DIA – 3.6

Doctrine interarmées

La guerre électronique (GUERELEC)

CENTRE INTERARMÉES
DE CONCEPTS,
DE DOCTRINES
ET D'EXPÉRIMENTATIONS

CICDE

E.M.A

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

N°1522/DEF/EMA/EMP.1/NP du 14 octobre 2008

DIA – 3.6

LA GUERRE ÉLECTRONIQUE (GUERELEC)

En attendant sa révision par le CICDE,
ce document reprend le texte intégral de
l'ancienne **PIA – 03.163** diffusée par EMA/EMPLOI
sous le titre
« Concept de la guerre électronique »
sous le

N° 1522/DEF/EMA/EMP.1/NP du 14 octobre 2008

MINISTÈRE DE LA DÉFENSE

ÉTAT-MAJOR
DES ARMÉES

Paris, le 14 octobre 2008
N° 1522/DEF/EMA/EMP.1/NP

Le général d'armée Jean-Louis Georgelin
chef d'état-major des armées

à

destinataires *in fine*

OBJET : Concept de la guerre électronique.

P JOINTE : a) PIA-03.163 : concept de la guerre électronique.

Par souci de cohérence, les forces armées françaises ont adopté, en matière de guerre électronique, les doctrines de l'OTAN. Or, l'alliance - dans le cadre de sa transformation, et en prenant en compte le retour d'expérience - a rédigé un nouveau concept de la guerre électronique, le MCM 142. Ce document devient donc une référence.

Afin d'en faciliter son appropriation, une traduction de « courtoisie » a été réalisée. Le document d'origine et sa traduction constituent la publication interarmées 03.163, en pièce jointe.

J'ai donc l'honneur de vous demander de bien vouloir assurer une large diffusion de ce document.

Signé
Le vice-amiral d'escadre Jean-Pierre Teule
Sous-chef d'état-major « Opérations »
De l'état-major des armées

14 rue Saint Dominique 00456 Armées – Tél : 01.76.64.86.50 – Fax : 01.76.64.86.73

DESTINATAIRES :

- Monsieur le général d'armée, chef de l'état-major de l'armée de terre
- Monsieur l'amiral, chef de l'état-major de la marine
- Monsieur le général d'armée aérienne, chef de l'état-major de l'armée de l'air
- Monsieur le général de corps d'armée, directeur du renseignement militaire
- Monsieur le vice-amiral, commandant de l'état-major interarmées de force et d'entraînement
- Monsieur le général de division aérienne, directeur interarmées des réseaux d'infrastructure et des systèmes d'information de la défense
- Monsieur le contre-amiral, commandant les opérations spéciales

COPIES :

- Messieurs les chefs de divisions EPI et C de l'état-major des armées
- Archives générales.

Préambule

Les documents de doctrine de l'OTAN en matière de guerre électronique sont en cours de réécriture. Les nouvelles versions s'appuient sur le retour d'expérience des opérations actuelles et les concepts fondateurs de la transformation de l'OTAN, comme les opérations basées sur les effets.

La doctrine interarmées de guerre électronique s'appuie sur :

- le concept de guerre électronique de l'OTAN (MCM 142) qui a été approuvé en 2008 ;
- la politique de la guerre électronique (MC 64/9) qui sera actualisée, une nouvelle version devrait sortir à la fin de l'année 2008 ;
- la doctrine interarmées de la guerre électronique (AJP 3.6) qui sera actualisée tout au long de l'année 2009 et dont une nouvelle version devrait sortir fin 2009.

Ces trois publications constituent les documents de référence des armées françaises, qui, dans le domaine de la guerre électronique, ont adopté la doctrine de l'Alliance.

Ils doivent donc être connus et mis en œuvre.

Cette publication interarmées regroupe à la fois le document de référence (en annexe) et une traduction dite « de courtoisie » afin de faciliter sa compréhension.

Sommaire

CHAPITRE

1

CONCEPT DE GUERRE ELECTRONIQUE

Ce concept a été rédigé par les nations de l'OTAN en vue de passer d'une vision traditionnelle de la guerre électronique à une approche basée sur les effets.

Il servira de base pour la définition et le développement d'une politique[1] de l'OTAN, puis d'une doctrine des opérations dans l'environnement électromagnétique.

1. Introduction

1.1. La transformation de l'OTAN et la guerre électronique

L'impératif de transformation de l'OTAN - formulé dans la déclaration du sommet de Prague en 2002 et validé lors du sommet de Riga en 2006 - a été reconnu comme une priorité pour l'Alliance par le conseil de l'Atlantique Nord et le comité militaire.

Le concept pour les opérations futures de l'Alliance (*Concepts for Alliance Future Joint Operations* - CAFJO) a été envoyé par les deux commandants suprêmes (SACEUR et ACT) au directeur de l'état-major international le 20 février 2006.

Il définit le cadre conceptuel pour l'élaboration des futurs concepts, doctrines et capacités, afin de développer une aptitude de l'Alliance à mener des opérations basées sur les effets.

Il sera revu, si nécessaire, pour rester cohérent avec les progrès de la transformation et l'apparition de nouvelles notions, de nouvelles idées et des hypothèses en cours d'évaluation.

Le concept de la guerre électronique, qui en découle, s'articule autour de l'idée que l'environnement électromagnétique est un environnement opérationnel.

1.2. L'autorité – la cohérence – l'origine – le suivi

La rédaction de ce concept a été initiée à l'occasion des deux sommets de l'OTAN et s'appuie sur les directives du CAFJO. Il est cohérent avec le document de politique (MC 64) et la doctrine interalliés[2] même si ces derniers devront être remis à jour pour tenir compte de ce nouveau concept.

Ce concept de la guerre électronique été rédigé par le « *Nato Electronic Warfare Advisory Committee* » (NEWAC), conformément aux directives du comité militaire qui est son organisme de tutelle.

Le groupe de travail a été constitué de représentants des nations, des états-majors (IMS, ACT et d'ACO) et de spécialistes, en particulier du « *Joint Electronic Warfare Core Staff* » (JEWCS), de la communauté du renseignement d'origine électromagnétique, de la radionavigation et des communications.

[1] La hiérarchie des documents de doctrine de l'OTAN est le concept, la politique et la doctrine.
[2] AJP-3.6(A) Allied Joint Electronic warfare Doctrine (12/2003).

Selon les directives du comité militaire, le NEWAC a la responsabilité du suivi et de la mise à jour de ce concept.

2. But

Rédiger un nouveau concept sur la gestion de l'environnement électromagnétique dans le cadre des opérations de l'OTAN et influer sur le développement de futurs concepts, de forces ou de capacités.

3. Objectifs

3.1. La définition

Ce concept a pour but d'aider la prise de décisions sur la définition, la livraison et l'emploi des futures capacités de guerre électronique, ainsi que des effets attendus. Il doit fournir une ligne de conduite sur le développement à long terme des capacités électromagnétiques.

Il traite de la dépendance grandissante des forces armées aux effets électromagnétiques et définit le contexte des futures opérations électromagnétiques et guerres électroniques. Il expose rapidement l'ampleur des menaces et traite des nouveaux environnements opérationnels, distincts des environnements traditionnels que sont les espaces maritimes, terrestres et aériens.

Il souligne la nécessité d'identifier l'environnement électromagnétique comme un environnement opérationnel à part entière. Il fournit une vision et des définitions nouvelles qui permettent d'avoir une approche pragmatique de l'environnement et des opérations électromagnétiques. Il décrit les effets de l'électromagnétisme et résume son impact sur certaines initiatives majeures de l'OTAN.

3.2. La terminologie de la guerre électronique dans le cadre des opérations basées sur les effets

Les opérations basées sur les effets de l'OTAN (EBAO) sont en accord avec l'approche globale développée dans le concept stratégique de l'Alliance et son processus de management de crise.
La déclinaison pour la guerre électronique de ce concept d'EBAO, qui souligne l'importance d'utiliser tous les moyens disponibles pour générer des effets permettant la résolution de la crise, s'inscrit donc dans cette logique. Il en décrit des modes d'action, comme l'attaque électronique, la défense, la surveillance, le management, l'exploitation et la gestion de l'environnement électromagnétique. Ils sont détaillés au paragraphe 5-2.

Ce concept développe une nouvelle terminologie qui s'adresse avant tout aux opérationnels et à ceux qui, à tous les niveaux, traitent de la guerre électronique et de ses effets.

La terminologie traditionnelle de la guerre électronique, qui décrit les mécanismes et s'appuie par exemple sur des notions comme les contre mesures électroniques (CME), reste d'actualité mais concerne davantage les spécialistes.

4. Contexte

4.1. L'environnement électromagnétique

Au cours du XXème siècle, l'environnement électromagnétique a joué un rôle important dans la guerre. Sa maîtrise était critique et parfois la clé de la survie et/ou du succès opérationnel.

Aujourd'hui, le mode de vie des pays industriels et postindustriels dépend totalement de la maîtrise de l'énergie électromagnétique et de ses dérivés - comme l'électricité, les communications, l'informatique, les voyages, les loisirs - et cette dépendance est croissante.

Il en est de même dans le monde militaire. De nombreuses capacités opérationnelles s'appuient sur l'énergie électromagnétique, dans des domaines aussi variés que, par exemple, les communications et les transmissions de données, les moyens de détection (imagerie, surveillance, reconnaissance et radar), le recueil du renseignement, la guerre électronique, la navigation et la guerre de la navigation, le ciblage ...

De fait, si l'emploi de ce type de capacités est déterminant et donne l'avantage aux armées modernes, en particulier sur des adversaires technologiquement moins avancés comme des forces irrégulières, il crée aussi des vulnérabilités.

Si les capacités et les modes d'actions sont similaires au sein de l'Alliance, il est clair que seule une parfaite coordination de ces moyens permettra la maîtrise de l'environnement électromagnétique, essentielle pour la réussite des opérations.

C'est pour ces raisons que l'OTAN a besoin d'un concept commun pour les opérations qui se déroulent dans l'environnement électromagnétique.

4.2. La menace électromagnétique

Les menaces qui pèsent sur les forces de l'OTAN dans l'environnement électromagnétique, sont réelles et doivent être prises en compte.

Elles s'appuient à la fois sur les systèmes les plus modernes - comme les systèmes de guidages des missiles (optique, électro-optique, infra rouge, radar) - mais aussi sur des systèmes plus anciens modernisés grâce aux progrès de l'informatique pour en faire, par exemple, des engins explosifs improvisés télécommandés (RCIEDS). Ces menaces s'exercent enfin sur nos systèmes de navigation, de communication et de détection que des adversaires potentiels peuvent aussi attaquer avec des équipements spécifiques.

Les armes électromagnétiques, qui attaquent « physiquement » le personnel, les détecteurs, les systèmes d'armes, les systèmes informatiques et les infrastructures, sont en cours de développement.

Les adversaires potentiels cherchent un moyen de sécuriser leurs communications et utilisent leur propre système de navigation et de détection pour faciliter leurs attaques.

4.3. L'importance de la domination de l'espace électromagnétique

La protection des forces aériennes, terrestres et des plates-formes maritimes de l'OTAN dépend autant de sa maîtrise de l'énergie électromagnétique que de ses défenses anti-aériennes.
L'essentiel de nos capacités dans les domaines de la surveillance, de l'acquisition d'objectifs, du renseignement et de la reconnaissance (SA2R)[3] dépend de l'énergie électromagnétique. Il en est, de même, pour la capacité à délivrer des effets, à naviguer, à communiquer, à opérer, à commander, etc. Dans la guerre moderne, le recours à l'énergie électromagnétique, aujourd'hui quasiment systématique, va continuer à se développer avec l'atteinte des objectifs de transformation.

Les opérations en réseaux[4], le déploiement de capteurs plus sophistiqués et le cycle décisionnel sont aujourd'hui mis en œuvre. Afin de s'assurer de l'atteinte des objectifs, l'OTAN reconnaît dans ce concept de transformation que l'environnement

[3] Intelligence, surveillance and reconnaissance (ISR).
[4] Nato Network Enabled Capability (NNEC).

électromagnétique est un environnement opérationnel où l'aptitude à délivrer une panoplie complète d'effets est essentielle.
Ce concept est destiné aux personnes impliquées dans les opérations dans l'espace électromagnétique et aux non initiés pour leur en expliquer les enjeux.

Il fournit un langage commun pour décrire tous les effets pouvant être atteints au travers de l'environnement électromagnétique dans l'espace de bataille interarmées. Il établit les éléments d'une domination de l'espace aérien, spatiale, terrestre, maritime et maintenant de l'environnement électromagnétique.

5. Transformation de la guerre électronique de l'OTAN – la vision

5.1. L'objectif général

La transformation de l'OTAN pour la guerre électronique et les disciplines associées a pour objectif de :
« façonner et exploiter l'environnement électromagnétique en vue de fournir une appréciation de situation partagée, permettre les communications et la navigation, participer à la protection de la force et délivrer des effets en s'appuyant sur un usage militaire de l'énergie électromagnétique et sur la domination de l'espace de bataille électromagnétique ».

5.2. L'environnement opérationnel

Les environnements opérationnels sont des espaces physiques ou non que l'on retrouve à tous les niveaux des affrontements. Ce sont des espaces où se déroulent les opérations militaires et dans lesquels des effets son délivrés.

En règle générale, ils comprennent les espaces physiques maritimes, terrestres, aériens et spatiaux.

Aujourd'hui, la maîtrise de l'espace électromagnétique et de l'espace de l'information sont devenus déterminants pour le succès des opérations militaires. Les commandants de force doivent les prendre en compte afin de réussir.

Les actions se passent au sein de tous ces environnements et l'information circule à travers eux. Ces actions et ces informations circulent puis exercent une influence dans le domaine cognitif, c'est-à-dire dans l'esprit des adversaires, de la population et de nos propres forces militaires. C'est un domaine différent où aucun effet ne peut être délivré, contrairement aux environnements opérationnels. Il doit être pris en compte dans le cadre de la planification.

Cette approche différente et plus large est nécessaire. Elle représente un défi de plus en plus reconnu par les chefs et penseurs militaires. En effet, cette approche va à l'encontre de notre perception traditionnelle des espaces physiques, seuls lieux d'affrontements pour lesquels nous sommes préparés.

Dans des conflits plus récents, où les idées et les perceptions l'emportent, la simple exploitation militaire de l'espace de bataille peut sembler de plus en plus maladroite et inapproprié. Aujourd'hui, il faut gagner « les cœurs, les esprits et l'image », ce qui suppose :

- une maîtrise de l'espace électromagnétique qui seule permettra une mise en œuvre adaptée des capacités militaires ;
- la domination de l'espace de l'information afin de contrôler la diffusion et l'exploitation ;
- enfin, pour vaincre, il faut dominer les domaines cognitifs qui conditionnent le sentiment de victoire ou de défaite.

Le schéma qui suit, montre comment ces environnements se recouvrent et interagissent entre eux, et démontre les liens entre les effets et les actions.

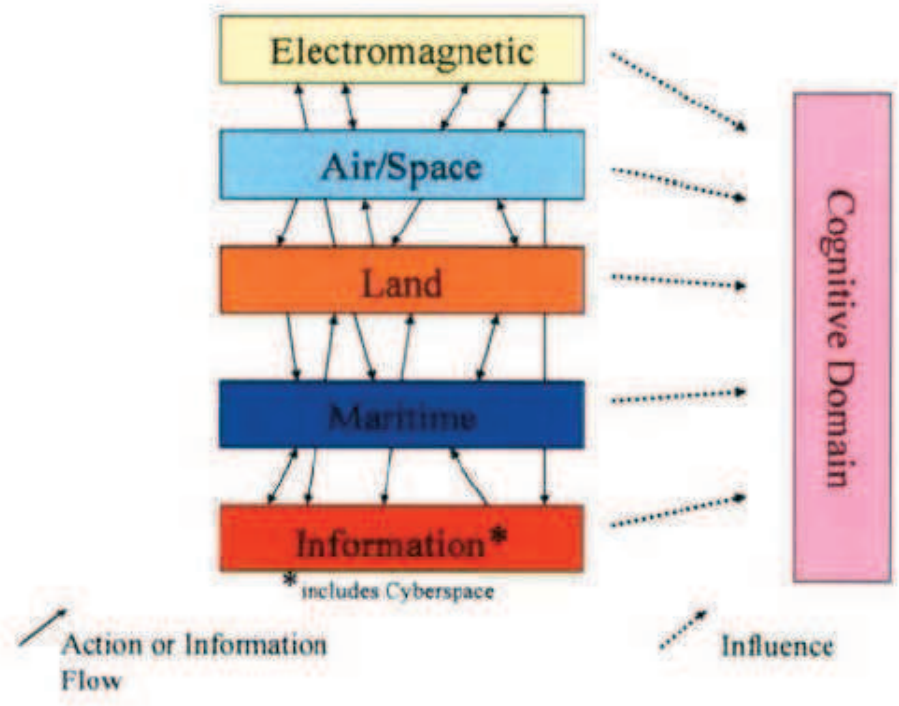


Schéma n°1 : environnements opérationnels (le but est de montrer le flot constant d'activités et d'informations qui circulent entre ces environnements et leur influence)

L'environnement électromagnétique relie les environnements maritime, terrestre, spatial et de l'information. Le succès dans l'environnement électromagnétique est souvent un préalable au succès dans les autres environnements. En fait, la maîtrise de l'espace électromagnétique peut s'avérer suffisante pour atteindre les effets recherchés.
La guerre électronique englobe toutes les actions offensives et défensives dans l'espace électromagnétique. Elles comprennent les actions sur le commandement et les communications, les systèmes de navigation, le SA2R. Le but est la prise en compte initiale des aspects et des effets électromagnétiques dans le cadre d'opérations basées sur les effets afin de maîtriser, dans le cadre « espace-temps » requis, les parties du spectre électromagnétique nécessaire pour mener les opérations de l'OTAN.
L'environnement électromagnétique, comme les autres, peut être exploité, façonné et utilisé pour attaquer ou pour se défendre.

5.3. La nouvelle terminologie

Les termes et définitions qui suivent s'inscrivent dans le contexte de l'environnement électromagnétique. Ils sont exhaustifs et doivent permettent de comprendre les effets qui peuvent être obtenus :

Environnements opérationnels : environnements dans lesquels se déroulent les opérations militaires et où les effets sont délivrés.[5]

[5] L'OTAN reconnaît différents environnements opérationnels - les environnements physiques (maritime, terre, air/espace), l'environnement électromagnétique et l'environnement de l'information. L'action se déroule dans et entre ces environnements et l'information circulent à travers eux. Les actions et l'information influencent le domaine cognitif qui est distinct car aucune action directe ne peut s'exercer sur lui.

Electromagnétique : relatif à l'énergie électromagnétique qui s'appuie sur les champs électriques et magnétiques orthogonaux et qui se déplace à une vitesse constante dans des milieux transparents et dans une direction perpendiculaire à celle des champs.

Environnement électromagnétique : environnement opérationnel où sont délivrés les effets électromagnétiques.

Spectre électromagnétique : séquence continue de radiation électromagnétique variable selon la fréquence, la longueur d'onde et l'énergie.

Management du spectre électromagnétique : organisation pour optimiser l'emploi par les forces amies du spectre électromagnétique disponible.

Opérations électromagnétiques : opérations qui utilisent ou exploitent l'environnement électromagnétique, ou qui l'utilisent à des fins offensives ou défensives, incluant l'usage de l'environnement électromagnétique en soutien des opérations dans les autres environnements.

Communications électromagnétiques et transmission de données : la disponibilité, la sécurité, la résilience et l'efficacité des échanges d'informations s'appuyant sur les ondes électromagnétiques comme support de transmission.

Navigation électromagnétique : positionnement géographique précis et daté, la mesure de la vitesse, la mesure du temps et la navigation utilisant des technologies électromagnétiques et des systèmes terrestres et satellitaires.

Guerre de la navigation : emploi des capacités de la guerre électronique pour défendre ou attaquer des systèmes de navigation[6].

Guerre électronique : action militaire qui exploite l'énergie électromagnétique pour obtenir une appréciation de situation et délivrer des effets offensifs ou défensifs.

Surveillance électronique : usage de l'énergie électromagnétique pour obtenir une appréciation de situation et du renseignement.

Défense électronique : usage de l'énergie électromagnétique pour protéger et s'assurer l'usage du spectre électromagnétique.

Attaque électronique : usage de l'énergie électromagnétique à des fins offensives.

Gestion de la guerre électronique : gestion des processus de la guerre électronique.

Soutien opérationnel de la guerre électronique : somme des données sur la mission de guerre électronique, des informations de guerre électronique, du renseignement, de la doctrine, de l'entraînement, des résultats d'essais et des recommandations.

Les définitions ci-dessus seront insérées dans l'AAP-6[7]. Les définitions traditionnelles, définies dans ce glossaire, des différents aspects de la guerre électronique - contre-mesures électroniques (ECM), mesures de protection électroniques (EPM) et mesures de support de la guerre électronique (ESM) - restent inchangées.

La combinaison avec d'autres capacités ou mesures électromagnétiques rendront possibles de nouvelles activités basées sur les effets. Par exemple, l'ESM, l'EPM et l'ECM pourraient avoir un rôle dans la défense électronique d'un vecteur aérien ou d'une force terrestre à l'encontre respectivement des missiles anti aérien portables (MANPADS), les missiles à fréquence radio ou les RCIEDs.
Ces relations seront développées lors des mises à jour du document de doctrine de l'OTAN, l'AJP-3.6 « *Allied Joint Electronic Warfare Doctrine »* de décembre 2003.

[6] Elle est définie dans le Stanag 4621 C3, navigation warfare définition du 2 novembre 2004.
[7] Glossaire des termes et définitions (édition du 16 avril 2007).

Les exemples des résultats de l'approche basée sur les effets des opérations de guerre électronique de l'OTAN pourraient inclure tout ou partie du schéma suivant :

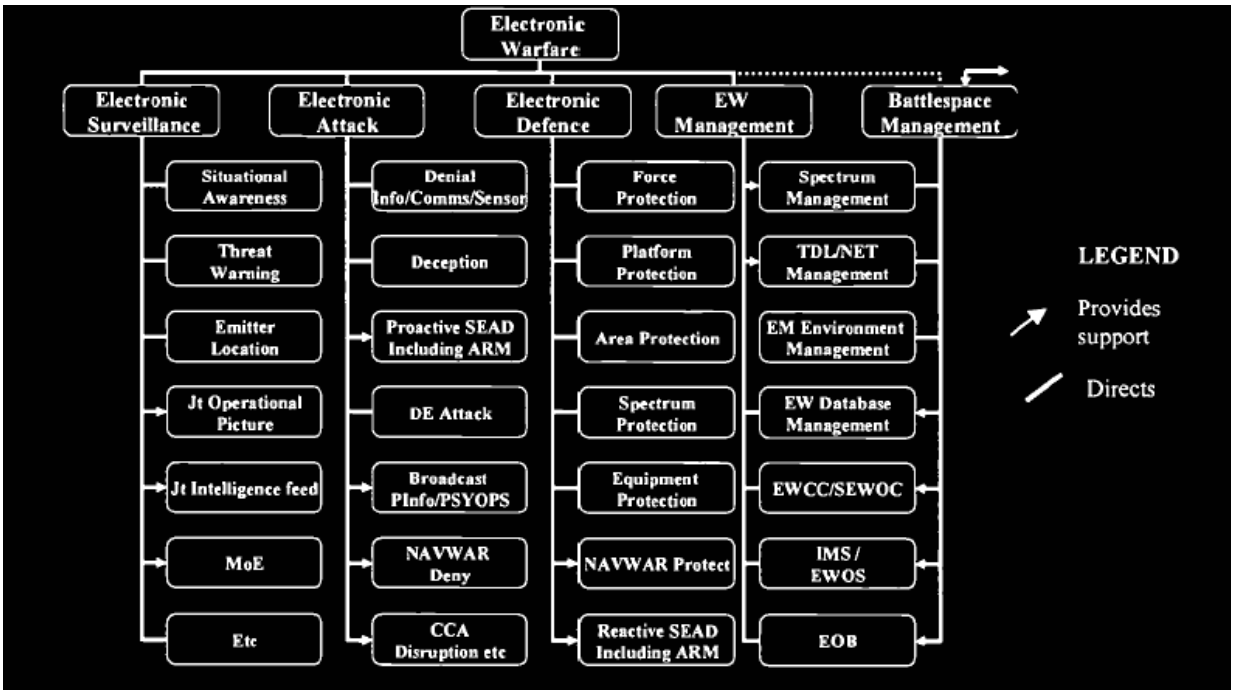


Schéma 2 : actions de guerre électronique et leur agencement dans l'environnement électromagnétique.

Les liens décrits dans cet exemple doivent être gérés par le J6. D'autres liens existent, par exemple, avec la navigation, les réseaux et le SA2R, mais ils ne sont pas présentés pour plus de clarté. Le schéma n° 3 montre ces communautés et quelques unes des capacités résultantes.

5.4. Les relations de la guerre électronique avec d'autres disciplines

L'approche actuelle qui consiste à vouloir distinguer les activités électromagnétiques - telles que celles des capteurs de renseignement (SA2R), des liaisons de données, de la navigation, des communications et de la guerre électronique - s'oppose à une prise en compte globale qui pourrait optimiser leur emploi. De plus, l'emploi désordonné de l'une ou l'autre de ces activités peut altérer de manière très significative l'efficacité de l'une d'entre elles.

Une coordination est donc indispensable. Ces capacités doivent être gérées par un état-major compétent, capable de coordonner et de décider. De même, à l'avenir, les effets des opérations dans l'environnement électromagnétique doivent être totalement intégrés dans l'espace de bataille.

Ce diagramme montre les zones clés des opérations électromagnétiques avec quelques exemples de la manière dont elles interagissent et comment les capacités de l'OTAN dépendent d'elles.

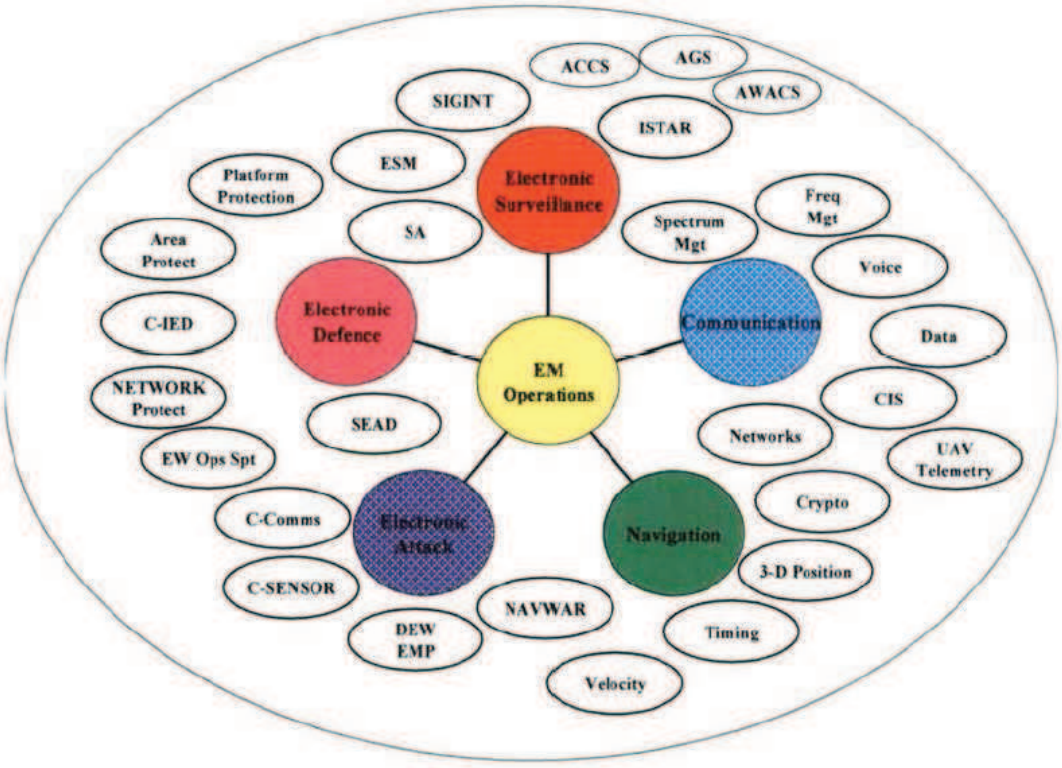


Schéma n°3 : opérations électromagnétiques majeure s et exemples de capacités afférentes (illustration non exhaustive)

Ce diagramme apporte des indications sur les effets mais il n'est pas exhaustif. Par exemple, le contrôle et la télémétrie d'un drone pourraient y être ajoutés en tant que capacité de plus en plus nécessaires en termes d'appui aux engagements et de la protection.
Ils existent des liens clairs entre la guerre électronique, le renseignement, le SA2R, la navigation et les communications. Certains d'entre eux sont déjà très proches et ces liens se manifestent surtout pendant des opérations prolongées. Il faut renforcer et formaliser quotidiennement ces relations, dans le cadre de la planification de leur emploi, des exercices et dans le cadre des travaux de développement des capacités.

5.5. L'état-major de bataille électromagnétique

S'il est évident que des compétences sommaires sur les opérations électromagnétiques sont essentielles pour toutes les forces engagées, la clé de la réussite est aussi liée à une chaîne de commandement consciente de la nécessité d'appréhender tous les environnements opérationnels.

Une cellule d'état-major en charge de l'espace électromagnétique coordonnera les opérations, des niveaux stratégiques aux niveaux tactiques.

Elle aura, tout d'abord, pour mission la mise en œuvre des réseaux de communications et des réseaux de liaisons de données tactiques, mais aussi la mise en œuvre des mesures de protection électronique, quel que soit la nature de la coalition. Elle pourra aussi mettre

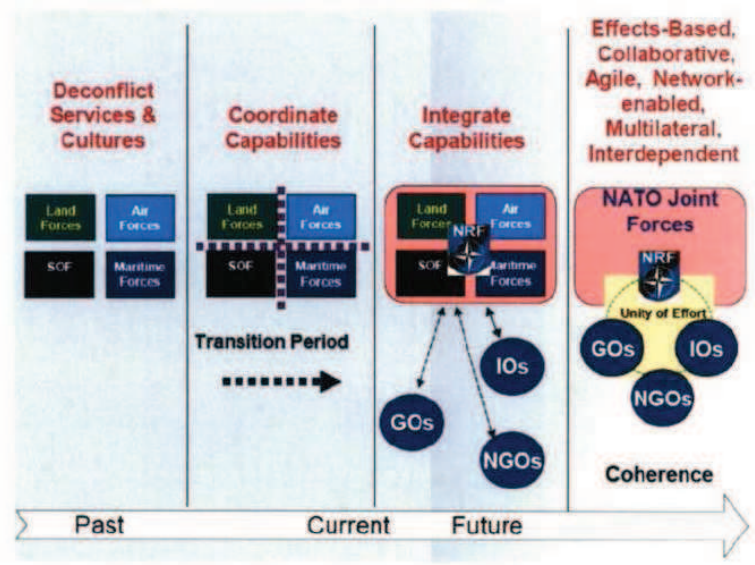
en œuvre, diriger, coordonner et évaluer les attaques électroniques en les coordonnant avec les autres feux.
Cette gestion totale du spectre permettra de s'assurer que les unités engagées dominent l'espace électromagnétique au moment et à l'endroit voulu, condition nécessaire pour garantir leur succès.

Le COMANFOR doit lui aussi pouvoir faire appel à une cellule spécialisée sur l'environnement électromagnétique, dirigé par des officiers expérimentés et constitué de spécialistes entraînés et exercés à travailler ensemble. Des structures appropriées, du personnel et une doctrine sont requis en fonction du retour d'expérience et des expérimentations. Cette cellule devra :

- diriger les opérations électromagnétiques pour fournir une appréciation de situation au commandant de la force : son état-major et aux forces déployées ;
- s'assurer que la navigation, les communications, les liaisons de données et les réseaux sont suffisants pour assurer la mission, la couverture, la résilience et la sécurité ;
- s'assurer que les défenses électroniques fournissent la meilleure protection des forces, des vecteurs et des zones ;
- développer, diriger et évaluer les attaques électroniques ;
- assurer la coordination avec les autres feux ;
- assurer le management du spectre pour fournir et protéger les fréquences nécessaires pour n'importe quelle opération, en coordonner les allocations et assurer les déconflictions.

5.6. L'établissement de la transformation de la guerre électronique d'après la vision du CAFJO

Le CAFJO doit établir des actions cohérentes au niveau de tous les environnements et se focaliser sur les forces comme le montre ce diagramme :



Jusqu'à présent, la transformation de l'OTAN a examiné les environnements géophysiques classiques. Dans le futur, les autres environnements opérationnels doivent aussi être pris en compte afin de rendre possible une approche cohérente des futures opérations interarmées.

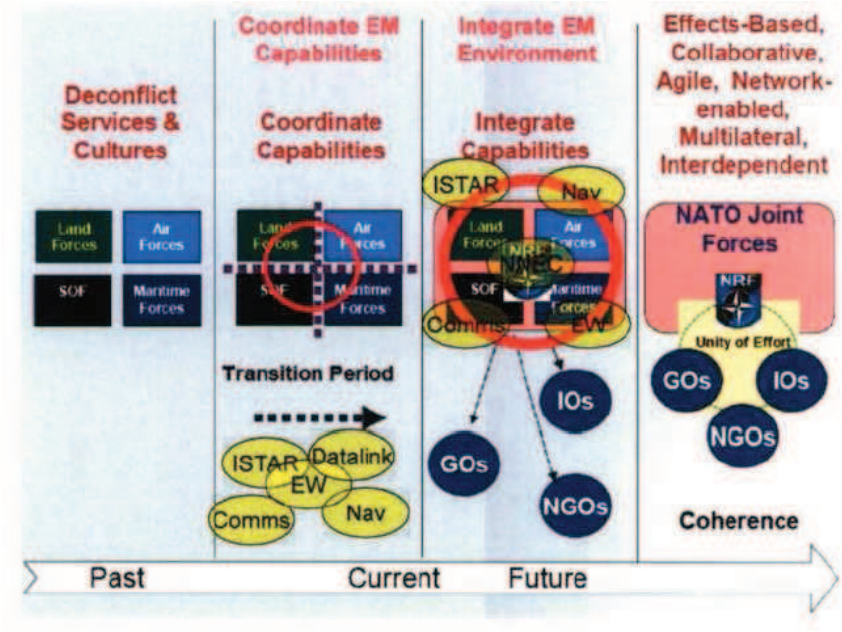


Schéma n°5 : établissement de la capacité électroma gnétique sur la transformation (seules quelques capacités électromagnétiques sont illustrés pour plus de clarté)

5.7. La future guerre électronique et les efforts et initiatives de l'OTAN

5.7.1. Recherche et technologie

L'OTAN a créée l'Organisation pour la Recherche et la Technologie (RTO) afin de diriger et de coordonner la recherche et la technologie de défense au sein l'OTAN, c'est-à-dire la coopération, l'échange d'information, la stratégie et le conseil.
Six comités permettent de couvrir toute la gamme de recherche et de technologie :

- « études, analyse et simulation » (« *studies, analysis and simulation »*, SAS) ;
- « concepts de systèmes et l'intégration » (« *sytems concepts and integration »* SCI) ;
- « technologies de l'électronique et des capteurs » (« *sensors and electronics technology »,* SET) ;
- « technologies des systèmes d'information » (« *informations systems technology »*, IST) ;
- « technologies appliquées aux véhicules » (« *applied vehicle technologies »,* AVT) ;
- « médecine et facteurs humains » (« *human factors and medicine* », HFM).

La communauté de guerre électronique de l'OTAN doit conserver des liens étroits avec la communauté de recherche et de technologie. Ces deux communautés doivent s'appuyer et faire appel à leurs expertises au travers de rencontres et de rapports réguliers.

5.7.2. L'expérimentation dans le domaine de l'électromagnétisme

Celle-ci devrait devenir un axe essentiel du programme expérimental de travail (EPOW). De plus, les essais de la conférence du « groupe de capacité nationale de l'armement » ont un rôle majeur à jouer dans le développement des capacités à tous les niveaux, comme démontré actuellement dans la série des essais Hammer (Trial hammer…).

5.7.3. Les forces de réaction de l'OTAN (« Nato Response Forces », NRF)

La NRF a besoin de forces projetables avec un court préavis, aptes à évoluer dans tous les environnements opérationnels. La capacité à comprendre et conduire les opérations électromagnétiques et la guerre électronique devrait devenir une aptitude essentielle de la NRF.

5.7.4. Les opérations en réseau (« Nato Network Enabled Capability », NNEC)

Les opérations en réseau se dérouleront dans l'environnement électromagnétique, support des liaisons entre les combattants, les détecteurs et les réseaux. C'est aussi dans cet environnement qu'un adversaire peut agir pour détecter, perturber, tromper ou mettre à mal les opérations en réseaux.
Comme l'OTAN s'appuie sur les opérations en réseau pour améliorer l'efficacité tout en diminuant le volume des forces, les réseaux deviennent de plus en plus un talon d'Achille, à moins que l'OTAN n'investisse dans la protection des composants électromagnétiques des radars, des moyens de communications, des liaisons de données, des outils de navigation de haute précision.
La mise en réseau des capacités électromagnétiques comme celles utilisées pour la guerre électronique augmente leur performance. Les capacités de la guerre électronique doivent être une partie de la NNEC intégré.

5.7.5. Opérations basés sur les effets (« Effects-based Approach to Operations », EBAO)

L'OTAN développe une approche des opérations basée sur les effets. Dès lors, ce nouveau concept de guerre électronique de l'OTAN a été élaboré pour avoir une approche de la guerre électronique non plus basée sur les mécanismes mais basée sur les effets.

5.7.6. Le SA2R/la défense aérienne/la surveillance du champ de bataille (« «air ground surveillance », AGS), le système d'alerte aérienne (« «airborne early warning », AEW)

L'OTAN, qui a déjà déployé de nombreux systèmes de capteurs électromagnétiques et de communications, en déploiera de plus en plus dans le futur avec les projets comme l'ACCS et AGS. Ces capteurs et les moyens de communication, dont les liaisons de données, sont le cœur de ces systèmes de surveillance électromagnétique qui sont mis en réseau.
La guerre électronique est alors nécessaire pour fournir la protection des plates formes. Elle fournit aussi les moyens complémentaires d'identification et de protection de ces capacités de soutien électronique. La guerre électronique est aussi une capacité SA2R fiable, qui participe à l'élaboration de la représentation opérationnelle partagée, à l'identification et permet ainsi d'éviter les tirs fratricides.

5.7.7. Navigation et guerre de navigation (Navigation Warfare – NAVWAR)

La communauté de la guerre électronique de l'OTAN doit travailler en liaison avec la communauté NAVWAR afin d'assurer une approche cohérente à tous les niveaux. Par exemple, la doctrine de guerre électronique de l'OTAN doit prendre en compte l'attaque et la protection des systèmes de navigation, ainsi que les moyens à déployer auprès du COMANFOR.

5.7.8. Communications, fréquences et gestion du spectre

La communauté de guerre électronique de l'OTAN doit rester engagée avec la communauté en charge des communications de l'OTAN pour développer des concepts et mettre à jour les doctrines.

5.7.9. Counter-improvised Explosive Device (C.IED)

La lutte contre les IED est une priorité pour l'OTAN et les vaincre - détecter, brouiller ou tromper ces menaces - repose non seulement sur des tactiques, techniques et procédures mais aussi la maîtrise de l'environnement électromagnétique.

5.7.10. La protection des aéroports

La protection des plates formes aéroportuaires est une priorité. Ceci suppose la capacité de vaincre les menaces de tous types comme les armes de petits calibres, les lance roquettes, les mitrailleuses et de l'artillerie antiaérienne.
Détecter, vaincre ou supprimer ces menaces par des manœuvres de déception ou de destruction est un but essentiel de la domination de l'espace électromagnétique.

6. Prochaines étapes

Le NEWAC va initier un programme avec ACO et ACT en s'appuyant sur de nombreux domaines : le développement du leadership, l'entraînement, le matériel, la doctrine et des concepts, les personnels (incluant les compétences essentielles en guerre électronique et en environnement électromagnétique), les installations, et l'interopérabilité.

Les efforts initiaux se focaliseront sur les « MC guidance » et sur les mises à jour des doctrines et des politiques.

Le JEWCS de l'OTAN, le « *Joint Analysis and Lessons Learned Centre »* (JALLC) et le « *Joint Warfare Centre* » (JWC) et l'Ecole de l'OTAN seront concernés.

annexe 1

MCM142