proposée en second partie se fonde partiellement sur une méthode d'analyse des dépendances et des vulnérabilités critiques dites « inter-domaines » (terre, air, mer, espace), développée dans le cadre de l'expérimentation multinationale MNE7 en 2011-2012, visant à proposer un complément à la méthode de planification opérationnelle de la COPD de l'OTAN. Cette méthode consiste en gros à réaliser une analyse systémique des fonctions PNT, communications, télédétection et gestion de l'information de leurs liens avec les autres éléments des forces amies. Elle comprend deux étapes principales : (1) l'élaboration de « *Knowledge Map* » cherchant à reconstituer les relations de dépendance entre les systèmes, par fonctions opérationnelles, (2) compte tenu des menaces connues, l'analyse des chaînes d'effets envisageables créées par l'attaque sur les systèmes d'exploitation du spectre et allant jusqu'aux *Mission Essential Tasks* fixées à la force. Dans la présente note, le premier volet de cette méthode est exploité, partiellement, sur un plan générique, par milieu. Dans la mesure où les dépendances vont varier d'un engagement à l'autre, seules les relations « d'enabling » et « d'enhancing » génériques sont envisagées ici.




Knowledge Map des dépendances EM : domaine de lutte terre vers 2025
Sicral-2
Athéna-Fidus COMCEPT
Syracuse III/ IV
SHF commercial
UHF commercial
Galileo
GPS
VHF PR4G VS4
V/UHF CONTACT
Caisson JRE
Ku LOS
Liaison-16
HF Melchior
RITA 2G
ASTRIDE
Ka SATCOM-OTM VENUS
ANW2
MQ 9
SDT
SMDR
RATAC
RSS
EMILIE
SENG
LYNX
CATIZ
PLAE
SAEC
WLAN des bases
CPCO
PC Force
LCC
PC BIA
PC GTIA
SGTIA
UHF RIF
SIA
SIA 0-3
SICS
RIF
SITALAT
HM-PC
ATLAS
PC GTA
JFACC
SCCOA
CMD3D
NC1
SORIA


Knowledge Map des dépendances EM : forces navales vers 2025
Sicral-2
Athéna-Fidus COMCEPT
Syracuse III/ IV
SHF commercial
UHF commercial
Galileo
GPS
Caisson JRE
Liaison-16
TRAM HF
VLF
Liaison-22
VHF
HQ II / SATURN
WLAN des bases
ATL2
E 2
Rafale
Helos
SMDR
Radars
ESM/ ROEM
CPCO
PC Force
EM
MCC
PA
Bâtiment 1er rang
Autres Bâtiment
SNA
Alliés
SIA
SIC-21
SCCOA
JFACC


Knowledge Map des dépendances EM : composante aérienne vers 2025
Sicral-2
Athéna-Fidus COMCEPT
Syracuse III/ IV
SHF commercial
UHF commercial
Galileo
GPS
LOS C
Caisson JRE
Liaison-16
HF
WLAN des bases
HQ II / SATURN
MQ-9
CUGE
ALSR
E-3
Rafale
M2000D
Alliés
Radars
ANW2
CPCO
PC Force
EM
JFACC
Bases
SIA
SCCOA
CMD3D
ASOC/AOCC
ALO
CTA
ALLIANCE
SIA 0-3
LCC
PC BIA
PC GTIA
SGTIA

RÉFÉRENCES

[1] « Edouard Branly, la naissance de la télégraphie sans fil » et « Les débuts de la radio dans la marine », ECE Ecole d'ingénieurs, non daté, *Un précurseur oublié de la T.S.F., Camille Tissot (1868-1917)*, Association Locmaria Patrimoine, non daté, locmaria.patrimoine.pagesperso-orange.fr/tsf.pdf, « Gustave Ferrié », *les Actus DN*, http://www.janinetis-sot.fdaf.org/jt_ferri%C3%A9.htm

[2] Que la doctrine française définit comme « *l'environnement opérationnel dans lequel les effets électromagnétiques sont réalisés* ».

[3] DIA 3.6 sur la guerre électronique d'octobre 2017 et *PIA-3.6.1 Maîtrise de l'environnement électromagnétique*, N°0-10786-2016/ALFAN/CEM/DR du 06 avril 2016 – documents DR.

[4] « La Guerre électronique a 100 ans - en brouillant les télégrammes », *Etoile Rouge*, Traduction effectuée par le Centre de Préparation Opérationnelle de la Guerre Electronique, CPOGE, 15 avril 2004, Association de la guerre électronique de l'armée de terre, Messager n°4 - mars 2005, tiré du site, https://groups.google.com/forum/#!msg/guerrelec/H2JHglA-ZOw4/bdfFhIN2TGIJ

[5] PIA-3.6 *Politique de la guerre électronique*, N°1812/DEF/EMA/EMP.1/NP du 23 décembre 2008, p. 6.

[6] Ibidem.

[7] Sydney J. Freedberg Jr "US Has Lost 'Dominance In Electromagnetic Spectrum': Shaffer", *Breaking Defense*, September 03, 2014.

[8] Kanika Grover; Alvin Lim; Qing Yang, « Jamming and Anti-jamming Techniques in Wireless Networks: A Survey », Int. J. Ad Hoc and Ubiquitous Computing, 2014 Vol.17, No.4, pp. 197 - 215

[9] Mahmood Enayat, *Satellite Jamming In Iran: A War Over Airwaves*, A Small Media Report, November 2012, p. 27 http://www-tc.pbs.org/wgbh/pages/frontline/tehranbureau/SatelliteJammingInIranSmallMedia.pdf

[10] Entretien avec un ingénieur spécialisé sur les transmissions de données et ayant œuvré sur un programme de drone proposé par un industriel français.

[11] George T. Schmidt, *Navigation Sensors and Systems in GNSS Degraded and Denied Environments*, NATO Science and Technology Organization, STO-EN-SET-197, 2013, p. 1-6.

[12] Entretien avec les ingérieurs et experts opérationnels d'un industriel spécialiste des GNSS et de la navigation.

[13] JNTC, *DoD Communication Waveform Inventory*, 2017 04 19.

[14] Todd Harrison, *The Future of Milsatcom*, Center for Strategic and Budgetary Assessments, 2013, p. 11, http://www.csbaonline.org/publications/2013/07/the-future-of-milsatcom/ consulté le 5 décembre 2012.

[15] Sydney J. Freedberg Jr., « US Jammed Own Satellites 261 Times; What If Enemy Did? », *Breaking Defense*, December 02, 2015.

[16] Voir le site de l'ANFR, https://www.anfr.fr/gestion-des-frequences-sites/tnrbf/

[17] Anthony Nigara, « Adaptive EW – the Future of Electronic Warfare », *Harris*, Feb 2, 2017.

[18] Christo Cloete*, (Some) EW Trends & Strategic Influences*, présentation, *Electronic Warfare South Africa 2017*, International Conference & Exhibition, 6-8 November 2017 CSIR, Pretoria.

[19] Aymeric Bonnemaison, Stéphane Dossé, *Attention Cyber, Vers le combat cyber-électronique*, Collection Cyberstratyégie, Economica, 2014.

[20] Headquarters of the Army, *FM 3-12 Cyberspace and Electronic Warfare Operations*, 11 April 2017, p. 1-1.

[21] Lire par exemple Ballantyne, S. N. T. (2016) *Wireless Communication Security: Software Defined Radio-based Threat Assessment.* Unpublished MSC by Research Thesis. Coventry: Coventry University.

[22] Entretien avec les ingérieurs et experts opérationnels d'un industriel spécialiste des GNSS et de la navigation.

[23] STO TECHNICAL REPORT TR-IST-077, Cognitive Radio in NATO (La radio cognitive au sein de l'OTAN), Findings of Task Group IST-077, January 2014.

[24] Peter Middleton, « Forecast Analysis: Internet of Things — Endpoints, Worldwide, 2017 Update », Gartner Research, 27 December 2017, https://www.gartner.com/doc/3841268/forecast-analysis-internet-things-

[25] « N-ZERO Envisions “Asleep-yet-Aware” Electronics that Could Revolutionize Remote Wireless Sensors », DARPA, 4/13/2015https://www.darpa.mil/news-events/2015-04-13.

[26] Rick Robinson, « Applying Photonics to Electronic Warfare Challenges », *Research News*, Georgia Institute of Technology, September 20, 2016.

[27] Gp Capt Ashish Gupta, *China’s Claim of Developing “Quantum Radar” For Detecting Stealth Planes: Beyond Scepticism*, Center for Airpower Studies, India, 02 November 2016.

[28] Kamleu Noumi Emeric, « Le radar quantique peut détecter les systèmes de brouillage électroniques », *Tech Connect*, 7 octobre 2013.

[29] USAF Scientific Advisory Board Study, *Utility of Quantum Systems for the Air Force*, Study Abstract, 2015 & G Matich et Dr Paul Kimber, *Quantum technological challenges for defence*, Brief, Cambriidge University, 2014.

[30] Viktor Khudoleev, “Voyska dlya srazheniya v efire” [Troops for combat on airwaves], Krasnaya Zvezda, April 14, 2014, cité par Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025 : Challenging NATO in the Electromagnetic Spectrum*, International Centre for Defence and Security, Estonian Ministry of Defence, September 2017, p. 3.

[31] Maksimilian Dura, « *Electronic Warfare: Russian Response to the NATO’s Advantage? [ANALYSIS]* », blog Defense24, 5 maja 2017, http://www.defence24.com/electronic-warfare-russian-response-to-the-natos-advantage-analysis.

[32] Voyennyy Entsiklopedicheskiy Slovar’” [Military Encyclopaedic Dictionary], Ministerstvo Oborony Rossiyskoy Federatsii, accessed May 19, 2017, cité par Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*, *op. cit,* p. 3.

[33] Andrey Garavskiy, “Svyaz’ reshaet vse” [Communications determine everything], Krasnaya Zvezda, June 4, 2010, cité dans Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*, *op cit,* p. 3. De fait les notions de qualité et de vitesse de l’information sont tout à fait analogues à l’approche théorique du Network-Centric Operations Framework élaboré par l’Office of Force Transformation du Pentagone en 2004

[34] Dr Lester W. Grau, Charles K. Bartles, *The Russian Way of War, Force Structure, Tactics and Modernization of the Ground Forces*, Foriegn Military Office Studies, 2016, p. 291.

[35] « Krasukha-4 v Sirii: god elektronnogo shchita na Khmeymim », *Defence.ru*, October 11, 2016, https://defence.ru/article/krasukha-4-v-sirii-god-elektronnogo-schitanad-khmeimim/ & « V Siriyu pribyli noveyshyye rossiyskiye kompleksy radioelektronnoy bor’by ‘Krasukha-4’ » *Voyennyy Informator*, October 5, 2015, http://military-informant.com/airforca/v-siriyu-pribyilinoveyshie-rossiyskie-kompleksyi-radioelektronnoy-borbyikrasuha-4.html ; « 1Л269 Красуха-2 », *MilitaryRussia.Ru*, 22.11.2014

[36] Michael Peck, « The Crazy Way Russia Could Hijack Your iPhone », *The National Interest*, 5 April 2017.

[37] Andrey Simonov, Denis Khripushin and Mikhail Chikin, “Perspektivy avtomatizirovannogo upravleniya vsoyedineniyakh radioelektronnoy bor’by Vooruzhonnykh Sil Rossiyskoy Federatsii” [Prospects of automated command and control in the formations of electronic warfare of the Armed Forces of the Russian Federation], Materialy ot voysk radioelektronnoy bor’by VS RF No. 1 (2017): 38-39, https://reb.informost.ru/2017/pdf/1-7.pdf, cité dans McDermott, *op cit*, p. 15 &,.http://bastion-karpenko.ru/rb-109a-bylina/

[38] Aleksey Ramm, “Elektronnaya voyna—mify i pravda (Part 1)” [Electronic warfare—myths and the truth], *Voyenno-Promyshlennyy Kuryer,* September 30, 2015

[39] Voir dossier d’A.V.Karpenko “КОМПЛЕКС РАДИОЭЛЕКТРОННОГО ПОДАВЛЕНИЯ (РЭП) КВ И УКВ РАДИОСВЯЗИ ТЗУ РБ-301Б «БОРИСОГЛЕБСК-2» COMPLEX ELECTRONIC COUNTERMEASURES (ECM) HF AND VHF RADIO TZU RB-301B «BORISOGLEBSK-2”, http://nevskii-bastion.ru/borisoglebsk-2/ ВТС «НЕВСКИЙ БАСТИОН», dernière mise à jour 31.03.2018.

[40] « Russia's Air Force received first batch of new Mi-8MPTR-1 electronic warfare helicopters », *Air Recognition*, 12 March 2015.

[41] Piotr Butowski, *2015 Russian Air Force Almanac*, Air Force Magazine, p. 65.

[42] « Project 20380 Steregushchy Class Corvettes », non daté, *Naval Technology*, https://www.naval-technology.com/projects/steregushchy-class/

[43] « In 2016, more than 50 tactical exercises were conducted with the electronic warfare units of the Central Air Defense Forces » (С подразделениями радиоэлектронной борьбы ЦВО в 2016 году проведено более 50 тактических учений), Ministry of Defense of the Russian Federation, 11/11/2016.

[44] McDermott, *op. cit,* p. 7.

[45] Joseph Trevithick, « The Russians Are Jamming US Drones in Syria Because They Have Every Reason To Be », Blog *The War Zone, The Drive*, April 10, 2018 & Alex Hollings, « SOCOM Commander: Russia is using electronic warfare to ‘disable’ SOCOM aircraft over Syria SOFREP Original Content » Foreign Policy, accessible sur le site SOFREP, 04.27.2018, https://sofrep. com/102518/socom-commander-russia-is-using-electronic-warfare-to-disable-socom-aircraft-over-syria/

[46] Dylan Malyasov, « In Syria Spotted «Krasuha-4» Russian Mobile Electronic Warfare Systems », *Defence Blog*, 5, October, 2015 & « Krasukha-4 in Syria_ One Year of Electronic Shield over Hmeymim Airbase », Southfront.org, 12.10.2016, Dylan Malyasov, « In Syria spotted new Russian RB-341V «Leer-3» electronic warfare system », *Defence Blog*, 14, March, 2016.

[47] Vyacheslav Gusarov, « Радиоэлектронная борьба российских террористических сил в начальной фазе военного конфликта в Украине », 20.09.2016, http://sprotyv.info/ru/news/kiev/radioelektronnaya-borba-rossiyskih-terroristicheskih-sil-v-nachalnoy-faze-voennogo & Anonyme, « The tactics of Russian EW formations in the battle of Debaltsevo. "IP" Analytics », *To Inform and to Influence,* 05/01/2017, https://toinformistoinfluence.com/2017/01/22/the-tactics-of-russian-ew-formations-in-the-battle-of-debaltsevo-ip-analytics/

[48] Roger Cliff, *Anti-Access Measures in Chinese Defense Strategy*; Testimony Before the U.S. China Economic and Security Review Commission, RAND Corporation, January 27, 2011.

[49] Deepak Sharma, « Integrated Network Electronic Warfare: China's New Concept of Information Warfare » *Indian Journal of Defence Studies*, Vol 4. No 2. April 2010, pp. 36-49 voir aussi la très bonne fiche wikipédia : https://en.wikipedia.org/wiki/Fourth_Department_of_the_General_Staff_Headquarters_Department

[50] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare*, RR1708, Rand Corporation, 2018.

[51] John Costello, *China's Strategic Support Force: A Force for a New Era*, Testimony to the U.S.-China Economic and Security Review Commission, February 15, 2018 & Kevin L. Pollpeter, Michael S. Chase, Eric Heginbotham, *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*, RR2058Rand Corporation

[52] Mark Pomerleau, « Breaking down China's electronic warfare tactics », *C4ISRNET*, March 22, 2017.

[53] Rick Joe, « J-16D electronic warfare/strike aircraft », Blog *PLA RealTalk*, 6 janv. 2016.

[54] « Chinese Navy gets new electronic warfare aircraft: Report » *The Economic Times*, JAN 22, 2018.

[55] Rick Joe*, op. cit.*

[56] Prepared Statement of Mr. David Chen, Independent Analyst, *China's Advanced Weapons*, Testimony before The U.S.-China Economic and Security Review Commission, February 23, 2017.

[57] « IDF's Electronic Warfare Battalion: the Enemy's Headache », *iHLS*, Dec 30, 2014.

[58] Yaakov Katz, « And they struck them with blindness », *The Jerusalem Post*, 09/29/2010 & Vered Talala, « A Peek into the Top Secret Unit », site de l'armée de l'air israélienne, 02.08.2016.

[59] IISS Military Balance 2016, Anthony H. Cordesman, *After The Storm: The Changing Military Balance in the Middle East*, Bloomsbury, 1993, p. 339.

[60] « Egypt displays South African EW system », *Jane's*, October 17, 2016, repris par le blog Pakistan Defence, file « Egyptian Armed Forces », Page 190.

[61] Dan Williams, « Egyptian jamming of Sinai insurgents disrupts phones in Israel, Gaza », *Reuters*, March 7, 201.

[62] Mahmood Enayat, *Satellite Jamming In Iran: A War Over Airwaves*, A Small Media Report, November 2012, http://www-tc.pbs.org/wgbh/pages/frontline/tehranbureau/SatelliteJammingInIranSmallMedia.pdf consulté le 6 décembre 2012.

[63] « GPS Jammer, GPSJ-25 », Iran Electronics Industries http://www.ieimil.ir/products/gps-jammer-gpsj-25

[64] « The Iranian Army's Drone Jamming 'Electronic Rifle' », *OE Watch*, Foreign Military Studies Office, Jan - Feb 2017, p. 9.

[65] Voir sur cette affaire, les articles de David Cenciotti, blog the Aviationist, https://theaviationist.com/tag/lockheed-martin-rq-170-sentinel/page/7/

[66] Voir par exemple, Anthony H. Cordesman, *The Changing Gulf Balance and the Iranian Threat*, working draft, CSIS, August 3, 2016.

[67] *North Korean Jamming of GPS Systems*, June 2012, TRADOC G-2 Intelligence Support Activity, « North Korea jams South's guided missiles » Blog Defence Forum India, http://defenceforumindia.com/forum/threads/north-korea-jams-souths-guided-missiles.19963/, Kyle Mizokami, « North Korea Is Jamming GPS Signals », *Popular Mechanics*, Apr 5, 2016.

[68] Lale Sariibrahimoglu, « Turkey receives first Koral land-based EW system », *IHS Jane's Defence Weekly*, 25 February 2016 & Dylan Malyasov, « Turkey's newest electronic warfare system spotted near border with Syria », *Defence Blog*, 19, January, 2018.

[69] « The MANDAT-B1E jamming complex », UKROBORONSERVICE". https://en.uos.ua/produktsiya/svyaz-i-asu/46-kompleks-radiopomeh-nazemnim-sredstvam-svyazi-mandat-b1ie

[70] « P-330 » https://ru.wikipedia.org/wiki/%D0%A0-330

[71] Strategic Defence Intelligence, « The Global Electronic Warfare Market 2017-2027 », Summary, December 19, 2017, https://www.giiresearch.com/report/sdi410243-global-electronic-warfare-market.html

[72] CICDE, *Les systèmes d'information et de communication (SIC) en opérations*, Doctrine interarmées DIA-6_SIC-OPS (2014) N° 147/DEF/CICDE/NP du 24 juin 2014, Amendée le 16 janvier 2016, pp. 29-32.

[73] Ruben Santamarta, *A Wake-up Call for SATCOM Security*, IOActive, 2014, pp. 9-11.

[74] Philippe Wodka-Gallien, « Le drone de surveillance longue endurance Patroller™ de Sagem a achevé avec succès sa quatrième campagne d'essais », Communiqué de presse Safran, 06/07/2010.

[75] « Liaison 16 », Wikipédia et Air Land Sea Application Center*, Introduction To Tactical Digital Information Link J and Quick Reference Guide (TADIL J),* June 2000.

[76] Second Generation Anti-Jam Tactical UHF Radio for NATO.

[77] Le résumé de l'étude classifiée du Defense Science Board américain sur la vulnérabilité des réseaux de transmission préconise ainsi, entre autres recommandations : « *The Air Force and Navy Acquisition Executives should accelerate Link-16 enhancements and development of a next generation directional network* ». Defense Science Board, *Task Force on Military Satellite Communication and Tactical Networking*, Executive Summary, p. 3.

[78] Director, Operational Test and Evaluation, « MQ-9 Reaper Armed Unmanned Aircraft System (UAS) », *FY 2017 Annual Report*, January 2018, pp. 269-270.

[79] George T. Schmidt, *Navigation Sensors and Systems in GNSS Degraded and Denied Environments*, NATO Science and Technology Organization, STO-EN-SET-197, 2013, p 1-20.

[80] CICDE, *Les systèmes d'information et de communication (SIC) en opérations, op. cit.*

[81] Idem, p. 35, lire également la bonne synthèse des différentes LDT, Anca Stoica, Diana Militaru, Dan Moldoveanu, Alina Popa, « Tactical Data Link – From Link 1 To Link 22 », Eng. Military Equipment and Technologies Research Agency, "Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 2, pp. 317-322.

[82] Ruben Santamarta, *A Wake-up Call for SATCOM Security*, IOActive, 2014, pp. 9-11.

[83] Lieutenant General Brad Webb, USA AF, *Special Operations in Degraded Environments*, Joint Air & Space Power Conference 2016.

[84] Entretien avec deux stagiaires de cours supérieur interarmes travaillant sur le thème, Ecole militaire, 17 mai 2018.

[85] Director, OperationalTest and Evaluation, « Network Integration Evaluation (NIE) », *FY 2015 Report*, Jan 2016, p. 104.

[86] Kris Osborn, « The U.S. Army's Battlefiield Networks Are Vulnerable to Russian Jamming », Blog *War is Boring*, July 1, 2017.

[87] Voir les différents post d blog *Breaking Defense*, https://breakingdefense.com/tag/electromagnetic-maneuver-warfare/

[88] Courtney McBride, « In new report, Army details network modernization plans », *Inside Defense*, February 02, 2018.

[89] Kris Osborn, « The U.S. Army's Battlefield Networks Are Vulnerable to Russian Jamming », Blog *War is Boring*, July 1, 2017.

[90] Michael Peck, « Electronic Warfare: The Russian Threat No One Is Paying Attention to (Until Now) », Blog The National Interest, February 4, 2018.

[91] Headquarters, Department of the Army, *Field Manual FM 11-32 Combat Net Radio Operations*, Washington, DC, 15 October 1990, p. 4-1.

[92] David Kramer, « DARPA looks beyond GPS for positioning, navigating, and timing », *Physics Today*, October 2014, p. 25.

[93] Dr. Robert Lutwak, Program Manager, Microsystems Technology Office, DARPA, *Micro-Technology for Positioning, Navigation, and Timing Towards PNT Everywhere and Always*, présentation, Space-Based Positioning Navigation & Timing National Advisory Board, Fourteenth Meeting, Washington, DC, December 10, 2014.

[94] US ARMY CERDEC *Dismounted Solder Navigation – Update, 2012* Présentation, Precision Indoor Personnel Location and Tracking Annual International Technology Workshop, 2014, https://web.wpi.edu/Images/CMS/ECE/Paul_Olson_2012_Presentation.pdf