

Valérie LADEGAILLERIE

**INTEROPERABILITE
NOUVEAUX ENJEUX**

Notes de conférences

Diffusion

Ladegaillerie

© Valérie LADEGAILLERIE
ISBN 979-10-96025-53-4

© Cette œuvre est protégée par le Code de la propriété intellectuelle selon la loi du 1^{er} juillet 1992.
Manuscrit déposé pour protection juridique. Coquilles non corrigées.
Citations autorisées avec mention de l'auteur et <http://valerie-ladegaillerie.e-monsite.com>

A Mo.

Valérie LADEGAILLERIE

Docteur ès Science politique, Docteur ès Droit, Docteur ès Philosophie
Directeur du Pôle Science politique, Droit, Stratégie militaire
Institut Européen de recherche sociétale et stratégique

SOMMAIRE

INTRODUCTION

□ **LE CADRE DE L'INTEROPERABILITE**

LES DEFINITIONS

LES FINALITES

LA GRADATION

LES MODALITES DE DEVELOPPEMENT

□ **LES NOUVEAUX ENJEUX DE L'INTEROPERABILITE**

L'INTEROPERABILITE : APPROCHE

LES INITIATIVES INTERNATIONALES DE CONSTRUCTION

LES PROSPECTIVES

□ **RECOMMANDATIONS POUR L'INTEROPERABILITE**

LES PRIORITES

LES RECOMMANDATIONS

Tableau des abréviations

ABMS	<i>Advanced Battle Management System</i>
ACCS	<i>Allied Command and Control System</i>
AFATDS	<i>Advanced Field Artillery Tactical Data System</i>
ALAT	Aviation légère de l'armée de Terre
ASI	<i>Air-Surface Integration</i>
BITD	Base industrielle et technologique de
défense CAOC	<i>Combined Air Operations Center</i>
CAS	<i>Close air support</i>
CENTRIXS	<i>Combined Enterprise Regional Information Exchange System</i>
CES	<i>Core Enterprise Services</i>
CJOS COE	<i>Combined Joint Operations from the Sea Centre of Excellence</i>
CMD3D	Centre de Management de la Défense dans la
3 ^{ème} Dimension	CONTACT Communications Numériques TACTiques
et de Théâtre	
CSP	Coopération structurée permanente
DACAS	<i>Digitally Aided CAS</i>
ESSOR	<i>European Secure Software Defined Radio</i>
FC-G5S	Force conjointe G5 Sahel
FMN	<i>Federated Mission Networking</i>
IAMD	<i>Integrated air and missile defense</i>
ISR	Intelligence, surveillance & reconnaissance
JADC2	<i>Joint All Domain C2</i>
JMTC	<i>Joint Maneuver Training Center</i>
MCDC	<i>Multinational Capability Development Campaign</i>
MDO	<i>Multi-domain Operations</i>
MPE	<i>Mission Partner Environment</i>
NIFC-CA	<i>Naval Integrated Fire Control - Counter-Air</i>
NNEC	<i>NATO Network Enabled Capability</i>
NRF	<i>NATO Response Force</i>
SCAF	Système de combat aérien futur
SDR	<i>Software-Defined Radio</i>
SIA	Système d'information des armées
SIC	Systèmes d'information et de communication
TEN	<i>Tactical Edge Networking</i>
SCA	<i>Software Communications Architecture</i>
TTP	Tactiques, techniques, procédures

En 2021, le budget du ministère des Armées représente 13% du budget général de l'Etat, soit 50.06 milliards d'euros - pensions incluses. La mission "Défense" : 47 695 millions d'euros - environnement et prospective de la politique de défense, équipement des forces, préparation et emploi des forces, soutien de la politique de défense. Le ministère des Armées suscite et accompagne l'innovation industrielle et technologique à travers différents programmes. En 2021, ce sont 6.6 milliards d'euros à la Recherche et Développement.

Dans la problématique de l'après Guerre froide avec la Chute du Mur de Berlin le 9 novembre 1989, la problématique de l'interopérabilité laisse apparaître de nouveaux enjeux avec la multiplication des opérations extérieures multinationales, le développement et la généralisation des systèmes d'information et de communication ou la prise en compte des exigences d'une approche globale pour les campagnes de stabilisation et de contre-insurrection.

□ LE CADRE DE L'INTEROPERABILITE

Qu'est-ce que l'interopérabilité? Quels en sont les acteurs? Quelles en sont les modalités de réalisation? Telles sont les interrogations appréhendées dans cette partie en vue d'une réponse compréhensible.

LES DEFINITIONS

⌘ Définition - capacité de plusieurs systèmes, unités ou organismes à opérer ensemble grâce à la comptabilité de leurs organisations, doctrines, procédures, équipements et relations respectives.

Remarque - L'interopérabilité désigne la capacité d'outils à communiquer entre eux, à ne pas confondre avec la compatibilité qui caractérise un outil dans un environnement déterminé en respectant les règles que ce dernier impose. L'on distingue plusieurs niveaux d'interopérabilité : elle s'envisage soit de manière étroite en excluant certaines notions comme l'intégration, soit de manière englobante avec l'idée d'opérer ensemble.

⌘ Définition de l'OTAN -

. l'interopérabilité des *forces* - *Force interoperability* : aptitude des forces de deux ou plusieurs États à s'entraîner, à s'exercer et à opérer efficacement ensemble en vue d'exécuter les missions et les tâches confiées

. l'interopérabilité militaire - *Military interoperability* : aptitude des *forces militaires* à s'entraîner, à s'exercer et à opérer efficacement ensemble en vue d'exécuter les missions et les tâches confiées

On n'évoque plus des systèmes mais des forces afin "de mettre en commun les ressources". De facto, il s'agit d'utiliser tous les forces pour qu'elles fonctionnent ensemble de manière cohérente afin d'atteindre les objectifs fixés.

LES FINALITES

Deux finalités à l'interopérabilité -

. l'exigence opérationnelle relative à la sécurité des opérations afin d'éviter que les forces interfèrent

. elle est une condition de l'efficacité des opérations

Trois domaines à l'interopérabilité -

. l'interopérabilité interarmées afin de garantir un emploi cohérent des forces pour des opérations multidomaines

. l'interopérabilité internationale ie faculté à opérer avec des forces partenaires

. l'interopérabilité en vue d'une approche globale ie avec les acteurs institutionnels, autorités et institutions du pays hôte... organisations internationales

LA GRADATION

Niveaux d'interopérabilité -

- . la déconfliction - gestion des interférences entre forces menant des opérations autonomes
- . la coordination - utilisation synchronisée via un CONOPS ou un OPLAN/OPORD commun
- . l'intégration opérationnelle ie "*The arrangement of military forces and their actions to create a force that operates by engaging as a whole*" ie un système de force unique au niveau opérationnel
- . la symbiose de préférence à la synergie des Américains, notion trop large ie une étape d'intégration qui combine divers systèmes pour composer un unique système en multidomaine - par analogie à la biologie définie comme : "l'association étroite de deux ou plusieurs organismes différents, mutuellement bénéfiques, voire indispensables à leur survie"

Concrétisation dans la notion de combat collaboratif, multiplateforme - L'Armée de l'air définit le "combat collaboratif connecté" : forme de combat dans lequel les capacités des différents systèmes d'arme se renforcent mutuellement sur l'ensemble des fonctions élémentaires du combat (détecter, classifier, décider, engager, évaluer les effets) pour fournir une capacité unique dont les performances dépassent celles des systèmes considérés isolément. La logique d'efficacité collective prime sur celle de meilleure performance individuelle, y compris entre systèmes hétérogènes, et ce quel que soit le milieu."

Le partage des forces - *pooling and sharing* - présente un niveau d'intégration qui dépasse l'interopérabilité. Dans la logique américaine, l'intégration vise l'efficacité, l'interdépendance vise l'efficacité mais elle est indissociable des niveaux d'intégration.

Temporalité de l'interopérabilité -

- . elle peut se limiter à la planification d'opérations et la conduite des opérations en temps réfléchi - implication possible d'un niveau de coordination ou d'intégration
- . elle peut concerner la conduite d'opérations en temps réel - ex : mission de ciblage d'opportunité, appui aérien - indissociable d'une forme d'intégration
- . elle peut réaliser des opérations en temps "immédiat" ou "réflexe" - situations opérationnelles évolutives comme la défense antimissile... ou la gestion de l'espace aérien

Le facteur différentiel -

Le différentiel capacitaire, ie des forces capacitaires asymétriques qui opèrent ensemble dans des opérations internationales, conditionne le niveau d'interopérabilité réalisable et dicte le degré de partenariat opérationnel.

Ex - Différentiel entre Barkhane/Sabre et les forces du G5 - impossible interopérabilité pour faire participer les forces du G5 à des opérations contre les groupes djihadistes.

Conséquences -

- . la logique de l'intégration opérationnelle voire la symbiose tactique dans des manoeuvres communes
- . la logique de la niche opérationnelle qui repose principalement sur la coordination confiée à la force ou aux forces moins capables que la force principale

□ LES MODALITES DE DEVELOPPEMENT

Construction de l'interopérabilité -

- . on peut la construire au long terme avec la stratégie capacitaire - approche implicite dans les axes des stratégies générales militaires, nationales ou multilatérales = l'interopérabilité par conception - *interoperability by design* - nécessite l'harmonisation des décisions des décideurs multiples aux impératifs divergents
- . on peut la construire par nécessité dans le cadre d'un engagement afin d'efficacité opérationnelle dans l'immédiat - facilitée par l'existence d'un commandeur opérationnel ex : en Irak, les Américains imposent leurs choix à leurs partenaires en matière de SIC ou pour certaines missions en Afghanistan

La capacité dépend de la durée de l'engagement qui enracine et institutionnalise les arrangements entre partenaires. C'est le rôle de l'OTAN avec *la Federated Mission Networking* (FMN).

Les chercheurs de la RAND distinguent deux ambitions -

- . l'interopérabilité générale lorsqu'"une force et un leadership (sont) prédisposés et efficaces pour résoudre les défis opérationnels et tactiques complexes du travail avec des partenaires étrangers disparates"
- . l'interopérabilité ciblée - *targeted interoperability* - désigne "une unité ou un ensemble d'unités qui ont surmonté les obstacles culturels, techniques et procéduraux pour opérer avec leur homologue étranger pour des fonctions spécifiques"

Champs constitutifs de l'interopérabilité -

Le niveau d'interopérabilité découle de convergences.

. le champ stratégique

L'interopérabilité découle de la cohérence des cadres stratégiques d'engagement.

Trois problématiques de compatibilité -

- . les objectifs confiés à la force et la stratégie opérationnelle adoptée et les caveats nationaux qui conditionnent l'emploi de chaque force
- . les cadres juridiques qui conditionnent l'engagement, en particulier les règles d'engagement (ROE)
- . les règles de partage des données opérationnelles nécessaires, ex : le renseignement

. le champ culturel

Il s'agit en premier lieu de la compréhension des cultures stratégiques des partenaires et des cultures institutionnelles des autres armées. La notion de culture stratégique renvoie à des interprétations nationales des intérêts, situations et options stratégiques... Il s'agit aussi d'appréhender les cultures institutionnelles des différentes armées.

- . la culture opérationnelle relative à la logique d'emploi des moyens, ce qui formalise une doctrine le cas échéant
- . la culture identitaire des personnels
- . la culture "métier" avec ses terminologies, théories... pratiques

. le champ opérationnel

Le champ opérationnel se constitue des normes opérationnelles incarnées dans la partie prescriptive des doctrines, tactiques, techniques, procédures (TTP), les *Standard Operating Procedures* (SOP) et les accords codifiant les convergences organisationnelles et opérationnelles des forces.

. le champ technique

L'interopérabilité technique concerne l'acquisition des équipements et celui des normes techniques dont la convergence permet aux matériels de fonctionner - les standards de fonctionnement de ces équipements, ceux structurant les données échangées... à l'heure des clouds, cette notion apparaît fondamentale.

Les procédés capacitaires qui permettent l'interopérabilité -

- . les opérations
- . les entraînements et exercices communs
- . les processus de développement commun des doctrines opérationnelles et tactiques, des TTP et standards
- . les jumelages d'unité
- . le partenariat militaire opérationnel
- . la formation
- . les échanges d'officiers
- . les équipements
- . la recherche et le développement

□ **LES NOUVEAUX ENJEUX DE L'INTEROPERABILITE**

L'interopérabilité évolue suivant les bouleversements géopolitiques et géostratégiques.

L'INTEROPERABILITE : APPROCHE

Existences de différents niveaux d'interopérabilité.

Interopérabilité multinationale -

α les opérations aériennes et navales

L'interopérabilité aérienne et navale est réelle mais de circonstance et répond aux exigences de sécurité des opérations.

- . dans le champ culturel - elle se fonde sur la référence commune à la notion d'*airpower*
- . dans le champ normatif opérationnel, les forces aériennes partagent la culture "métier"
- . dans le champ technique, elle est permise au sein de l'OTAN par le réseau ACCS, l'identité de certains systèmes comme l'E-3 AWACS et l'E-2 HAWHEVE, les radios SATURN... mais des incompatibilités parfois existent

α les opérations de la Marine avec les homologues de l'OTAN

Elle découle a minima d'une compatibilité des procédures qui vient de l'habitude des opérations, ex : lutte contre la piraterie... opérations au sein de l'OTAN. Le commandement de la CTF50, task force aéronavale déployée dans le Golfe confié en 2015 à la France est un exemple de l'aptitude française.

L'interopérabilité est de circonstance par exemple avec les Américains. Pour eux, l'OTAN n'est qu'un des éléments de l'équation. Le commandement opérationnel américain fait un effort afin d'intégrer ses partenaires via ses réseaux à l'exemple de CENTRIXS mais selon ses règles et procédures. A souligner que créer un environnement interopérable nécessite un effort de convergence lors des conférences de planification.

α les opérations des forces terrestres

Dans le domaine normatif opérationnel, l'interopérabilité est relativement satisfaisante malgré les diverses doctrines tactiques. Des divergences notamment existent entre les forces occidentales historiques et les forces des pays de l'Est marquées par l'héritage soviétique. Des centres comme le *Joint Maneuver Training Center (JMTC)* oeuvrent au développement de TTP compatibles.

Traditionnellement, l'interopérabilité multinationale s'articule au niveau de la brigade - sauf pour certaines opérations d'appui. Or, la réalisation opérationnelle dépend des échelons subordonnés, ce qui peut être problématique. Ex : les niveaux de

numérisation sont variés - existence de 13 systèmes de suivi de la situation opérationnelle tactique.

Ex : l'interopérabilité technique existe avec la compatibilité du système Automatisation des Tirs et Liaisons de l'Artillerie Sol-sol (ATLAS) et de l'*Advanced Field Artillery Tactical Data System* (AFATDS) de l'US Army. A noter aussi les progrès enregistrés dans le *Digitally Aided-Close Air Support* (DACAS).

⌘ L'interopérabilité multinationale - Elle reste contrainte par des divergences nationales variant d'une opération à l'autre.

. les caveats, règles d'engagement et partage d'informations
pb : les caveats qui conditionnent l'action de nos partenaires européens peuvent entraver l'interopérabilité de la coalition au Sahel

A noter que la perception américaine de l'utilité stratégique du partenariat varie selon les circonstances, ce qui influence les règles de partage d'informations.

Operation Unified Protector (2011) - les règles évoluent à l'initiative du Président Obama en raison de la poussée des insurgés vers Tripoli. Autre exemple : les Américains sont en appui des Français au Sahel - échange de renseignements et intégration.

L'interopérabilité avec l'Afrique - Théoriquement, elle doit être améliorée par un partenariat militaire opérationnel (PMO).

. coopération structurelle pilotée par la DSCD
. plans de coopération opérationnelle, ex avec les pays d'Afrique de l'Ouest
. coopération en opération avec les détachements interarmes (DIA)

Dans la pratique, l'interopérabilité se situe essentiellement à un niveau de coordination a minima.

. au niveau des états-majors comme celui de la Force conjointe G5 Sahel (C-G5S) par nos officiers de liaison ; le commandement conjoint (MCC) mis en place entre Barkhane et la FC-G5S - intégrant les officiers insérés au PC interarmées de théâtre français - une cellule de partage et de renseignements et un poste de commandement conjoint renforcent cette coordination

Cette interopérabilité est de fait problématique. Dans le domaine technique, elle est victime des multiples sources d'équipements des forces locales. Dans le champ culturel et celui des normes opérationnelles, l'interopérabilité pâtit de l'éclatement des PMO tant au niveau global que sur celui des théâtres d'opérations. Certains partenariats consistent à enseigner normes et processus d'état-major occidentaux à des officiers dont la culture diffère. Autre problème : institutions militaires réduites dans ces pays, moral défaillant... qui limitent ces coopérations structurelle et opérationnelle.

Interopérabilité interarmées -

L'interopérabilité interarmées s'illustre dans les engagements récents et se concrétise par des échelons interarmées robustes du CPCO aux COMANFOR - ou autres, ex : opérations de l'ALAT depuis le BPC en Libye, ou les appuis aériens aux unités de l'armée de Terre engagées de Barkhane.

Dans le domaine d'une opération multidomaine comme le CAS, après des années d'opérations communes en Afrique par ex, en dépit de normes identiques OTAN d'origine américaine et des productions du CICDE, les armées de Terre et de l'Air ne partagent pas la même vision des besoins d'échanges d'informations entre les acteurs (JTAC, aéronefs, PC...). L'opération Serval : friction entre l'armée de Terre et l'armée de l'Air quand à l'emploi de systèmes de coordination comme le CMD3D, ce qui entrave

l'interopérabilité de niveau intégration. A noter que l'interopérabilité avec les Américains en situation de forte asymétrie capacitaire vise à incorporer les éléments de leurs partenaires au sein d'une matrice interarmées américaine, ce qui défavorise la consolidation de l'interopérabilité interarmées.

Interopérabilité et approche globale -

La notion d'approche globale évolue suivant les circonstances. Nos orientations stratégiques évoquent cette exigence et l'OTAN ainsi que l'UE réaffirment leurs rôles dans ces architectures. L'OTAN puis le CICDE rédigent de nouvelles versions de leurs manuels de doctrine d'action civilo-militaire.

LES INITIATIVES INTERNATIONALES DE CONSTRUCTION

Existence d'initiatives au sein des structures multilatérales.

L'OTAN est l'une des grandes puissances normatives militaires mondiales avec l'appareil militaire américain, ses mécanismes de développement des doctrines, des standards, ses centres comme le *Joint Air Power Competence Centre* (JAPCC). L'Union européenne avec ses structures comme le comité Finabel pour les forces terrestres. Les structures multinationales comme le MDCD, le *Combined Joint Operations from the Sea Centre of Excellence* (CJOS COE) et le JMTC qui développent des TTPs ou la force de réaction rapide européenne avec le CRR-E.

L'OTAN : le Federated Mission Networking -

Depuis 2015, l'OTAN s'est engagée dans le programme *du Federated Mission Networking* (FMN). Le FMN recouvre trois volets : une structure de gouvernance et de gestion, un cadre de planification afin de développer une fédération de réseaux et les spécifications de réseaux qui synchronisent des centaines de standards techniques dans tous les domaines des SIC : STANAG, Mil Standard américains, standards civils tels que *World Wide Web Consortium*. A noter que l'Alliance exploite autant que faire se peut les normes existantes. La documentation est corrigée et complétée en spirale sur une base biannuelle.

La spirale 1 concerne les *Core Enterprise Services* (systèmes d'exploitation, messagerie...). En 2018, avec la troisième, le FMN couvre des domaines fonctionnels comme le partage de données et la gestion de la recherche en JISR, la *Recognized Air Picture* ou certains domaines logistiques ainsi que la sécurité avec le *Protected Core Networking*.

Un *Coalition Verification and Validation Environment* combinant de multiples laboratoires certifie chaque spirale puis elle est testée dans les exercices de l'OTAN. La *Coalition Warrior Interoperability Exercice* (CWIX) est une vaste plateforme d'expérimentation des SIC. En septembre 2019, le système d'information des armées (SIA) démontre sa compatibilité avec les standards FMN. Le processus FMN s'applique aussi dans les missions opérationnelles et est synchronisé avec celui de la génération de la *Nato Response Force* dont il norme les services C4ISR. Au-delà des réseaux OTAN, FMN offre la méthode et les spécifications qui permettent aux pays engagés sur un théâtre de développer l'interopérabilité nécessaire entre leurs réseaux : il s'illustre comme un processus complet et évolutif ayant vocation à s'étendre notamment au niveau tactique, à transiter vers le *cloud computing* et développer des standards de cyberdéfense.

A noter que le projet FMN ne déroge pas au schéma établi avec NCW/NNEC : concepts et architectures américaines adaptés par les alliés européens qui les corrigent en fonction de leurs moyens si nécessaire.

La coopération permanente entre initiatives européennes -

La CSP est indissociable de la création d'un Fonds Européen de Défense mais elle reste une plateforme de programmes de RDT&E découplée des éventuels volets d'acquisition nationale des systèmes développés, aussi représente-t-elle un risque pour les

industriels. Même réduite et dispersée, elle fournira un vecteur de développement capacitaire, un moyen de soutenir les BITD nationales et de partager les coûts de développement de systèmes. Son impact sur l'interopérabilité doit être mesuré mais l'on peut penser qu'elle améliorera les capacités stratégiques (espace, défense antimissile...) et la dissuasion face à l'Est, principalement en terme de soutien et de protection. A noter qu'à l'exception de la Belgique et des Pays-Bas, nos partenaires ne participent pas ou peu aux OPEX impliquant des opérations de combat¹.

La Mission Partner Environment, approche américaine -

En 2015, un mémo signé des commandants opérations géographiques que sont AFRICOM, EUCOM, CENTCOM, INDOPACOM et l'USSOCOM demande à l'OSD le financement et le soutien pour créer un réseau commun multinational de partage de l'information. Le CIO du DOD met en place le projet de *Mission Partner Environment* (MPE), rebaptisé MPE-Information Sharing (MPE-IS).

Deux configurations doivent coexister -

- . le *MPE Enduring* permanent de niveau stratégique pour les travaux de planification et de partage de l'information asynchrone intégré avec le *Joint Information Environment* américain
- . le *MPE Episodic* pour une mission donnée où les partenaires de coalition sont élevés au niveau de *peer* et doivent pouvoir opérer avec leurs propres systèmes

Le MPE uniformise et met à disposition des partenaires une série de CES et un Virtual Data Center par COCOM qui permet de gérer des enclaves CENTRIXS avec des passerelles multiniveaux.

Le projet s'étale de 2017 à 2024 et en 2019 le CIO désigne l'Air Force comme agent d'exécution du développement de ce MPE.

EUCOM est le premier commandement à le déployer, que le *Joint Warfighting Assessment* (JWA) 18 de l'Army a permis de tester avec succès semble-t-il. Sur cette base, IWA permet de valider un autre système, le *Common Operational Picture Shop* qui permet de partager les données de situation entre les systèmes C2 des nations participantes. Ce système utilise le protocole *NATO friendly force information* (NFFI) employé par le FMN. L'on peut en conséquence penser que l'interopérabilité du suivi des unités alliées est assurée.

IEI, l'Initiative Européen d'Intervention -

L'IEI lancée par le Président de la République française en 2017 rassemble 9 partenaires: Danemark, Estonie, Espagne, Belgique, Finlande, Pays-Bas, Portugal, Royaume-Uni et l'Allemagne. Elle s'inscrit dans le champ culturel puisque vise à créer une "culture stratégique commune" avec des travaux communs de prospective, planification de doctrine... et faciliter l'interopérabilité pour des situations données.

¹ Le Danemark est exempté de participer à la politique de défense européenne.

Intégration pérenne ciblée -

La période est aux projets ciblés stratégiques, d'interopérabilité par l'intégration opérationnelle *by design* à différencier des intégrations de circonstance auxquelles préparent les forces multinationales (CJEF, JEF UK...) en raison de la difficulté de réalisation de l'interopérabilité de conception avec nombre de partenaires.

Limitée à ce jour à quelques *battlegroups* de l'UE et à la communauté des systèmes comme l'illustre le programme CAMO par lequel l'armée de Terre belge adopte la doctrine et les équipements Scorpion².

L'Allemagne fournit un modèle dans le domaine terrestre. Elle souhaite constituer une "armée d'ancrage" pour les petites puissances militaires européennes et s'approprie le *Framework Nation Concept* (FNC) de l'OTAN.

Une intégration achevée avec les Pays-Bas : une brigade d'assaut aéromobile néerlandaise dans la division des forces de réaction rapides allemandes, celle des unités de chars, la compatibilité ou l'interchangeabilité d'éléments de maintenance et même l'intégration système avec le *Tactical Edge Networking* (TFN). Signé en 2019, le TEN vise à l'intégration (doctrines, TTPs, équipements communs...) des SIC terrestres du *Digitilisation of Land Based Operations* (D-LBO) allemand et FOXTROT néerlandais jusqu'au niveau plate-forme. La première unité est planifiée pour 2024. La Belgique désire rester interopérable avec ce TEN, son objectif étant de bâtir "un pont solide entre ce partenariat franco-belge et le duo germano- hollandais".

Les intégrations ciblées s'articulent avec des programmes dans le domaine aérien où les systèmes actuels à l'exemple du F-35 ou les programmes SCAF et Tempest constituent des systèmes de systèmes. Leur adoption concerne aussi les munitions, le soutien, les politiques de gestion de données... L'on va vers la constitution de bulles F-35, SCAF ou Tempest qui constitueront l'essentiel des capacités engagement/combat et un élément C21SR de chaque force aérienne.

Exemples d'initiatives -

. la *Maritime Theatre Missile Defence Forum* initiée en 2004 qui rassemble 11 nations européennes et américaines qui disposent de capacités antimissiles navales

. le projet *Framework Architecture 2030* qui vise à développer les processus, les modèles de données, les standards d'interface afin de permettre l'engagement multiplateforme entre les navires des nations qui participent à l'action - à l'image des bâtiments Aegis de l'US Navy avec l'architecture *Naval Integrated Fire Control*

- *Counter Air* (NIFC-CA).

LES PROSPECTIVES

Facteurs stratégiques -

Les facteurs stratégiques sont fondamentaux en ces temps troublés qui exacerbent les tensions entre les superpuissances et où les menaces et les risques mutent.

Le partenariat avec les Etats-Unis -

La théorie voudrait que le contexte stratégique plaide pour un renforcement de l'interopérabilité avec les Etats-Unis comme l'illustrent les accords US-UK-FRA. A noter la nécessité du soutien des alliés aux déploiements des forces américaines en cas de crise, aussi l'attachement des alliés reste fondamental.

² Voir annexe.

Pourtant des interrogations relativement à l'engagement américain sur la scène internationale se posent. L'on note un intérêt plus économique qu'un intérêt relatif aux équilibres stratégiques. Cette approche peut-elle être le signe d'une réduction de l'interventionnisme militaire des Etats-Unis au niveau mondial ? A voir.

Les partenariats européens -

Le partenariat avec les pays européens semble fragilisé. A souligner que la compétition industrielle avec la BITD américaine tendrait à consolider les efforts de stratégie au travers notamment de l'OTAN et de la CSP. Du 29 janvier au 6 février 2022, 1 400 militaires français et estoniens participent à l'exercice interarmes WINTER CAMP avec les objectifs de perfectionner leur savoir-faire tactique dans un environnement hivernal très exigeant et de développer leur interopérabilité avec les alliés de l'OTAN.

En ce qui concerne le Royaume-Uni, si les Britanniques semblent marginalisés au sein de l'OTAN suite au Brexit, leur investissement dans le F-35 ou leur initiative aéronavale leur garantit une place dans les coalitions au côté des Américains. Toutefois il faut souligner qu'ils ne pourront peut-être pas maintenir le niveau de cohérence interarmées de leur force en raison de sous-financement. Si l'Allemagne devient le gardien des pays d'Europe centrale et de l'Est - hormis la Pologne en partenariat avec les Etats-Unis - sa coopération avec la France qui cumule les forces opérationnelles et BITD du continent lui est nécessaire et ce, même si une divergence fondamentale réside dans la primauté qu'accorde l'Allemagne aux intérêts de sa BITD par rapports aux objectifs stratégiques et capacitaires militaires.

Les ruptures technologiques dans le domaine des SIC -

Les avancées technologiques relativement aux systèmes d'information et de communication change l'interopérabilité technique.

L'interopérabilité en matière de communication -

⌘ la radio logicielle - *Software-Defined Radio* (SDR)

Le spectre électromagnétique permet une flexibilité des moyens de transmission qui permet d'optimiser les communications et de contourner les menaces de guerre électronique. La radio logicielle communique sur plusieurs formes d'onde utilisées en fonction des correspondants. Le programme qui l'exploite était le Joint Tactical Radio System (JTRS) américain fin 1990. L'architecture de communication logicielle, le *Software Communications Architecture* (SCA) offre un cadre de développement de la partie logicielle de ces radios. Le PR4G de Thalès est aussi une SDR. Les partenaires européens se sont dotés de leur propre programme, *European Secure Software Defined Radio* (ESSOR) géré par l'OCCAR pris en compte par la CSP. ESSOR, mise en oeuvre par le programme de COmmunications Numériques TACTiques et de Théâtre (CONTACT) de Thalès, développe une architecture et une forme d'onde haut débit, elle est basée sur la SCA américaine. Les postes CONTACT continueront de prendre en compte la forme d'onde PR4G. Les technologies évoluent, la logique "software-defined" est étendue à la gestion du réseau ouvrant l'ère du "Software-Defined Networking" (SDN).

⌘ les nouvelles architectures spatiales

L'interconnexion croissant permet le développement d'architectures aérospatiales intégrant les communications par relais aéroportés.

⌘ le développement des réseaux 5G

La mise en oeuvre de la 5G, en matière de communications cellulaires promet une rupture entendue qu'elle offre un débit de 10 à 20 fois plus important que la 4G et permet d'interconnecter plus d'éléments que cette dernière. Indissociable des technologies de SDN et de l'intelligence artificielle, la 5G permet de virtualiser plusieurs réseaux de nature et de fonctions différentes.

⌘ Le Cloud et l'approche data-centric

L'avenir des SIC est au *cloud computing* qui consiste à partager, mutualiser les ressources informatiques. Le programme JEDI vise à créer un cloud général unique que compléteront des clouds spécifiques. Le FMN de l'OTAN fait appel à ces technologies.

Le cloud renouvelle la problématique du *Network Centric Warfare* caractérisé par ses 5V : *volume, vélocité, variété, véracité* et *valeur*. Le cloud tactique doit permettre aux unités d'accéder à un outil disponible auparavant aux seuls opérateurs de niveau stratégique. Les Américains sont en avance dans le développement incrémental de ces technologies : *usion Warfare* présente sur le F-35, CloudONE de l'*Airbone Battle Management System* (ABMS) ou encore le système C2 de l'Air force désigné comme pilote de l'intégration des SIC tactiques des forces américaines. En France, le MINARM explique que "(garantir la supériorité opérationnelle et la maîtrise de l'information sur les théâtres d'opérations) nécessite une transformation importante de nos architectures opérationnelles pour mettre la donnée au coeur du futur combat en Cloud". Le SCAF se présente comme "un système de systèmes intégrant au sein d'un véritable Cloud des senseurs et des effecteurs de différentes natures et de différentes générations".

Qu'en sera-t-il de l'interopérabilité de ces clouds? Sur le plan technique, le défi est relatif entendu que nombre de technologies utilisées sont principalement civiles. La capacité d'un cloud à exploiter le big data repose sur une stratégie de gestion des données opérationnelles. Donc nous allons vers un environnement Data-Centric. Les évolutions technologiques qui caractérisent ces SIC impliquent une intégration croissante du cyber au niveau tactique. Le ROEM et la surveillance électronique occuperont une place fondamentale.

Les facteurs opérationnels -

. le combat

La mise en réseau et l'infovalorisation impriment des changements opérationnels significatifs pour l'interopérabilité. Elles permettent de passer à l'intégration opérationnelle au plus bas niveau tactique : la symbiose. Ex : les opérations aériennes

Elles sont conduites selon le principe du contrôle centralisé des opérations (au niveau des structures de conduite du JFACC) et de l'exécution au niveau des AWACS et équivalent des centres terrestres de détection et de contrôle... En cas de multiples opérations tactiques, cette organisation est trop centralisée pour réagir et saisir les opportunités entendu qu'elle ne permet pas d'exploiter la perception des opérateurs tactiques souvent supérieure à celle du JFACC. La nouvelle technologie permet de décentraliser ce contrôle au niveau des plateformes devenant des noeuds C2ISR. Le programme d'*Alliance Future Surveillance and Control* (AFSC) de l'OTAN qui combine les fonctions de guet aérien et de *battle management* des AWACS qu'il remplace mais aussi la défense antimissile et la surveillance du champ de bataille pourrait aller de même. C'est un véritable défi de l'interopérabilité. Dans le domaine aérien, le F-35 représente une étape de cette capacité de fusion warfare et préfigure l'évolution vers la capacité *Next Generation Air Dominance* dans le cadre de l'ABMS. L'armée de l'Air inscrit le combat collaboratif connecté dans le coeur de la modernisation de ses capacités actuelles dont le programme Connect@aéro doit assurer les interconnexions et à terme au coeur du SCAF.

. le multidomaine

Le développement des opérations multidomaines ou interdomaines est consubstantiel de du niveau supérieur d'interopérabilité. Il s'inscrit dans une logique identique à l'intégration opérationnelle interarmées et reste avant tout une problématique d'interopérabilité au sein de la matrice d'intégration interarmées constituée par les grandes puissances militaires.

Les évolutions dues aux postures -

Des évolutions capacitaires et opérationnelles façonnent les besoins d'interopérabilité.

Ex : l'allongement des systèmes de feux terrestres dans la profondeur

A noter que la Field Artillery américaine connaîtra bientôt un doublement de la portée de ses canons, roquettes guidées et missiles tactiques. Autre exemple, la

guerre électronique avec les opérations cyber tactiques.

Le système capacitare américain -

Les Américains renforcent le recours aux architectures modulaires et aux méthodes flexibles.

. les architectures ouvertes modulaires

Elles combinent deux aspects : la modularité d'un système qui permet d'adapter certaines de ses composantes en fonction du besoin sans changer l'ensemble du système et les standards ouverts par opposition aux standards propriétaires. Une quinzaine de standards matériels et/ou logiciels pour systèmes terrestres et aériens sont produits. Ces architectures fournissent des standards d'interface et exploitent des *Government Reference Architectures* (GRA) qui permettent un point de référence pour une fonction donnée. Existe un effort de convergence de ces standards gérés par le *Defense Standardization Program Office* (DSPO) que sanctionne un mémo signé par les chefs d'état-major en janvier 2019.

. l'innovation

Les Américains sollicitent les entreprises de la high-tech pour développer leurs systèmes d'information. Une relation étroite entre développeurs et opérationnels et une délégation d'autorité par la hiérarchie accélèrent le processus. L'opération *Kessel Run* a permis en peu de temps de moderniser une série d'applications de planification et de conduite du CAOC d'Al Udeid.

L'innovation permet une accélération du rythme de modernisation des systèmes d'armes et d'information mais rend plus complexe l'interopérabilité avec les SIC des partenaires. Cette offensive américaine se heurte à la volonté des pays européens membres de l'OTAN qui désirent préserver leurs BITD à l'instar de l'Allemagne et la France.

□ RECOMMANDATIONS POUR L'INTEROPERABILITE

Les priorités d'interopérabilité dépendent de l'ambition opérationnelle française, des types d'interventions envisagées et envisageables et des partenariats opérationnels.

LES PRIORITES

L'interopérabilité dépend des avancées de la France sur le plan stratégique. Si la volonté politique, notamment la capacité financière, entrave la conduite des OPEX, la position stratégique de la France serait celle de son positionnement géostratégique comme Finistère occidental d'une Europe tournée vers l'Est et l'interopérabilité serait à maintenir avec les alliés de l'OTAN.

Les interventions envisagées -

L'endiguement djihadiste et la gestion de crise en Afrique : une crise est de nature à fragiliser les Etats de la région générant des risques de gestion de crise. La confrontation avec un adversaire émergent ou la capacité à réaliser une gestion de crise en Méditerranée, au Levant et au Moyen-Orient. La réponse à une menace exercée par ex sur une de nos ZEE.

Les partenariats opérationnels -

Le US-UK-FR demeure le coeur de la capacité d'intervention occidentale et, en cas d'intervention, le maintien d'un haut niveau d'interopérabilité demeure un impératif.

Nécessité de renforcer ou maintenir une interopérabilité ciblée avec les alliés européens interventionnistes, les nations du Su (ex : Italie, Espagne...) en raison des risques sur la Méditerranée... l'Allemagne, la Pologne et des partenaires autres peuvent constituer une part importante d'un dispositif à l'Est.

Le renforcement de l'interopérabilité interarmées : priorité de notre stratégie militaire - Il est nécessaire d'envisager des scénarios où nos partenaires réduiraient leur implication militaire extérieure et, par conséquent, nécessité est pour la France de constituer la nation-cadre d'une coalition limitée - notamment en Afrique, en Méditerranée ou encore au Levant. Ses forces constitueraient une matrice interarmées de coordination ou d'intégration de la coalition sur laquelle viendraient se plugger les partenaires. Sur le plan opérationnel, le multidomaine comme symbiose tactique entre composantes de milieu pour les missions communes constitue un impératif afin de garantir le maintien de notre aptitude à agir.

LES RECOMMANDATIONS

Interopérabilité internationale -

Les axes de priorité d'interopérabilité : les initiatives trilatérales avec Américains et Britannique ; la *Combined Joint Expeditionary Force* (CJEF) avec les Britanniques ; les travaux de l'OTAN qui fournissent un socle commun au travers du FMN pour les SIC ; les jumelages d'unités avec plusieurs alliés clés tels les Britanniques, Italien, Belges... ; l'Eurocorps ; l'accroissement en opérations en BSS avec nos forces déployées ou ... CAMO.

Il semble opportun de développer d'autres initiatives avec d'autres pays européens.

- Ex - avec les systèmes germano-néerlandais déjà évoqués...
- de rejoindre la JEF britannique en complément de la CJEF
- de développer un groupe amphibie méditerranéen

Le développement des opérations multidomaines impose une intégration système et une symbiose tactique qui reposent sur des technologies militaires spécifiques aussi plusieurs éléments communs à l'exemple de la SCA pour les transmissions ou la convergence partielle entre le MPE américain et le FMN montrent que des réalisations sont possibles. Toutefois il paraît difficile d'espérer une interopérabilité sur un spectre large de systèmes entendu les différences dans les stratégies de données des différents projets. Ces limites induisent un risque de découplage accru relativement aux opérations tactiques réalisables en commun et à un renforcement des opérations de niche confiées aux forces français dans le domaine aéroterrestre.

Interopérabilité multidomaine interarmées -

Opérations selon la logique multidomaines : les opérations aéroportées et amphibies, le CAS ou la défense sol-air. Une extension de ces logiques peut exister.

Domaines d'interopérabilité multidomaine afin de

- "collecter, exploiter et diffuser du renseignement"
- "construire, entretenir, partage une situation opérationnel" - comme avec le SIA
- "obtenir et conserver les supériorités terrestre, aérienne et aéromaritime"
- "protéger les forces déployées contre les menaces surface-surface et contre les menaces air-surface et balistiques"
- "frapper en profondeur en territoire ennemi"
- "appuyer les forces au contact" - renseignement, feux et cyber

Pour ces différentes aptitudes, l'interopérabilité doit reposer sur le développement de capacités intégrées en matière offensive, notamment la SEAD, d'interdiction, incluant les missions de ciblage d'opportunité, de *Time Sensitive Targeting* (TST) et de lutte antinavire. Ces missions implique l'armée de l'Air, l'aéronavale et les missiles de croisière de la Marine, ainsi que les hélicoptères de combat de l'ALAT et implique les organisations de C2 ainsi que les capacités ISF.

Démarche capacitaire envisageable -

Ces évolutions impliquent des transformations dans le spectre DORESE. A moyen

terme, il faut progresser sur l'intégration opérationnelle des unités puis envisager une fédération des systèmes de combat collaboratif élaborés par chacune des armées.

. sur le court et moyen terme, progression de l'interopérabilité opérationnelle
 Les armées disposent de capacités opérant de manière coordonnée, ex : les données tactiques comme la L16, les systèmes ATLAS, MARTHA pour la défense sol-air avec les modules CMD3D. Elles disposent d'un corpus doctrinal interarmées significatif avec les doctrines récentes sur le commandement des engagements opérationnels hors du territoire national (CEO) et sur l'ASI qui fournissent déjà des instruments pédagogiques qui prescrivent des arrangements de C2 entre composantes permettant une intégration opérationnelle à haut niveau. Pour développer cette intégration vers le bas, l'approche incrémentale fondée sur une suite d'expérimentations tactiques, mission par mission, se développe comme le proposent divers officiers de TACP de l'USAF. Pour la développer l'on peut envisager une extension de la logique DACAS et/ou une extension des procédés de conduite en mode collaboratif du processus de TST qui associe l'ensemble des composantes au niveau des états-majors interarmées de coalition.

Se pose la problématique de la doctrine et des organisations : quel doit être le niveau de contrôle de l'engagement, selon quelle organisation, en vertu de quels principes partagés?

Le défi d'une intégration opérationnelle en temps proche du réel est de pouvoir affecter en vertu du principe de subsidiarité les autorités de prise de décision au niveau le plus élevé en fonction du contexte opérationnel : nécessité de flexibiliser et rendre dynamique la délégation au sein d'une composante ou le transfert vers une autre composante tactique des moyens employés.

Autre problématique : l'information à partager. Il faut élaborer une série de Joint Mission Thread (JMT) articulant les effets à réaliser et la séquence des actions associées à la mission considérée et les échanges d'information entre les acteurs impliqués.

Ce développement irait avec celui de l'interopérabilité technique des éléments de C2, ex : entre CAOC/AWACS, porte-avions Hawkeye/frégates ou chasseurs utilisés en noeuds tactiques et PC terrestres gérant l'ALAT et les feux. Le développement de telles interfaces nécessite de prendre en compte le développement des nouvelles architectures de chaque armée (SIC-S, Connect@aéron, Axon@V...). Il serait aussi logique de développer des TTP communes en matière de guerre cyber-électronique.

Le défi auquel se heurte cette intégration opérationnelle réside dans la formation et l'entraînement :

- . nécessité de maintenir les savoir-faire en matière de gestion des appuis et des soutiens
- . nécessité de faire des TTPs d'intégration
- . nécessité de trouver une place dans les cursus de formation et les exercices interarmées
- . nécessité de mettre en réseau l'ensemble des sites d'entraînement ainsi que le recours aux outils de stimulation sous-exploités actuellement

. sur le long terme : le développement du combat collaboratif fondé sur la symbiose. Il serait nécessaire à plus long terme de développer un combat collaboratif interarmées réel intégrant les systèmes, les éléments ISR et effecteurs terrestres, aériens et navals pour les missions considérées. Cette interopérabilité implique une doctrine interarmées et des TTPs de combat collaboratif consolidant le champ normatif.

Sur le plan technique et normatif, chaque armée est engagée dans le plan de son architecture future :

- . SIC-S puis Titan ainsi que les chaînes fonctionnelles (ATLAS, MARTHA) pour l'armée de Terre
- . Connect@aéro, l'opération de mise en cohérence numérique, étape vers le SCAF pour l'armée de l'Air

. la Veille Coopérative Navale (VCN) puis la Veille Coopérative Aéromaritime (VCAM) enfin le combat collaboratif naval pour la Marine, adossés à la nouvelle architecture de communication développée avec Axon@V

La convergences de ces projets permet la réalisation d'opérations multiplateformes. La démarche implique une synchronisation des projets. Il est possible aussi de créer de nouvelles organisations intégrées de combat collaboratif multidomaine.

mai 2022

ANNEXE

Parmi les programme en cours, nous pouvons évoquer le programme SCORPION ou le programme MYRIADE.

LE PROGRAMME SCORPION

Le programme d'armement Scorpion : "Synergie du COntract Renforcé par la Polyvalence et l'info valorisatiON" se déroule sur une période de 20 ans en deux étapes.

L'étape 1 couvre la période 2015-2027 et correspond au déploiement de 800 Griffon et 110 Jaguar sur 41 sites (au profit de 44 formations).

La réalisation d'un programme "infrastructures Scorpion étape 1", adossé à l'étape 1 du programme d'armement sera prochainement finalisé. Il consiste à mettre à niveau les infrastructures des formations de l'armée de Terre dotées des matériels de nouvelle génération pour leur permettre d'une part de donner et d'entraîner leur personnel et d'autre part d'assurer le maintien en condition opérationnelle.

L'étape 2 se déroulera à partir de 2026 avec le déploiement complémentaire de 1018 Griffon, 190 Jaguar, 1998 Serval, 54 MEPAC (Griffon avec mortier embarqué), 77 MAC (Moyen du génie d'Appui au Contact, le successeur des EBG) et 1600 VBAE (Véhicule blindé d'aide à l'engagement) au profit de 90 formations environ.

L'étape 2 "infrastructures Scorpion étape 2" sera mise en oeuvre afin d'accompagner ce second déploiement. Il prévoit un marché passé en externalisation de la réalisation des études initiales de faisabilité sur l'ensemble des emprises ; il s'agit de pouvoir déterminer s'il faut en matière d'infrastructures réhabiliter soit de l'existant, soit construire du neuf et affiner le coût prévisionnel de l'étape 2. Une synthèse permettra de consolider la vision du programme d'investissement sur le territoire. Ce marché portera sur les fonctions suivantes : stationnement des véhicules, atelier de maintenance NT1 et 2, atelier multitechnique, station d'entretien, station de lavage et station carburant.

PROJET MYRIADE

Au Forum Innovation Défense de 2021, la ministre des Armées évoque "les possibilités d'une nouvelle forme de menace combinant des capacités dans la manipulation de l'information, de désinformation, de cybernétique, de psychologie, d'ingénierie sociale, de biotechnologie et que l'on pourrait résumer en une sorte de nouvelle forme de guerre : la guerre cognitive". « La guerre cognitive, c'est la capacité à exploiter les vulnérabilités du cerveau humain en ayant recours à toutes les méthodes que je viens de citer » a poursuivi Mme Parly.

Le ministère des Armées investit dans la "guerre cognitive" avec le projet Myriade. Il vise à comprendre, anticiper et identifier les facteurs critiques de la guerre cognitive, cette capacité à exploiter les vulnérabilités du cerveau humain.

La guerre cognitive consiste à s'adresser à des groupes d'individus, de profiter de leur crédulité pour leur faire croire ce que l'on veut afin d'obtenir un effet tactique, voire stratégique quand il faut déstabiliser une société dans le cadre d'une campagne sur le long terme.

Les progrès technologiques, en particulier dans les domaines de la cybernétique et des biotechnologies, associés aux connaissances nouvelles en matière de neurosciences,

fait qu'il est plus facile d'exploiter les faiblesses du cerveau humain.

Le sociologue Gérard Bronner explique qu'il est aisé de trouver une information qui confirme nos croyances : "Une information (politique dans le cas de son expérimentation) contraire à nos idées excite des modules cérébraux essentiels dans l'évaluation du moi... la rencontre d'informations contradictoires à nos croyances nous met en danger, au moins au sens figuré : elle représente une attaque à notre identité. La crédulité, parce qu'elle est véloce, est souvent la première forme de narration qui s'offre à rendre compte d'un phénomène énigmatique. Dans ces conditions, elle a des chances d'ancrer en nous des formes de représentation du monde auxquelles nous nous mettrons à tenir dès lors que nous les aurons endossées".

Il ajoute la loi de Brandolini : "la quantité d'énergie nécessaire à réfuter des idioties est supérieure à celle qu'il faut pour les produire", la "crédulité possède un avantage concurrentiel sur le marché cognitif dérégulé car rétablir la vérité est souvent plus coûteux que de la travestir".

Ce que Tocqueville décrivait en affirmant qu'une "idée fausse mais claire et précise, aura toujours plus de puissance dans le monde qu'une idée vraie, mais complexe". L'on peut en conclure que les infox se diffusent plus rapidement et largement que les vraies.

Ex - Une étude publiée par l'OTAN en mai 2021 explique qu'il suffit d'un "document officiel embarrassant, piraté à partir de la messagerie d'un responsable public et partagé anonymement sur un média social ou diffusé de manière ciblée à des groupes d'opposition sur un réseau social, pour créer de la dissension". Et d'ajouter : « Si les faux comptes sur les médias sociaux ou les bots, avec leurs messages automatisés, peuvent renforcer cette dynamique, ils ne sont pas indispensables [une étude récente du MIT a montré que les seules émotions de la surprise et du dégoût suffisaient pour que les messages se répandent comme une traînée de poudre, repartagés en une fraction de seconde par des utilisateurs ordinaires ».

A souligner le rôle prépondérant des réseaux sociaux car ils tendent à monopoliser l'attention.

QUELQUES REFERENCES

http://www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf

https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2075/RAND_RR2075.pdf

<https://www.navalnews.com/naval-news/2020/03/u-s-french-navies-conduct-dual-carrier-ops-in-mediterranean/>

<https://www.colsbleus.fr/articles/10553>

<http://www.cjoscoe.org/infosite/wp-content/uploads/2018/10/Allied-Interoperability-and-Coordination-Guide.pdf>

<https://theatrum-belli.com/interoperabilite-on-peut-encore-sameliorer/>

<http://www.assemblee-nationale.fr/14/cr-cdef/14-15/c1415049.asp>

https://storage.nisp.nw3.dk/20181118_Final_FMN_Spiral_3_Standards_Profile_Bundle.pdf

<https://www.defense.gouv.fr/dga/actualite/le-systeme-d-information-des-armees-sia-a->

[l- heure-du-standard-fmn-de-l-otan](#)

https://www.afcea.de/fileadmin/user_upload/Sonderveranstaltungen/FA_mit_FueUstgKdoBw/13-NCIA-FMN1.pdf

<https://publications.ffi.no/nb/item/asset/dspace:4084/1302683.pdf>

<https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=531>

<https://www.bruxelles2.eu/2019/12/le-fonds-europeen-de-defense-rapiece-est-ce-grave-docteur/>

https://www.wirelessinnovation.org/assets/Proceedings/2019Europe/TS0.1_20190516_TE_N%20Wireless%20Comms%20Forum.pdf

<https://forcesoperations.com/camo-derriere-lequipement-la-construction-dun-modele-dinteroperabilite/>

<https://finabel.org/latest-developments-on-german-interoperability-efforts/>

<https://breakingdefense.com/2020/04/dod-budget-cuts-likely-as-4-trillion-deficit-looms/>

<https://www.nytimes.com/2020/02/27/world/africa/terrorism-west-africa.html>

<https://www.viavisolutions.com/en-us/literature/enduring-myths-software-communications-architecture-sca-white-paper-en.pdf>

<http://www.occar.int/programmes/essor>

<https://futurenetworks.ieee.org/images/files/pdf/FirstResponder/2019/Jack-Burbank.pdf>
<https://www.afcea.org/content/5g-offers-opportunity-improved-allied-and-coalition-communications>