PIA – 3.6

Publication interarmées

Politique de la guerre électronique

ÉTAT-MAJOR DES ARMÉES

Division Emploi 1

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

N°1812/DEF/EMA/EMP.1/NP du 23 décembre 2008

PIA – 3.6

POLITIQUE DE LA GUERRE ELECTRONIQUE

En attendant sa révision par le bureau rédacteur,
ce document reprend le texte intégral de
l'ancienne **PIA – 03.263** diffusée par EMA/EMPLOI
sous le même titre
et sous le

N° 1812/DEF/EMA/EMP.1/NP du 23 décembre 2008

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

ÉTAT-MAJOR
DES ARMÉES

Paris, le 23 décembre 2008
N° 1812/DEF/EMA/EMP.1/NP

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

à

destinataires *in fine*

OBJET : Politique de la guerre électronique.

P JOINTE : a) PIA-03.263 : 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.

L'alliance - dans le cadre de sa transformation et du retour d'expérience – a rédigé le nouveau concept de la guerre électronique, qui a été traduit et vous a été diffusé en octobre 2008 sous l'appellation « concept de la guerre électronique » (PIA 03.163).

Le nouveau document de politique MC 64/10, qui s'inscrit dans le cadre de ces travaux, vient d'être publié.

Afin d'en faciliter son appropriation, une traduction de « courtoisie » a été réalisée. Le document d'origine et sa traduction constituent la publication interarmées 03.263.

Je vous demande de bien vouloir assurer une large diffusion de ce document.

Par ordre
Le vice-amiral d'escadre Jean-Pierre Toulo
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 d'état-major de l'armée de terre
- Monsieur l'amiral, chef d'état-major de la marine
- Monsieur le général d'armée aérienne, chef d'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 corps aérien, directeur interarmées des réseaux d'infrastructure et des systèmes d'information de la défense
- Monsieur le contre-amiral, commandant les opérations spéciales

COPIES :

- Monsieur le général de brigade aérienne, directeur du centre du centre interarmées de concepts, de doctrines et d'expérimentations
- 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.

Le corpus doctrinal interarmées de guerre électronique est composé des documents suivants :

- le concept de guerre électronique de l'OTAN (MCM 142) qui a été approuvé en 2008. Il a été diffusé sous la forme d'une publication interarmées (PIA 03-163) contenant le texte de référence et une traduction dite « de courtoisie » ;

- la politique de la guerre électronique (MC 64/10), objet de cette publication ;

- 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

Annexes

CHAPITRE

1

INTRODUCTION

1.1 Les généralités.

L'OTAN considère l'environnement électromagnétique (EME) comme un environnement opérationnel. Tout succès dans les opérations militaires de l'OTAN repose, à la fois, sur notre maîtrise de cet espace électromagnétique et sur les contraintes que nous faisons peser sur l'adversaire.

Les principales actions mises en œuvre dans le cadre spécifique d'opérations électromagnétiques ou dans le cadre plus traditionnel de l'appui aux opérations comprennent les communications, la navigation, la surveillance électronique (ES), l'attaque électronique (EA) et la défense électronique (ED). Ces trois derniers items constituent la guerre électronique (GE), une fonction militaire clé dans le spectre des opérations et l'objet de cette politique.

Alors que son rôle évolue, l'OTAN doit disposer de l'ensemble des capacités de guerre électroniques nécessaire pour mener l'ensemble des missions dans un cadre interarmées et interallié. De plus, face à l'émergence de menaces asymétriques, telles que celles que font peser des forces irrégulières comme le terrorisme, la guerre électronique a un rôle important pour les contenir et les vaincre.

De nombreuses opérations impliquerons des nations non Otan ou seront conduites en dehors du cadre de l'organisation. Les moyens de guerre électronique de l'OTAN pourraient être requis pour appuyer ce type d'opération. Cette politique contient des orientations en termes de développement, de capacité et de partenariat.

La guerre électronique de l'OTAN s'inscrit en cohérence avec les concepts de transformation. Le concept de la guerre électronique (PIA 03-163) fournit un point de départ pour une approche basée sur les effets en termes de guerre électronique.

Les commandeurs de l'OTAN doivent pouvoir disposer des capacités de guerre électronique appropriées à la nature et à l'intensité de l'opération qu'il mène. Ces capacités doivent permettre de s'appuyer sur la guerre électronique dans la lutte contre les menaces émergentes, telles que les affrontements asymétriques et la lutte contre le terrorisme. Pour s'en assurer, il est essentiel d'avoir au sein de l'alliance une approche davantage fondée sur les effets que sur les tâches. Les commandeurs et les planificateurs doivent s'interroger sur l'effet électronique à obtenir dans une situation donnée et sur ce qui est nécessaire pour délivrer cet effet, même si l'emploi de ce système diffère de son usage traditionnel.

1.2 Le but.

Ce document formalise la nouvelle politique de la guerre électronique de l'OTAN.

1.3 Les objectifs.

Ce document décrit la politique pour les commandeurs de l'OTAN à tous les niveaux : les personnels concernés par le développement des capacités de guerre électronique qui viennent appuyer les forces de l'OTAN, les officiers en charge de la planification et les forces agissant dans le cadre d'une opération de l'OTAN ou impliquant des forces de l'alliance. Il décrit les responsabilités, y compris celle des nations.

1.4 Les définitions.

La guerre électronique est une action militaire qui exploite l'énergie électromagnétique pour fournir une appréciation de situation opérationnelle et délivrer des effets offensifs ou défensifs. La guerre électronique, vecteur des opérations électromagnétiques, est l'affrontement dans l'espace électromagnétique.
Cela comprend :

- 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.

L'AAP-6 contient la terminologie générale contenue dans cette politique. Cependant, si certaines nations de l'OTAN veulent employer une terminologie qui diffère de ces définitions, celle-ci sera utilisée comme langage commun dans les opérations conduites par l'OTAN.
Il est cependant souhaitable que les nations de l'OTAN, ou qui soutiennent l'OTAN, adoptent ces définitions.

CHAPITRE
2

LES FACTEURS D'ENVIRONNEMENT

2.1 L'environnement opérationnel.

La protection des forces de l'OTAN et des plates formes terrestres, aériennes ou maritimes dépendent largement de notre maîtrise de l'énergie électromagnétique. La mise en œuvre du concept SA2R (Surveillance, Acquisition, Reconnaissance, Renseignement) comme notre capacité à délivrer des effets précis, à utiliser des outils de navigation, à communiquer et à commander dépend de l'énergie électromagnétique. La dépendance vis-à-vis de l'énergie électromagnétique est de plus en plus grande dans les conflits modernes et elle s'accroitra encore au fur et à mesure de la transformation de nos forces.
Les opérations en réseaux (NNEC : *Nato Network Enabled Capability*) sont un objectif majeur de l'OTAN. Elles ont pour but d'améliorer la circulation de l'information, de partager les appréciations de situation et d'obtenir la supériorité décisionnelle. Sa mise en œuvre doit être prise en compte au sein des forces de l'OTAN avec le déploiement des senseurs nécessaires.
C'est pour s'assurer que les enjeux sont bien perçus et bien pris en compte que l'OTAN considère l'environnement électromagnétique comme un environnement opérationnel.

Des compétences de base sur les opérations électromagnétiques sont nécessaires pour l'ensemble des forces au contact dont les chefs ont pris conscience que le succès est subordonné à la nécessité d'opérer dans l'ensemble des espaces opérationnels.

Le concept d'un état-major en charge de la lutte électromagnétique, évoqué dans le concept de la guerre électronique, reste vague et imprécis. Il doit, cependant, être en mesure de fournir au COMANFOR et à son état-major :

- une appréciation de situation allant du niveau stratégique au niveau tactique ;
- des communications et des transmissions de données qui s'appuient sur des réseaux omnipotents et fiables ;
- la meilleure protection possible des individus, des forces et des plates formes au sein d'une coalition menée par l'OTAN ;
- la capacité à mettre en œuvre, diriger et évaluer une attaque électronique et d'en assurer la coordination avec les autres feux ;
- le management du spectre pour s'assurer le contrôle au moment et à l'emplacement requis pour le succès.

2.2 L'environnement technologique.

Les progrès technologiques et le développement rapide des réseaux de télécommunication font que la guerre électronique s'appuie sur un espace de bataille de plus en plus encombré, de plus en plus complexe et de plus en plus menaçant. La dépendance grandissante vis-à-vis des satellites de navigation et les opérations réseaux centrées, pour des usagers civils ou militaires, rendront de nombreux vecteurs et systèmes d'armes vulnérables à des brouillages relativement peu compliqués à mettre en œuvre. L'usage croissant de système électronique « clé en main », qui font aujourd'hui partie de l'environnement civil - comme le téléphone portable - font qu'il est de plus en plus difficile de différencier l'usage civil ou militaire de l'environnement électromagnétique. Des systèmes d'armes sophistiqués et utilisés au niveau tactique, comme par exemple, la

dernière génération de missiles sol air portables, les menaces croissantes que font peser des forces étatiques ou non, en utilisant des engins explosifs improvisés, impose un challenge à l'OTAN qui doit apporter une réponse appropriée et à temps en termes de guerre électronique.

Inversement, l'exploitation de nouvelles technologies, comme les drones, offre des opportunités d'améliorer les performances et la contribution des systèmes de guerre électronique alliés.

Les systèmes de guerre électronique et les concepts doivent prendre en compte la sophistication croissante. La tendance est une globalisation des technologies militaires. Les exportations, ainsi que la prolifération des technologies et des expertises, augmentent chaque année. Le futur environnement électromagnétique va devenir un mélange complexe de systèmes interconnectés de différents pays. Le classement de ces émissions et leur identification (ami-ennemi) va ainsi devenir un challenge majeur.

CHAPITRE

3

LES PRINCIPES ESSENTIELS

3.1 Les généralités.

La politique de l'OTAN en matière de guerre électronique est de contrôler, exploiter et utiliser l'environnement électromagnétique afin de mener des actions de guerre électronique, et d'empêcher l'adversaire de faire de même. Cela est fondamental pour le succès des opérations de l'OTAN, et doit être pris en compte par les autorités militaires de l'OTAN et les commandeurs dans le cadre de l'entrainement, de la planification et des opérations.

Le principe fondateur de la politique de la guerre électronique est la coopération dans le but de contrôler l'environnement électromagnétique. Les capacités en guerre électronique de l'OTAN découlent d'une grande variété de moyens et de modes d'action. Ces moyens peuvent appartenir à l'OTAN, être mis à la disposition de l'alliance, voire être déclarés par les nations. Ils peuvent aussi comprendre des moyens d'une nation n'appartenant pas à l'alliance.

L'emploi de la guerre électronique doit apparaître dans les règles d'engagement. La coordination des capacités et le partage de l'information sont essentiels pour éviter les tirs fratricides. Les organisations de guerre électronique doivent être clairement définies au sein des structures de commandement.

Les commandeurs doivent s'assurer que les forces, avant tout engagement, disposent des capacités de défense électronique nécessaires à l'accomplissement de leur mission.

3.2 La planification.

3.2.1 Les forces de l'OTAN.

Décrites dans le CJSOR[1], les forces de l'OTAN doivent planifier et s'exercer aux procédures SEWOC[2]/EWCC[3] afin de renforcer l'intégration de la guerre électronique et de se garantir de disposer des capacités adéquates en opération.

3.2.2 Les données.

Pour une préparation et une mise en œuvre efficace de la guerre électronique, disposer à temps des informations relatives à la GE est essentiel. Ces informations doivent comprendre les données sur l'ensemble des émetteurs (ami, ennemi et neutre) contenues dans l'ordre de bataille et dans les bases de données.

---

[1] CJSOR (Combined Joint Statement of Requirements) : document OTAN qui fournit la liste des capacités interarmées multinationales.

[2] Signal Intelligence (SIGINT) and Electronic Warfare Operations Centre: cellule au sein d'un état major opératif qui traite la GE et le ROEM (renseignement d'origine électromagnétique).

[3] Electronic Warfare Co ordination Cell: cellule au sein d'un état major opératif ou tactique qui traite de la GE.

3.2.3 L'équipement.

Les commandeurs de l'OTAN requièrent les capacités de guerre électronique nécessaires à leurs besoins pour maitriser la partie de l'espace électromagnétique nécessaire. Les forces désignées pour une opération de l'OTAN doivent disposer d'équipements de guerre électronique efficace et si possible, paramétrables pour améliorer leur survivabilité, leur interopérabilité et leur efficacité. Les nations membres de l'alliance doivent faire l'effort de s'assurer - durant le processus d'acquisition de nouvelles capacités – que celles-ci soient paramétrables et interopérables avec les systèmes des autres nations de l'alliance. De plus, les nations membres de l'alliance doivent s'efforcer d'informer l'OTAN sur les technologies émergentes ayant des applications sur la guerre électronique, ce qui permettra de déterminer comment elles pourraient contribuer aux mieux à l'amélioration des capacités de l'OTAN.
Les principes directeurs qui pourraient être appliqués aux développements des capacités de GE au sein de l'OTAN imposent des qualités. Ces capacités doivent donc être :

- adaptable et configurables. Capables d'être utilisées dans le cadre des missions types contre toutes les menaces actuelles et futures dans l'ensemble du spectre des opérations de l'OTAN. Conçues et dimensionnées pour s'adapter aux impératifs du niveau stratégique, opératif ou tactique ;

- réactives. Les forces de GE doivent être capables de réagir rapidement à toutes les situations. Elles doivent être au niveau de disponibilité nécessaire avec les éléments de soutien nécessaires ;

- mobiles. La mobilité inter et intra théâtre est importante afin d'obtenir une efficacité maximale de moyens comptés et optimiser leur emploi en réponse aux exigences des commandeurs ;

- aptes à durer. Les moyens de GE doivent être aptes à durer. Ils doivent de plus faire l'objet d'une protection rapprochée par les forces appuyées ;

- interopérables. L'interopérabilité des forces de l'OTAN est essentielle pour le succès des opérations. En outre, les nations partenaires et les autres organisations, comme l'Union européenne, doivent être encouragées à améliorer leur interopérabilité avec l'OTAN ;

- équilibrés. Un large éventail de capacités doit être disponible. Il faut veiller à ce que l'OTAN dispose de l'ensemble nécessaires aux différents environnements ;

- soutenables. Les moyens de GE doivent être déployés avec un personnel entrainé et un soutien logistique adéquat. La fourniture, à temps, des données de qualité est essentielle dans la durée ;

- connectés. Les moyens de GE doivent être connectés entre elles. Elles doivent bénéficier de transmissions de données sûres et à haut débits pour être capables de diffuser rapidement une information issue de ces capteurs ou fusionnée avec celle d'autres vecteurs.

3.3 La coordination.

Pour améliorer le succès des opérations de l'OTAN, une coordination étroite avec les domaines suivants est nécessaire :
- le renseignement d'origine électromagnétique (ROEM). Si le soutien électronique et le ROEM mettent en œuvre des capacités complémentaires, ils diffèrent par leur subordination. La politique de soutien électronique est contenue dans ce document, la politique ROEM dans le MC 0101. Nonobstant ces subordinations distinctes, les deux structures peuvent être colocalisées et/ou conduites à partir d'une plate forme commune, dans le but d'augmenter les synergies entre les deux ;
- le management du spectre de l'espace de bataille ;

- les communications ;
- les opérations info-centrées ;
- l'activité de « contre commandement » ;
- la lutte contre les IED (AJP-3.15)[1] ;
- les opérations d'information (MC 0422[2] et AJP-3.10[3]) ;
- l'ISR (« Intelligence Surveillance et Reconnaissance ») ;
- les opérations en réseaux (NNEC[4]) ;
- la navigation et la guerre de la navigation (NAVWAR) ;
- la suppression des défenses aériennes de l'ennemi (SEAD) (MC 0485) [5].

3.4 Les exercices et l'entraînement.

Les MC 0094[6] et MC 0458[7] décrivent la politique de l'OTAN pour les exercices militaires.

L'entraînement des forces de l'OTAN est une responsabilité de l'OTAN. Dans le domaine de la guerre électronique, c'est une des tâches du JEWCS.
L'entraînement individuel ou collectif est de la responsabilité des nations.
Il y a cependant une nécessité pour l'OTAN d'entraîner les unités qui lui sont affectées dans le cadre du système de défense aérienne de l'OTAN[8]. Cet entraînement à la guerre électronique sera réalisé au sein du programme d'intégration des forces de guerre électronique de l'OTAN. Le NEWAC défendra cette exigence auprès du comité militaire. Les exercices ROEM/GE[9] permettent d'entraîner les éléments intégrés de ces deux domaines, en amont de la description des modes de fonctionnement au sein d'un SEWOC.

La prise en compte de la guerre électronique au sein des exercices est essentielle pour améliorer le niveau de préparation des forces et doit faire l'objet d'efforts continus en temps de paix. Les exercices doivent être rigoureux et privilégier l'aspect interarmées et interallié. Les forces doivent s'exercer dans un environnement électromagnétique complexe pour améliorer leurs capacités opérationnelles en opération. Les moyens ROEM et GE doivent aussi coopérer au maximum afin de pouvoir améliorer le soutien apporté au commandeur durant les affrontements. Le NEWAC soutient ces exigences et les défend devant le comité militaire et devant les nations.

3.5 Les partenariats.

Ce paragraphe décrit les relations essentielles au sein de la guerre électronique. La doctrine correspondante est l'AJP 3.6 « Allied Joint Electronic Warfare ». Elle décrit précisément l'emploi et les moyens de coordination dans les opérations de l'OTAN ou en coalition.

Operational Preparation Directorate (OPD) : il est responsable de la certification NRF des commandements, qui comprend l'évaluation du niveau d'atteinte des objectifs en termes de GE.

Nato EW Advisory Committee (NEWAC) : sa mission est d'améliorer les capacités GE de l'OTAN en prodiguant des conseils et des recommandations au comité militaire sur les aspects de politique, de doctrine, de programme et de besoins en matière de GE et de faire appliquer en accord avec les nations les décisions prises par le comité militaire en la matière.

---

[1] Allied doctrine for Joint Counter Improvised Explosives Devices (C-IED) Operations.
[2] Nato Military Policy on Information Operations.
[3] Allied Joint Doctrine for Information Operations.
[4] NNEC : Nato Network Enabled Capability.
[5] NATO Suppression of Enemy Air Defences.
[6] NATO Military Exercice Policy.
[7] NATO Education Training Exercise and Evaluation Policy.
[8] NATO Integrated Air Defense System (NATINADS).
[9] ROEM/GE : renseignement d'origine électromagnétique/guerre électronique.

Nato Emitter Data Base Advisory Goup (NEDBAG) : structure de l'OTAN responsable du développement, de la maintenance, de la production et de la distribution de la base de données de l'OTAN (NEDB : NATO Electronic Data Base) selon les termes du Stanag 6009, afin de satisfaire les besoins opérationnels des nations et des commandements de l'OTAN.

NATO Joint EW Staff (JEWCS) : il est responsable de fournir l'expertise GE à l'OTAN, de soutenir et d'entraîner ses forces pour les opérations ou les exercices.

Joint Warfare Centre (JWC) / Joint Force Training Center (JFTC) : ces centres suivent l'entraînement de la NRF, en veillant à la prise en compte de la GE et au déploiement des structures SEWOC/EWCC.

Joint Analysis Lesson Learned Centre (JALLC) : il contrôle la cohérence des objectifs dans le domaine de la guerre électronique avec l'environnement opérationnel et d'entraînement et il fournit des recommandations ou des réactions en retour.

Electronic Warfare Coordination Cell (EWCC) : elle coordonne l'emploi des ressources GE dans les opérations de l'OTAN. Elle est le moyen de coordonner toutes les activités de GE des forces et doit donc être considéré comme un moyen à mettre en œuvre systématiquement.

SIGINT/Electronic Warfare Operations Centre (SEWOC) : il coordonne les ressources consacrées à la GE et au ROEM dans le cadre des opérations de l'OTAN ou des moyens dévolus à ces deux missions sont déployés. Le déploiement d'un SEWOC offre l'intérêt pour un commandeur de créer des synergies entre la cellule en charge de la GE (EWCC) et la section ROEM. C'est le commandant de théâtre qui décide de la mise en œuvre d'un EWCC ou d'un SEWOC. S'il décide de déployer un SEWOC, il lui appartient de préciser la chaîne de commandement[1].

Les nations non OTAN et les entités :
Les objectifs de la politique de la guerre électronique de l'OTAN avec ces interlocuteurs sont de :

- s'assurer que les forces de la coalition peuvent opérer de manière coordonnée, en évitant la confusion entre les émissions amies et les émissions ennemies ;
- s'assurer que les commandements de l'OTAN sont capables d'échanger sur les menaces sans dévoiler les caractéristiques des sources ;
- protéger les informations sensibles détenus par l'OTAN ou qui appartiennent aux nations de l'OTAN ou à des partenaires ;
- augmenter la diffusion des documents de l'OTAN relatifs à la guerre électronique aux nations du partenariat pour la paix.

De plus, les directives suivantes s'appliquent aux commandeurs de l'OTAN dans le cas d'une coalition comprenant des nations non OTAN :

- fournir la liste de l'ensemble des menaces de guerre électronique aux nations non OTAN ;
- fournir aux membres de la coalition l'emplacement et les caractéristiques sur les systèmes électromagnétiques déployés sur le théâtre. Le niveau de détail de ces informations doit être suffisant pour établir les bases de données du théâtre suffisamment exhaustives pour mener des opérations en toute sécurité ;
- utiliser la procédure « *Partner Emitter data Base* » qui consiste à ce que chaque membre d'une coalition fournisse les paramètres radar des moyens déployés. Cette méthode, décrite dans le manuel de la NEDB, permet de partager l'information, de minimiser les interférences, de réduire les ambiguïtés et de prévenir les tirs fratricides.

[1] MC 515 : concept for the NATO SIGINT and EW Operations Centre.

CHAPITRE

4

ORGANISATION

4.1 Le comité militaire.

Le comité militaire est l'autorité en charge de définir la politique en matière de guerre électronique pour l'OTAN. Il exerce son autorité à travers le NEWAC.

4.2 La division des opérations de l'état major international.

La branche opération d'information et défense aérienne (IO&AD) dans la division opérations au sein de l'état-major international sert d'état-major permanent du NEWAC. Le chef de la branche IO&AD est le président du NEWAC. Les termes de référence sont décrits dans l'annexe A.

4.3 Le « *Nato Electronic Warfare Advisory Committee* » (NEWAC).

Le NEWAC est la principale instance consultative et de coordination en matière de guerre électronique. Le NEWAC est chargé de conseiller le comité militaire et de rédiger les documents de politique de ce dernier.
Une description détaillée des missions du NEWAC, des directives générales, des tâches, de la méthode de travail et des termes de référence est contenue dans l'annexe A.
Le NEWAC est constitué de membres votants, un par nation membre de l'alliance, et de représentants, non votants, de l'état-major international, des commandements stratégiques et d'autres entités de l'OTAN si nécessaire. Le représentant national est normalement l'officier guerre électronique le plus ancien ou le chef de l'organisation guerre électronique interarmées. Le représentant du commandant suprême est l'officier guerre électronique le plus ancien de cet état-major.
Il est important que le NEWAC entretienne des relations avec d'autres agences ou comités concernés par la guerre électronique.

4.4 Le « *Nato Electronic Warfare Working Group* » (NEWWG).

Le NEWWG est subordonné au NEWAC. Les termes de référence sont contenus dans l'annexe B.

4.5 Le « *Nato Emitter Data Base Advisory Group* » (NEDBAG).

Le NEDBAG est subordonné au NEWAC. Les termes de référence sont contenus dans l'annexe C.

4.6 Le « *Nato Joint EW Core Staff* » (JEWCS).

Le JEWCS est subordonné à SHAPE (cf. MC0486) et entretient des liens privilégiés avec le NEWAC. Le directeur du JEWCS participe au NEWAC comme conseiller, avec le statut de membre « non votant ».

CHAPITRE

5

LES RESPONSABILITES AU SEIN DE L'OTAN DANS LE DOMAINE DE LA GUERRE ELECTRONIQUE

5.1 Les nations.

Les nations sont responsables de :

- la distribution et la mise en œuvre de la politique et de la doctrine de l'OTAN dans le domaine de la guerre électronique ;
- l'entraînement et l'équipement des unités/moyens/personnel de guerre électronique pouvant de participer à une opération ou à des exercices de l'OTAN, ainsi que la formation du personnel constituant ou renforçant les états-majors de l'OTAN ;
- la fourniture aux commandements suprêmes et aux commandants de théâtre les informations sur leur moyens de guerre électronique et tous les émetteurs d'ondes électromagnétiques mis en œuvre dans le cadre d'une opération de l'OTAN, afin d'améliorer l'interopérabilité, d'éviter les tirs fratricides et contribuer à l'établissement de la liste des fréquences réservées du théâtre d'opération. ;
- la collecte des informations à partir des moyens de guerre électronique sur le potentiel de l'adversaire et le mettre immédiatement à la disposition des commandements suprêmes, des commandants d'opération et si possible, dans la NEDB ;
- la fourniture aux commandants suprêmes les informations sur les capacités nationale de guerre électronique, en service ou à l'étude, en soutien des opérations, en soutien de l'évaluation des situations, pour satisfaire le besoin des forces, et en soutien de l'engagement des forces et de leur emploi ;
- le soutien à l'entraînement et la formation dans le domaine de la guerre électronique en sponsorisant les cours de guerre électronique de l'OTAN, les conférences ou les réunions et en incluant un volet guerre électronique dans l'ensemble des entrainements ou exercices, nationaux ou de l'alliance ;
- l'interopérabilité de leurs équipements de guerre électronique ;
- l'amélioration des capacités de guerre électronique de l'OTAN par le soutien qu'elles apportent aux programmes de recherche et de développement ainsi qu'aux essais et aux évaluations, par leur volonté à satisfaire les besoins opérationnels et les objectifs des forces dans le processus de planification, et par les efforts qu'elles consentent à développer des équipements, des logiciels, des tactiques, des techniques et des procédures ;
- la fourniture des paramètres de leur radar selon les procédures décrites dans le système de réponse de crise de l'OTAN et les documents de politique du comité militaire afférents ;
- la protection du personnel et des équipements contre les effets des systèmes de défense de guerre «électronique ».

5.2 Le comité militaire.

Les responsabilités spécifiques du comité militaire dans le domaine de la guerre électronique sont de :

- affirmer le rôle du NEWAC comme organisation chargée de consulter en matière de guerre électronique ;
- approuver la politique de guerre électronique et encourager la coopération et la coordination de la guerre électronique au sein de l'OTAN.

5.3 Le commandement stratégique.

Les responsabilités spécifiques du commandement stratégique dans le domaine de la guerre électronique comprennent :

- le déploiement au sein de leur quartier général et de leurs commandements subordonnés, des cellules guerre électronique et des interfaces nécessaires au soutien du renseignement ;
- l'intégration, quand cela s'avère nécessaire, de cellule en charge de la guerre électronique au sein de leur état-major et des commandements subordonnées ;
- le développement, la coordination et la mise à jour des concepts et procédures de guerre électronique, ainsi que des aspects relatifs à la planification à un niveau stratégique ;
- le développement, la promulgation et la mise en œuvre détaillée des procédures d'échange d'information guerre électronique ;
- le développement et la maintenance des directives de guerre électronique à long terme suivant le MC 0299 qui servent de base pour établir des besoins dans le domaine de la guerre électronique ;
- la rédaction de règles d'engagement et de mesures de précaution soumises à l'approbation du comité militaire ;
- la participation, si nécessaire, aux groupes de travail relatifs à la guerre électronique dans le cadre des conférences des directeurs nationaux d'armement ;
- la collecte et la diffusion d'information relatives à la guerre électronique, et des échanges avec d'autres commandements et autorités nationales selon les directives appropriées,
- l'établissement du mécanisme pour rassembler et maintenir une estimation actualisée des capacités et des vulnérabilités dans le domaine de la guerre électronique de l'adversaire potentiel ;
- la vérification des développements des capacités de guerre électronique des nations de l'OTAN ;
- la rédaction de standards d'entraînement, la vérification de la prise en compte de la guerre électronique dans les entraînements et exercices de l'OTAN ;
- la participation aux travaux de rédaction de la doctrine et des procédures opérationnelles, ainsi que la mise en place des ressources nécessaires à l'activation des SEWOC et EWCC.

5.4 Le JEWCS.

Les responsabilités spécifiques du JEWCS dans le domaine de la guerre électronique comprennent :

- le soutien du commandant suprême des forces alliés en Europe (SACEUR), et des commandements subordonnés au commandement alliés des opérations (ACO) en apportant l'expertise et les moyens d'entraînement dans le domaine de la guerre électronique en soutien lors de la planification et le déroulement des exercices et des opérations de l'OTAN ;
- le soutien du quartier général de l'OTAN, du SACEUR et le commandement allié pour la transformation dans le développement de la politique guerre électronique de l'OTAN.

Annexe 1

LE *NATO ELECTRONIC WARFARE ADVISORY COMMITTEE*

Les missions.

La mission du NEWAC est :

- d'améliorer les capacités en guerre électronique de l'OTAN en fournissant au comité militaire des conseils et des recommandations en termes de politique, de doctrine, de programmes et de besoins,
- de faire appliquer les décisions du comité militaire dans le domaine de la guerre électronique en liaisons avec les nations.

Les généralités.

Le NEWAC reçoit des directives et des travaux du comité militaire par l'intermédiaire de l'état major international (IMS). Le NEWAC donne des directives aux groupes qui lui sont subordonnés, est destinataire de leur rapport et approuve leur programme de travail en accord avec le comité militaire.

Les tâches.

Le NEWAC est chargé de développer la politique et la doctrine allié en matière de guerre électronique, d'encourager les exercices d'entraînement, d'encourager l'échange d'information entre les nations, d'évaluer les contre-mesures électroniques prises dans le cas d'une crise, et de soumettre des objectifs dans le domaine de la guerre électronique aux directives ministériels de l'OTAN.
Le NEWAC doit aussi travailler avec attention sur les problèmes relatifs à la guerre électronique et les besoins futurs avec les autres agences ou comité de l'OTAN, en particulier le NACSI[1], le JEWCS, le « NATO Standardisation Agency » (NSA), le CNAD et le NC3A[2] et d'autres

Les membres du NEWAC.

Pour assure un consensus, chaque nation de l'alliance est représentée aux réunions du NEWAC, à l'exception du Luxembourg (représenté par la Belgique) et de l'Islande (qui n'a pas de forces militaires). Les autres participants sont le président du NEWAC, le secrétaire du NEWAC, le président du NACSI, les représentants des commandements suprêmes, le président du NEWWG[3] si nécessaire et le président du NEDBAG. D'autres personnes peuvent participer aux réunions plénières, sur invitation d'un membre permanent et sous couvert de l'état major du NEWAC.

La méthode de travail.

Le président du NEWAC organise au moins deux réunions par an, avec un ordre du jour et un compte rendu final. Ce compte rendu est envoyé aux différents membres pour être approuvé. Au moins une des réunions annuelles se déroule dans un quartier général de

[1] NATO Advisory Committee on Signals Intelligence.
[2] NATO consultation Command and Control Agency.
[3] NATO Electronic Warfare Working Group.

l'OTAN. Les réunions du NEWAC qui se tiennent en dehors des quartiers généraux ne nécessitent pas d'interprète français.

Les décisions du NEWAC sont prises sur la base du consensus des nations.

Les représentants des commandants suprêmes et des autres organismes n'ont ni le droit de vote, ni le droit de véto. Ils peuvent exprimer leurs avis durant les séances et les faire enregistrer s'ils le souhaitent.

Les aspects terrestres et aériens sont traités par le NEWWG. Les aspects maritimes sont traités en liaison avec le MAROPS WG[1]. Le président du comité 2 (combat maritime de surface) de ce groupe de travail est invité à participer aux réunions du NEWAC.

Le président du NEWAC.

Le président du NEWAC :

- rend comte au comité militaire, donne des directives pour le NEWAC et peut agir au nom du comité militaire entre les réunions. Pour cela, le président consulte le NEWAC quand il dispose du temps nécessaire et dans tous les cas, il rend compte des actions décidées à la réunion suivante du NEWAC ;
- fournit un compte rendu actualisé à l'issue de chaque réunion du NEWAC ;
- est le chef de la branche IO&AD à la division opération de l'état major international ;
- participe, ou se fait représenter, aux réunions du NACSI ;
- peut être remplacé, en cas d'absence, par le secrétaire du NEWAC. Lors d'une réunion du NEWAC, et en cas d'absence simultanée du président et du secrétaire, les membres « votants » élisent un président provisoire, à la majorité simple.

[1] Maritime Operations Working Groups.

Annexe 2

LE *NATO ELECTRONIC WARFARE WORKING GROUP*

La mission.

Le NEWWG est responsable devant le NEWAC. Sa mission est de l'appuyer en tenant des réunions et en préparant des recommandations qui seront soumises au NEWAC.

Les généralités.

Le NEWWG conseille le NEWAC sur les aspects de politique et de doctrine de la guerre électronique interalliés, aériens, maritimes et terrestres.
Il apporte aussi son soutien dans le développement de tactique de guerre électronique, la rédaction et propose des changements rédige

Les tâches.

Le NEWWG est l'enceinte de consultation et de coordination sur des sujets de guerre électronique qui ne sont pas du niveau du NEWAC. Les tâches confiées au NEWWG sont diverses et il fait des propositions soumises aux séances plénières du NEWAC.
En plus de toutes ces tâches, le NEWWG doit :

- fournir des recommandations, qui seront soumises au NEWAC, en matière de politique de guerre électronique en interallié ou dans le domaine terrestre ou aérien ;
- développer les concepts et doctrines de guerre électronique de l'OTAN et aider le développement de TTPs de guerre électronique ;
- entretenir des liens avec le MAROPS WG pour le domaine maritime ;
- valider les références à la guerre électronique dans les publications de doctrine, selon les termes de l'AAP-3[1]

La méthode de travail.

Le NEWAC approuve la planification et le programme de travail du NEWWG, qui consiste traditionnellement en quatre réunions plénières et davantage si nécessaire. Le NEWAC valide les sujets traités dans chacune de ces réunions, il peut aussi exprimer des besoins.
Le président du NEWWG rend compte de ses travaux lors de réunion suivante du NEWAC. Le directeur du JEWCS désigne le président du NEWWG. Si nécessaire, le président du NEWWG désigne un secrétaire. Les nations et les organismes membres du NEWAC désignent des représentants pour participer au NEWWG.
Le consensus n'est pas requis dans les réunions du NEWWG. Le NEWAC est informé des différentes opinions sur les différents sujets. Les travaux menés par le NEWWG sont soumis à la validation du NEWAC et du comité militaire, si nécessaire.
Les membres du NEWWG peuvent proposer des items de travail en sus de ceux qui sont planifiés. Le secrétaire assiste le président dans la préparation et la conduite du meeting. A l'issue de la réunion, le secrétaire établit le compte rendu et la liste d'action. La validation des propositions est obtenue auprès des nations lors du NEWAC.

[1] Procedures for the Development, Preparation, Production and the Updating of NATO Standardization Agreements and llie Publications.

Annexe 3

LE *NATO EMITTER DATA BASE ADVISORY GROUP*

Les missions.

Le NEDBAG est responsable devant le NEWAC de :

- développer et de maintenir la base de données électronique de l'OTAN, selon les termes du Stanag 6009, afin de satisfaire les exigences des nations et des commandements de l'OTAN ;
- fournir les conseils techniques afin d'assurer la compatibilité de la NEDB avec les standards et procédures actuelles de l'OTAN ;
- développer et déployer des standards et des procédures mis en œuvre au sein de la base de données ;
- développer et produire la documentation et les manuels d'instruction nécessaires ;
- identifier les difficultés liées à la NEDB qui requièrent la coordination du NEWAC avec d'autres organismes ;
- diffuser des informations complètes et actualisées.

Le président du NEDBAG.

Le président du NEDBAG :

- est fourni par les nations ; il devient le chef de section de la « NATO JEWCS DB » ;
- peut inviter des spécialistes aux réunions du NEDBAG pour dispenser de l'information spécifiques ;
- est garant de la compatibilité des travaux du NEDBAG avec les standards et les procédures de l'OTAN. Pour ce faire, il entretient les liens nécessaires et coopère avec les organisations appropriées ;
- il rend compte au NEWAC de ses réunions.

Le secrétaire du NEDBAG.

Le secrétaire du NEDBAG est fourni par les nations. Il devient le « NATO JEWCS DB Staff Officer ». Le secrétaire peut remplacer le président en son absence.

La méthode de travail.

Le NEDBAG est composé de représentants des nations volontaires, disposant d'un droit de vote, et des représentants d'ACO, d'ACT et d'autres entités de l'OTAN, qui ne disposent pas d'un droit de vote. Les représentants d'organisations civiles ou militaires nationales, intéressés par les échanges de données de guerre électronique, peuvent être invités comme observateurs.

Le NEDBAG se réunit normalement deux fois par an, ou selon les directives du NEWAC. Un ordre du jour est établi, et un compte rendu est rédigé à l'issue.

Les décisions au sein du NEDBAG sont prises suivant le principe du consensus des membres votants.

Les nations qui n'assistent pas aux réunions du NEDBAG coordonneront leur position nationale par rapport à l'ordre du jour ou à la liste d'actions en amont de la réunion de ce dernier. Cela évitera de retarder les travaux menés par le NEDBAG,

Annexe 4

LES DEFINITIONS DE GUERRE ELECRONIQUE

Le renseignement de communication (COMINT) : renseignements issus des communications électromagnétiques et des systèmes de communication.

Le spectre électromagnétique (EMS) : la répartition de l'ensemble des ondes électromagnétiques en fonction de leur fréquence et de leur amplitude. Il inclut les ondes radio, les micro-ondes, les radiations thermiques, les ondes lumineuses, les radiations ultra violet, les rayons X, les rayonnements électromagnétiques cosmiques et les rayons gamma.

L'attaque électronique : usage de l'énergie électromagnétique à des fins offensives. Cela inclut les armes à énergie dirigée, les micro-ondes fortes puissances et les pulsations électromagnétiques tout autant que les appareils à fréquence radio.

La défense électronique : usage de l'énergie électromagnétique pour protéger et s'assurer l'usage du spectre électromagnétique. Cela inclut la protection de la force, des aires et des vecteurs.

Le renseignement électronique : renseignement obtenu à partir de l'interception d'ondes électromagnétiques non communicante.

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

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

Le renseignement radio (SIGINT) : terme générique employé pour décrire le renseignement de communication et le renseignement d'origine électronique quand il n'y a pas nécessité de les dissocier.

La suppression des défenses antiaériennes de l'adversaire : action qui vise à neutraliser, à dégrader temporairement ou à détruire les défenses anti aériennes de l'adversaire avec des moyens de destruction et/ou de neutralisation.