NOTE 13

Avril 2020

Note n° 223/Consortium CONFLITS-2035
version finale du 19 novembre 2020

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

Les nouveaux enjeux de l'interopérabilité

PHILIPPE GROS

En partenariat avec

WWW.FRSTRATEGIE.ORG | 4 BIS RUE DES PATURES 75016 PARIS | TEL : 01.43.13.77.77 | MAIL : CONTACT@FRSTRATEGIE.FR

SIRET 39409553300052 TVA FR74 394 095 533 CODE APE 7220Z FONDATION RECONNUE D'UTILITÉ PUBLIQUE DÉCRET DU 26 FÉVRIER 1993

WWW.IFRI.ORG | 27 RUE DE LA PROCESSION 75015 PARIS | TEL : 01.40.6.60.00 | MAIL : ACCUEIL@IFRI.ORG
SIRET 78430892600038 TVA FR21 78 43 08 926 – APE 7220Z ASSOCIATION DE LA LOI 1901 RECONNUE D'UTILITE PUBLIQUE – DECRET DU 8/9/1949

Table des abréviations

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

SOMMAIRE

Les nouveaux enjeux de l'interopérabilité

Résumé

Les travaux menés ces dernières décennies sur l'interopérabilité ont abouti à l'empilement de nombreuses définitions n'étant pas toujours cohérentes. La présente note propose donc tout d'abord un cadre terminologique unifié, englobant les trois domaines de l'interopérabilité : interarmées, international et « interagences » (ou d'approche globale). Entre les forces, unités ou systèmes impliqués, l'interopérabilité relève de plusieurs niveaux : la « déconfliction », la coordination, l'intégration opérationnelle (que l'on peut nommer aussi coopération ou fédération) enfin, l'« intégration des systèmes » (ou symbiose tactique). Elle peut être bâtie « par conception » ou rester de circonstance (pour une opération). Elle se concrétise dans quatre champs : stratégique (qui conditionne les règles d'engagement ou encore le partage de l'information), culturel, normatif opérationnel et technique, auxquels contribuent les opérations elles-mêmes et les multiples procédés capacitaires : doctrines et TTP, exercices, formation, etc.

Le bilan de l'interopérabilité de nos armées reste assez mitigé. Sur le plan international, elle reste avant tout de circonstance même si elle peut se traduire par des niveaux poussés d'intégration opérationnelle dans les opérations aériennes et navales, notamment avec les alliés anglo-saxons. Il convient dans ce contexte de marquer la différence entre les Américains et les autres alliés de l'OTAN. C'est avec les premiers que le champ stratégique est le plus problématique. Sur le plan interarmées, elle est plus pérenne mais reste perfectible, sa principale limitation résidant probablement dans le champ culturel entre armées. Plusieurs initiatives en cours la renforcent : le *Federated Mission Networking* de l'OTAN, la coopération structurée permanente de l'UE, le *Mission Partner Environment* américain, les initiatives d'intégration ciblée comme CAMO, les démarches équivalentes de nos partenaires, notamment l'Allemagne, mais aussi le développement de « systèmes de systèmes » comme le SCAF. De nombreux facteurs vont contribuer à en faire évoluer les conditions et les niveaux : l'incertitude quant à nos partenariats stratégiques, qu'aggrave la crise actuelle ; l'évolution des systèmes d'information et de communication (diffusion des radios logicielles, mise en place de « *clouds* tactiques » qui devraient faciliter la coordination mais compliquer l'atteinte de niveaux d'intégration plus poussés), l'émergence du combat collaboratif et des opérations multidomaines ; enfin, l'accélération des stratégies de modernisation, notamment outre-Atlantique.

Dans cet environnement, si l'interopérabilité avec nos alliés – en premier lieu américains et britanniques, en second lieu nos autres partenaires européens – doit être approfondie, elle continuera d'être limitée, notamment dans les champs stratégique et technique. Surtout,

étant donné les incertitudes sur l'avenir de ces partenariats, la priorité absolue pour la France doit être accordée à l'amélioration de l'interopérabilité interarmées, tant pour garantir l'efficacité de forces aux formats contraints que pour permettre à la France d'assurer le rôle de matrice d'intégration interarmées d'une coalition limitée à quelques partenaires. Il s'agit en particulier d'étendre le champ des opérations multidomaines au sein des forces françaises. Une progression passant par l'extension progressive de l'intégration opérationnelle actuelle puis par la recherche d'effets de symbiose sélectifs entre les futurs « systèmes de systèmes » d'armée (Scorpion, SCAF, etc.) pourrait être une approche intéressante.

Introduction

La question de l'interopérabilité est aussi ancienne que les opérations militaires elles-mêmes dans la mesure où ces dernières ont toujours relevé de la combinaison d'armes disparates au sein d'une même force ou de celle de plusieurs entités stratégiques distinctes, qu'il convient de faire combattre ensemble pour assurer le succès de l'entreprise. La célèbre phrase de Foch, « *J'ai beaucoup moins d'admiration pour Napoléon depuis que j'ai commandé une coalition* » en souligne tout le défi. L'action interarmes ou interarmées, condition indépassable de l'efficacité opérationnelle, repose sur cette interopérabilité.

Dans l'immédiat après-Guerre froide, la problématique de l'interopérabilité occupe le devant de la scène en raison de plusieurs enjeux nouveaux : la multiplication des opérations extérieures multinationales, l'émergence concomitante des doctrines et institutions interarmées, la généralisation des systèmes d'information et de communication, enfin la redécouverte des exigences « d'approche globale » pour mener à bien les campagnes de stabilisation et de contre-insurrection.

Trois raisons amènent aujourd'hui à réexaminer la problématique de l'interopérabilité. En premier lieu, les travaux de ces trois dernières décennies et la diversité des cadres d'interopérabilité qui se sont succédé ont amené un empilement de définitions et de typologies n'étant pas toujours cohérentes. Il importe dans un premier temps de s'attarder sur ce cadre théorique en vue de le clarifier. En second lieu, le paysage stratégique évolue et avec lui la nature des partenariats opérationnels motivant l'interopérabilité. En troisième lieu, la révolution des technologies de l'information, marquée par exemple par l'émergence des technologies du « *cloud* », renouvelle la question de l'interopérabilité technique entre armées. Elle ouvre la voie à de nouvelles capacités opérationnelles, comme le combat collaboratif, qui à leur tour changent la donne en matière d'interopérabilité. Ces réflexions sont l'objet de la seconde partie.

Ce cadre et ces réflexions permettent de développer des implications et recommandations pour les armées françaises, qui feront l'objet d'une troisième partie. Contrairement aux autres travaux, dans la mesure où nous traitons précisément de l'interopérabilité entre nos armées, nous avons pris le parti de ne pas découper ces recommandations par armées, ce qui aurait constitué des développements redondants.

Partie 1 – Rappel du cadre de l'interopérabilité

1. Les définitions de l'interopérabilité

Comme tous les sujets complexes, l'interopérabilité fait l'objet d'un empilement de définitions. Le glossaire de terminologie opérationnelle n'en comprend pas moins de trois. La définition d'ordre général est la suivante :

> *Capacité de plusieurs systèmes, unités ou organismes à opérer ensemble grâce à la compatibilité de leurs organisations, doctrines, procédures, équipements et relations respectives. Note : l'interopérabilité porte sur les domaines des opérations, du matériel et de l'administration. On distingue trois niveaux croissants d'interopérabilité :*
>
> - *la compatibilité ;*
> - *l'interchangeabilité ;*
> - *la communité.*

Cette définition porte principalement sur le *comment*. Elle juxtapose deux apports contradictoires. Ainsi la première phrase associe l'interopérabilité à la simple « compatibilité » quand la seconde évoque trois niveaux croissants, parmi lesquels la compatibilité.

En réalité, deux visions de l'interopérabilité se dégagent parmi bon nombre de spécialistes : l'une, étroite, privilégiant la compatibilité mais excluant des notions telles que l'intégration, et une autre vision plus englobante. Le parti pris de cette note est de reprendre cette vision la plus extensive dans la mesure où elle permet d'engerber toute la richesse de la problématique qu'implique « opérer ensemble ».

Cette définition coexiste avec deux autres, émanant de la version 2010 de l'AAP-6 de OTAN :

> ***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 qui leur sont confiées.*
>
> ***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 qui leur sont confiées.*

Dans ces définitions, on ne parle plus de systèmes et d'unités mais uniquement de « forces » et on peine à distinguer les deux. Or, la définition de l'OTAN a elle-même évolué. Dans sa politique actuelle d'interopérabilité, l'Alliance définit l'interopérabilité comme étant :

> *L'aptitude à agir ensemble de manière cohérente, efficace et efficiente afin d'atteindre les objectifs tactiques, opérationnels et stratégiques de l'Alliance.*
>
> *Elle permet plus particulièrement aux forces, aux unités et/ou aux systèmes de fonctionner ensemble et de partager une doctrine et des procédures communes, ainsi que leurs infrastructures et leurs bases respectives, et de communiquer les uns avec les autres. L'interopérabilité permet d'éviter les doubles emplois, de mettre en commun les ressources et de créer des synergies entre tous les Alliés et, chaque fois que possible, avec les pays partenaires.*

Mentionnons en premier lieu une formulation surprenante : l'interopérabilité nous semble « découler » plus que « permettre » le partage des doctrines et autres. Ensuite, cette définition de l'OTAN est très prescriptive, peut-être trop. Si elle rétablit la gradation système / unité / force, elle précise également la communité (ou l'identité) des doctrines et des procédures, ce qui va au-delà de la compatibilité. Enfin, en étant caractérisée comme permettant « d'éviter les doublons » et « de mettre en commun les ressources », elle implique une intégration des stratégies capacitaires qui va au-delà des intentions affichées par la première phrase. Cette première phrase de la définition otanienne est une reprise de la définition interarmées américaine de portée générale, le *Joint Staff* en ayant une seconde, applicable plus spécifiquement aux systèmes d'information et de communication.

> 1. *The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. (JP 3-0)*
>
> *2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. (JP 6-0).*

Comme s'y réfèrent les chercheurs de la RAND dans une étude de 2019, une autre définition datant des années 1970 fut longtemps la plus utilisée chez les Américains, et mérite l'attention :

> *The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.*

Cette définition présente le grand avantage d'expliquer ce que signifie l'interopérabilité en termes de relations concrètes entre systèmes, unités et forces, *stricto sensu* mais selon des termes assez génériques. Elle reste évasive quant aux finalités. Il est proposé d'évacuer de la définition proprement dite la question des degrés que nous allons aborder ensuite. En combinant les éléments de ces définitions, il est donc possible de proposer la définition de travail suivante :

> *La capacité des systèmes, unités ou forces à fournir des services à d'autres systèmes, unités ou forces et à accepter des services de ceux-ci, et à utiliser les services ainsi échangés pour leur permettre de fonctionner ensemble de manière cohérente, efficace et efficiente, afin d'atteindre les objectifs tactiques, opérationnels et stratégiques fixés.*

2. Finalités générales et dimensions de l'interopérabilité

Il apparaît que l'interopérabilité relève de deux finalités :

- Elle relève tout d'abord de **l'exigence opérationnelle**, relative à la **sécurité des opérations**. Il s'agit simplement d'éviter que les éléments d'une force interfèrent mutuellement sous la forme de parasitage, d'accident, voire de tir fratricide ;
- Elle représente ensuite **une condition nécessaire de l'efficacité et de l'efficience des opérations** exécutées par différents systèmes, unités et forces, comme le précisent les définitions. Sans interopérabilité, l'emploi synergétique de ces éléments n'est pas possible ou reste hasardeux.

L'interopérabilité d'un appareil militaire relève de trois domaines :

- **L'interopérabilité interarmées**, entre composantes de milieu. Son application au niveau national devrait représenter, en théorie, le socle garantissant un emploi cohérent de l'instrument militaire. En réalité, elle n'est pas la plus facile à développer. Cette interopérabilité interarmées connaît aujourd'hui un prolongement spécifique avec la notion d'opérations « multidomaines » ;
- **L'interopérabilité internationale**, la faculté à opérer avec les forces partenaires (alliées, dans un cadre multilatéral, ou coalisées, dans un cadre multinational). Dans la période actuelle, elle fait l'objet des développements les plus nombreux ;
- **L'interopérabilité au profit de « l'approche globale »** incluant les volets interministériel et « interagences »**,** c'est-à-dire l'interopérabilité avec les autres acteurs impliqués dans l'entreprise stratégique considérée : acteurs institutionnels français (MEAE, AFD, etc.), autorités et institutions du pays hôte, organisations internationales, ONG, etc. Elle représente un impératif des engagements de gestion de crise, de sécurisation et, bien entendu, des campagnes visant des objectifs de restructuration politique.

3. La gradation de l'interopérabilité

3.1. Les niveaux d'interopérabilité

Les systèmes, unités ou forces peuvent être interopérables à des degrés divers selon la conception retenue *supra*. Une première approche consiste à qualifier l'échelle des relations entre ces éléments. Comme exposé dans notre note sur le multidomaine, les Américains, notamment les cénacles interarmées, ont conçu puis actualisé une démarche au long court intégratrice de leurs appareils de force comme un guide de stratégie capacitaire. La démarche de l'OTAN avec la mise en œuvre de la NNEC poursuit la même logique tout en proposant une typologie sensiblement différente[1]. En combinant les deux, on peut avancer les niveaux d'interopérabilité suivants :

1. La « ***déconfliction*** **»**, la gestion des interférences entre forces menant des opérations de façon autonome ;

2. La **coordination**, signifiant que les différentes composantes sont employées de façon synchronisée via un CONOPS ou un OPLAN/OPORD commun de niveau supérieur. Selon l'OTAN, elle se traduit aussi par une tenue de situation commune, réalisée *a minima* ;

3. L'**intégration opérationnelle, la coopération ou la fédération.** Les Américains retiennent à ce stade la notion d'intégration qu'ils définissent comme « *The arrangement of military forces and their actions to create a force that operates by engaging as a whole* »[2]. En fait, cette définition recouvre des réalités variées. Selon nous, elle doit être comprise ici comme la constitution d'un système de force unique au niveau opératif, voire au niveau tactique, dans un milieu et/ou pour une fonction opérationnelle donnée, d'où notre proposition du terme « d'intégration opérationnelle ». Par référence aux désignations dans le domaine de l'entreprise, il nous semble également juste de parler ici de coopération. Il peut aussi être intéressant d'attribuer un sens élargi à la notion de « fédération » que l'OTAN utilise dans le domaine des systèmes d'information (sur lequel nous revenons plus bas) mais qui correspond bien à ce niveau dans lequel il s'agit de créer des interfaces entre forces, composantes ou unités conservant leur homogénéité ;

4. Le niveau de **symbiose** ou **d'intégration système** de préférence à la notion de « synergie » avancée par les Américains mais qui reste trop générale[3]. L'OTAN évoquait pour sa part le terme intéressant **« d'effets cohérents »**, qui serait là encore l'objectif ultime de la NNEC. En réalité, ce dont on parle ici renvoie à une étape de l'intégration combinant différents systèmes pour composer à la demande un unique système d'arme/C2/ISR au niveau engagement d'où l'utilisation du terme de symbiose par analogie à la biologie dans laquelle elle est définie comme « *l'association étroite de deux ou plusieurs organismes différents, mutuellement bénéfique, voire indispensable à leur survie* ». Cette intégration s'opère entre systèmes d'un même milieu ou en multidomaine. Elle se concrétise tout particulièrement dans la notion de **combat collaboratif, multiplateforme**. L'armée de l'Air définit en effet le « combat collaboratif connecté » comme « *une 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 alors sur celle de meilleure performance individuelle, y compris entre systèmes hétérogènes, et ce quel que soit le milieu* »[4].

En revanche, l'interopérabilité suppose, en soi, que les forces qui opèrent restent distinctes. En ce sens, le partage de forces (*pooling and sharing*) représente un niveau d'intégration organique dépassant l'interopérabilité. Le niveau interarmées américain a rajouté, puis retiré par la suite, le niveau de **l'interdépendance** par lequel les éléments interopérables consentent une dépendance mutuelle de leurs capacités. Ainsi, dans la logique américaine, alors que l'intégration vise avant tout l'efficacité, l'interdépendance vise l'efficience, la lutte contre les redondances dans un contexte budgétaire contraint. Cependant, l'interdépendance devient indissociable des niveaux d'intégration, dans la mesure où un appareil de force privé de l'un de ces éléments peut devenir incohérent et ne peut plus atteindre ses objectifs.

3.2. Interopérabilité et dimensions temporelles

La gradation de l'interopérabilité peut se mesurer également à l'aune de la temporalité des cycles décisionnels en opérations réalisées de conserve. Ainsi :

- L'interopérabilité peut se borner à la **planification opérationnelle** et à la **conduite des opérations en temps réfléchi** (par exemple, le cadre du cycle de l'*Air Tasking Order* ou encore de la manœuvre future des unités terrestres). Elle peut impliquer un niveau de coordination voire d'intégration ;
- Elle peut également être réalisée pour la **conduite des opérations en temps proche du réel** qui exige réactivité comme par exemple une mission de ciblage d'opportunité, d'appui aérien rapproché non planifié ou encore de RESCO, plus généralement la conduite du combat tactique en cours et, pour certaines missions, les nouvelles perspectives de combat collaboratif. Être interopérable en temps réel apparaît indissociable d'une forme d'intégration ;
- Enfin, son plus gros défi concerne les **opérations en temps « immédiat » ou « réflexe »**, le propre des situations opérationnelles les plus rapidement évolutives comme la défense antiaérienne et antimissile, la gestion de l'espace aérien et d'autres formes du combat collaboratif.

Dans la pratique, **les relations entre les forces impliquées se situent rarement à un niveau unique sur ces échelles d'interopérabilité**. Pour certaines missions ou fonctions opérationnelles, la coordination, sinon la déconfliction, s'avèrera suffisante alors que d'autres éléments seront ou devront être intégrés. Structurellement, compte tenu des différences de fluidité propre à chaque milieu, l'interopérabilité dans le milieu terrestre procède du mariage de situations hétérogènes entre coordination et intégration alors que l'interopérabilité dans les milieux naval ou aérien sera plutôt synonyme de formes variées d'intégration.

3.3. Le différentiel capacitaire : un facteur d'interopérabilité en interallié

Dans les opérations internationales, rien n'empêche des forces de capacités asymétriques d'opérer ensemble. Cependant, ce différentiel capacitaire va mécaniquement conditionner le niveau d'interopérabilité *stricto sensu* réalisable en dictant le degré de partenariat opérationnel envisageable. Par exemple, en 2003, en Irak, les Britanniques ont été chargés de la prise de Bassorah car l'interopérabilité avec l'US Army n'était pas suffisante pour permettre leur intégration dans la manœuvre exécutée par les forces terrestres américaines vers Bagdad. À un autre niveau, le différentiel de capacités entre Barkhane/Sabre et les forces du G5 ne prédispose pas ces dernières à participer à nos opérations les plus exigeantes contre les groupes djihadistes. Deux schémas émergent donc :

- **La logique de l'intégration opérationnelle voire de la symbiose tactique dans des manœuvres communes,** aéroterrestres ou autres, constituant la ou les lignes d'opérations principales du mode d'action exécuté ;
- **La logique de la niche opérationnelle** reposant principalement sur la coordination, confiée à la force ou aux forces moins « capables » que la force principale. Il peut s'agir principalement d'une mission ou d'une zone d'opération spécifiques.

4. Les modalités de développement de l'interopérabilité

4.1. Interopérabilité par conception et interopérabilité de circonstance

Il existe fondamentalement deux façons de construire une interopérabilité :

- **La plus évidente est de la bâtir au long terme par le biais de la stratégie capacitaire**. Cette approche est implicite dans les axes des stratégies générales militaires, nationales ou multilatérales. **« L'interopérabilité par conception » (*interoperability by design*)** qu'elle représente reste cependant un objectif élusif dans la mesure où elle nécessite d'harmoniser les décisions de décideurs multiples aux impératifs divergents en matière de priorités, d'agenda et de budgets.
- **D'où une interopérabilité de circonstance construite dans le cadre d'un engagement, par nécessité** de parvenir à une efficacité opérationnelle immédiate. Elle est facilitée par l'existence d'un commandeur opérationnel et/ou d'un partenaire dominant imposant ses choix. Ainsi, les Américains ont imposé leurs choix à leurs partenaires en matière de SIC en Irak ou encore pour certaines missions en Afghanistan (exemple du Rover pour les missions CAS). Elle se construit aussi par l'intermédiation des détachements de liaison qui représentent dans bien des cas une solution aussi nécessaire que suffisante.

Cependant, cette interopérabilité de circonstance n'est pas en soi pérenne. Le lien avec la stratégie capacitaire provient alors de la durée de l'engagement qui enracine et institutionnalise les arrangements entre partenaires. C'est précisément ce que bâtit l'OTAN avec le *Federated Mission Networking* (FMN) sur la base des enseignements de l'*Afghan Mission Network* (AMN). Les chercheurs de la RAND distinguent pour leur part deux ambitions d'interopérabilité :

- **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 quant à elle « *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* »[5].

4.2. Les quatre champs constitutifs de l'interopérabilité

L'interopérabilité découle ainsi fondamentalement de la faculté de plusieurs entités à pouvoir légalement, matériellement et politiquement opérer ensemble, à se comprendre puis à échanger ou partager de l'information, des biens et des services. En d'autres termes, le niveau d'interopérabilité réalisable découle de quatre champs de convergence.

4.2.1. Le champ stratégique

Il va de soi pour la dimension interarmées, raison pour laquelle il est largement absent des typologies américaines qui visent avant tout à jalonner intellectuellement la *Jointness* nationale. Il est en revanche primordial pour l'interopérabilité multinationale. L'interopérabilité découle largement en effet de la cohérence des cadres stratégiques d'engagement, laquelle se concrétise dans trois problématiques de compatibilité :

- Celle **des objectifs** confiés à la force **et de la stratégie opérationnelle** adoptée, traduits directement par les niveaux d'investissement et les ***caveats*** nationaux conditionnant l'emploi de chaque force ;
- Celle des **cadres juridiques** conditionnant ces engagements, tout particulièrement la question des règles d'engagement (ROE) ;
- Celle des **règles de partage des données opérationnelles nécessaires**, notamment le renseignement. L'essentiel de la question se situe là encore au croisement des cadres juridiques nationaux et de la volonté politique.

4.2.2. Le champ culturel

Il renvoie tout d'abord à la compréhension des cultures stratégiques du ou des partenaires et des cultures institutionnelles des autres armées. Bien que floue, la notion de culture stratégique renvoie à une réalité : celle des prismes mentaux nationaux d'interprétation de leurs intérêts, des situations et des options stratégiques, de la conception du recours à la force et de la place et des logiques d'organisation de l'instrument militaire. À un second niveau intervient la compréhension des cultures institutionnelles qui caractérisent chaque armée. Elle se compose de trois sous-cultures : une culture opérationnelle (relative à la logique d'emploi des moyens, ce qui formalise une doctrine le cas échéant), une culture identitaire des personnels qui la compose et une culture « métier » avec ses pratiques, ses terminologies (etc.). Ces différentes sous-cultures, tout particulièrement la culture métier, se partagent entre armées de différentes nationalités. D'où le constat, maintes fois souligné, que deux pilotes de nations différentes se comprendront mieux qu'ils ne comprennent chacun leurs homologues respectifs des armées de Terre.

4.2.3. Le champ opérationnel

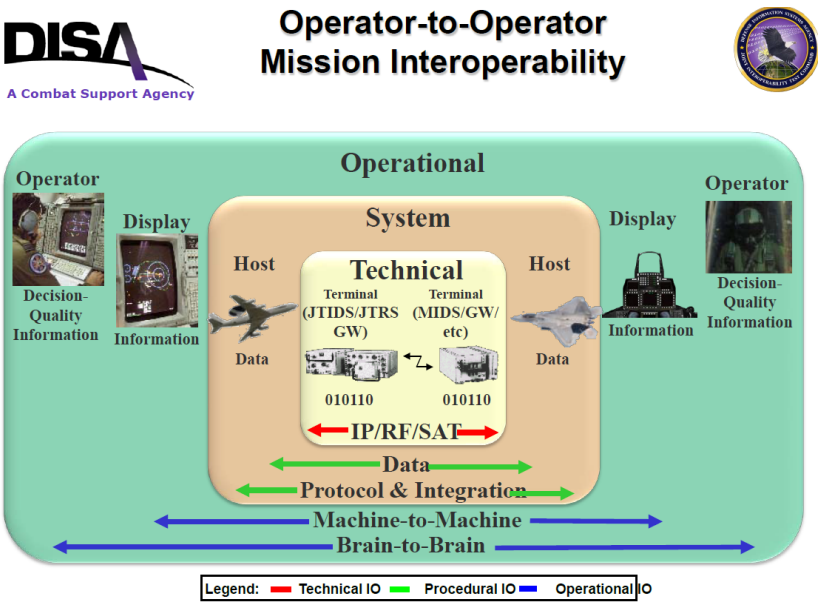
Il est constitué des **normes opérationnelles**. Il s'incarne dans la partie la plus prescriptive des doctrines, dans les tactiques, techniques, procédures (TTP), les *Standard Operating Procedures* (SOP) et les accords de standardisation codifiant les convergences en matière d'organisations et d'actions des différentes fonctions opérationnelles des systèmes de force en présence.

4.2.4. Le champ technique

C'est le champ le plus connu, celui des équipements et infrastructures**.** Bien entendu, l'exigence d'échanger les informations soulignée plus haut place **les systèmes d'information et de communication** (SIC) au premier plan des équipements considérés mais ce champ ne s'y limite nullement. L'interopérabilité technique se met en place à deux niveaux : celui de l'acquisition des équipements et celui des normes techniques dont la convergence permet

aux matériels et logiciels des partenaires de fonctionner de conserve. Il ne concerne pas uniquement les standards de fonctionnement de ces équipements mais aussi ceux structurant les données échangées, s'inscrivant pleinement dans le prolongement du champ précédent. On verra qu'à l'heure des « *clouds* », cette notion a une grande importance.

Les trois derniers champs sont assez proches de la classification de la *Defense Information System Agency* (DISA) américaine même si cette dernière, très orientée SIC, inclut les normes opérationnelles et techniques sous le même ensemble de l'interopérabilité technique et entre systèmes d'armes.



CIAV Management Group, *AMN Coalition Interoperability Assurance and Validation (CIAV)*, présentation, NDIA T&E Conference, 30 janvier 2012.

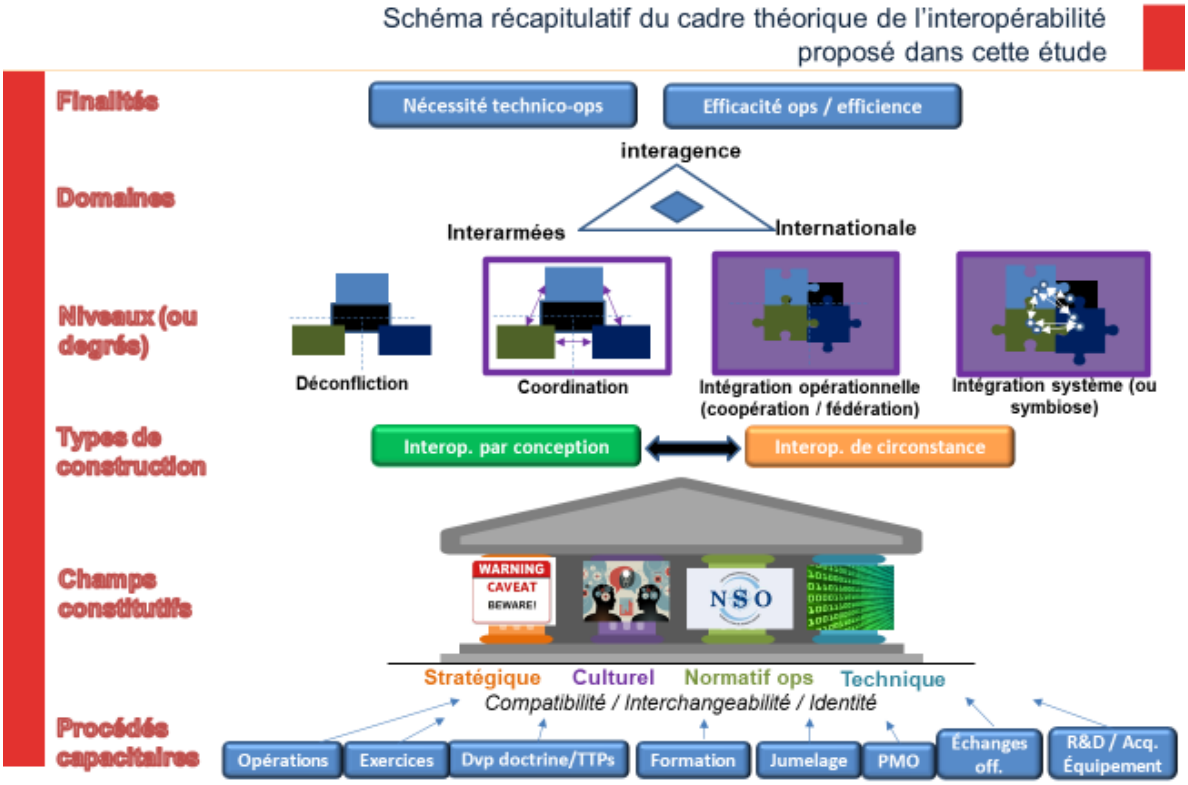
4.3. Les procédés capacitaires bâtissant l'interopérabilité

Les activités permettant de construire cette interopérabilité sont largement celles de la classification des domaines capacitaires, auxquelles s'ajoutent les opérations. Elles interviennent, à des degrés divers, pour développer l'interopérabilité selon les quatre champs considérés. Il s'agit ainsi :

- Des opérations elles-mêmes, le plus puissant moteur d'interopérabilité ;
- Des entraînements et exercices communs ;
- Des processus de développement commun des doctrines opérationnelles et tactiques, des TTP et standards ;
- Des jumelages d'unité ;
- Du partenariat militaire opérationnel ;
- De la formation, qui va contribuer surtout au champ culturel ;
- Des échanges d'officiers insérés ou de liaison ;
- Des équipements proprement dits, allant d'efforts de recherche et développement communs aux acquisitions partagées.

C'est ici qu'intervient la classification des « niveaux d'interopérabilité » proposés par les définitions *supra* (identité, interchangeabilité, compatibilité) qui qualifient les niveaux de convergence entre les objets tant intellectuels que matériels produits par chaque acteur dans ces différents domaines.

5. Schéma récapitulatif du cadre proposé



Partie 2 – Les nouveaux enjeux, défis et opportunités de l'interopérabilité

1. Une interopérabilité qui reste insuffisante

Il s'agit dans cette section de dresser un bref bilan de nos niveaux d'interopérabilité.

1.1. Interopérabilité multinationale

1.1.1. Les opérations aériennes et navales : une interopérabilité technico-opérationnelle réelle mais souvent de circonstance

L'interopérabilité de nos forces avec leurs alliés et partenaires dépend largement des milieux considérés. Globalement, elle reste cependant très imparfaite.

Ainsi, on peut avancer que **l'interopérabilité de la composante aérienne** avec ses alliés permet une coopération voire une intégration limitée, en raison d'opérations presque ininterrompues depuis au moins une douzaine d'années, mais aussi de l'homogénéité du milieu. Elle répond tout particulièrement aux exigences de sécurité des opérations. Ainsi :

- Dans le champ culturel, elle se fonde sur la référence commune à la notion d'*airpower*. Les doctrines semblent assez compatibles même si elles ont leurs spécificités ;
- Dans le champ normatif opérationnel, les forces aériennes partagent la même culture « métier », la même grammaire des opérations : organisation des JFAC et des CAOC, procédures dont l'exemple emblématique est le fameux cycle de l'ATO. Cependant, là encore, de nombreuses spécificités nationales existent ;
- Dans le champ technique, elle est permise au sein de l'OTAN par le réseau ACCS, par l'identité de certains systèmes clés uniques comme l'E-3 AWACS et l'E-2 Hawkeye, des systèmes comme les radios SATURN et la liaison 16 qui assurent la glu des dispositifs aériens même si, là encore, des incompatibilités peuvent parfois exister.

Celle de la Marine avec ses homologues de l'OTAN serait du même ordre. Elle découle d'une compatibilité, *a minima*, des procédures, entretenue là encore par la longue habitude des opérations (lutte contre la piraterie, opérations dans le Golfe, opérations au sein de l'OTAN) et de l'entraînement communs. Techniquement, elle est tout particulièrement réalisée via les liaisons de données (L11, L16, L22). Cette compatibilité permet depuis de nom-

breuses années de constituer des groupes de combat intégrés. Les amiraux américains et français, comme le Vice-amiral Isnard, qualifient l'interopérabilité des marines française et américaine de « *plug and fight* », de « *seamless interoperability* » permettant des « *high-end integrated operations* »[6]. Le commandement de la CTF50, *task force* aéronavale déployée dans le Golfe, confié en 2015 à la France par les États-Unis ou encore *« Chesapeake 2018 »*, cadre de l'accueil d'une unité de Rafale sur l'*USS George H. W. Bush*[7] témoignent de la reconnaissance de cette aptitude. Les Américains s'y réfèrent hors cadre bilatéral et sans présence de Français, ce qui est assez rare pour être souligné. Cependant, cette interopérabilité ne va pas jusqu'à l'intégration permettant des actions en temps réflexe.

Dans les deux cas et au niveau du C2 interarmées, elle est aussi techniquement réalisée par les réseaux de coalition, BICES ou de type CENTRIXS, déployés selon de multiples déclinaisons par les commandements opérationnels américains et qui permettent les échanges de base (services de messagerie, voix sur IP, de partage de la COP, etc.).

Cependant, on parle essentiellement ici **d'interopérabilité de circonstance**, **tout particulièrement avec les forces américaines**. La matrice d'intégration des coalitions que les forces américaines constituent, étant donné les asymétries capacitaires, est plurielle. Elle continue de se décliner en fonction des choix faits d'une part par les *Services* qui équipent et organisent les forces, d'autre part par les différents commandements opérationnels qui les emploient. Vu de Washington, l'OTAN n'est qu'un des éléments de l'équation et la majorité des forces américaines ne connaissent pas du tout l'Alliance. Les standards et équipements de ces forces, sur le continent ou relevant des autres commandements opérationnels (CENTCOM et INDOPACOM) sont souvent, par défaut, incompatibles avec leurs équivalents OTAN. Par exemple, le principal SIC opérationnel de l'USAF, le *Theater Battle Management Core Systems* (TBMCS) n'est interopérable qu'*a minima* avec l'ACCS de l'Alliance, développé entre partenaires européens. Certes, chaque commandement opérationnel américain fait un effort important pour intégrer ses partenaires via ses réseaux type CENTRIXS, mais selon les règles et procédures américaines. Créer un environnement interopérable nécessite donc un effort important de convergence lors des conférences de planification de chaque engagement tant en matière de normes opérationnelles que de SIC. Lors de cette planification et de la conduite de l'engagement, le rôle des officiers de liaison est primordial pour garantir la cohérence de l'attelage[8]. Enfin, une variable essentielle du niveau d'interopérabilité réside dans le champ stratégique (voir ci-dessous).

1.1.2. L'interopérabilité des forces terrestres : une situation plus problématique

La situation est encore différente en ce qui concerne les forces terrestres. Selon le général Margail, qui a commandé le CRR-FR, elle est relativement satisfaisante dans le domaine normatif opérationnel en dépit des nombreuses spécificités des doctrines tactiques. Les lignes de faille restent toutefois multiples comme entre forces occidentales historiques et forces des pays de l'Est qui seraient encore marquées par l'héritage soviétique[9]. Des centres comme le *Joint Maneuver Training Center* (JMTC) œuvrent au développement de TTP compatibles. La situation est plus problématique encore dans le domaine des SIC. Si elle est réalisée dans le cadre d'exercices dont la préparation permet de mettre sur pied une interopérabilité de circonstance, une mise en œuvre pérenne reste encore un vœu pieux[10].

De fait, structurellement, la multiplicité des fonctions et des niveaux hiérarchiques aux environnements opérationnels forcément hétérogènes favorise plus qu'ailleurs la fragmentation des systèmes, d'où un risque accru d'incompatibilité. Traditionnellement, l'interopérabilité multinationale s'articule à partir du niveau de la brigade, au mieux du GTIA, sauf pour certaines fonctions d'appui. Or, la tenue de la situation opérationnelle agrégée à ces niveaux découle des éléments des échelons subordonnés. Cette tenue de situation, dès lors, repose sur des pratiques et des systèmes propres à chaque armée de terre. Ainsi, les niveaux de numérisation restent extrêmement variés. Pas moins de 13 systèmes de suivi de la situation opérationnelle tactique (comme notre suite SIR/SITEL et le *Joint Battle Command-Platform* américain) sont utilisés par les armées de terre de l'OTAN. Ceci n'empêche nullement plusieurs fonctions opérationnelles de cultiver l'interopérabilité technique avec leur partenaires, comme les feux sol-sol, 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 ou encore les progrès sensibles enregistrés dans le *Digititally Aided-Close Air Support* (DACAS).

1.1.3. Le champ stratégique, « plafond de verre » pérenne de l'interopérabilité multinationale

Enfin, et de façon générale, **l'interopérabilité multinationale reste étroitement contrainte par les divergences nationales, qui varient d'une opération à l'autre**. Les trois principales sont probablement les ***caveats*, les règles d'engagement ainsi que les directives quant au partage de l'information**, tout particulièrement à l'échange de renseignement, qui ne va jamais de soi.

On a vu à quel point les multiples *caveats*, conditionnant en particulier l'action de nos partenaires européens, pouvaient entraver l'interopérabilité des forces de la coalition en Afghanistan ou encore, actuellement, au Sahel.

Une fois encore, le cas de l'allié américain se situe sur un autre registre. Le *Multinational Information Sharing* est mentionné comme une priorité dans les orientations stratégiques américaines depuis 2001. Cependant, il est mécaniquement limité en pratique. L'appui ISR américain, en particulier, est en théorie déterminant pour tout membre de la coalition. Or, les forces américaines opèrent principalement sur leurs réseaux nationaux SIPRNET et JWICS, auxquels seuls leurs partenaires des *Five Eyes* peuvent avoir un accès limité. La règle générale reste, par défaut, « retenir tout, partager par exception » (*withhold all, share by exception*)[11]. Les données transmises aux autres partenaires sont souvent dégradées tant en contenu qu'en délai de livraison par cette règle stricte de partage de l'information, appliquée par les *Foreign Disclosure Officers* (FDO).

Une raison majeure pouvant expliquer cette posture réside dans **l'asymétrie capacitaire et donc le degré d'utilité du partenariat pour Washington**. Lorsque les Américains assurent le leadership d'un engagement, ils se déploient avec l'ensemble des moyens nécessaires pour garantir l'atteinte de leurs objectifs. Il n'existe pas réellement d'interdépendance avec leurs partenaires qui sont attendus le cas échéant sur des capacités de niche ou pour renforcer le volume des moyens. En Afghanistan en 2001, comme en Irak en 2003, ou contre Daech en 2014, on peine à conclure que les capacités de combat des partenaires européens ont été absolument nécessaires au succès des armes de la coalition. Ce faisant, l'interopérabilité

pour Washington n'est probablement nécessaire que pour la gestion politique de cette coalition et au regard des exigences de sécurité des opérations. Il n'est alors pas étonnant qu'elle se traduise par un effort technique *a minima* et une absence de convergence sur certains points critiques dans le champ stratégique.

La perception qu'ont les Américains de l'utilité stratégique du partenariat varie cependant selon les circonstances, influençant alors ces règles de partage de l'information. Lors de l'opération *Unified Protector* en 2011, ces règles auraient évolué à l'été à l'initiative du Président Obama dans la perspective de la poussée décisive des insurgés vers Tripoli[12]. C'est plus encore le cas pour les opérations au Sahel où les Américains sont en appui des Français. Les échanges de renseignements et l'intégration y atteignent des niveaux équivalents à ceux des *Five Eyes*, tant au niveau stratégique, entre la DRM et les agences américaines, que sur le théâtre entre l'*US Special Operations Command* et le Commandement des opérations spéciales[13]. Le niveau d'interopérabilité vanté par les deux marines n'est probablement pas étranger non plus à la plus-value que constitue le groupe aéronaval français dans la conception d'une coalition permanente et flexible de marines, promue par la Navy depuis deux décennies. Au même moment, les échanges étaient beaucoup plus limités entre les autres composantes au sein de CENTCOM dans le cadre de la lutte contre Daech. On verra de plus ci-dessous que la pression augmente du côté américain pour améliorer cette capacité d'*information sharing*.

Il faut souligner que les mêmes limitations semblent émaner de notre fonction renseignement à destination des Américains ou d'autres partenaires. De fait, même si la France et bon nombre de ses alliés européens continentaux se prévalent d'une règle de partage de l'information inverse de celle des Anglo-saxons, les limites aux échanges n'auraient pas manqué non plus entre eux lors de plusieurs engagements récents.

1.1.4. L'interopérabilité « vers le bas »

La question de l'interopérabilité avec nos armées partenaires moins sophistiquées, en Afrique tout particulièrement, se pose de façon radicalement différente. Dans sa globalité, elle devrait en théorie être améliorée par les nombreux efforts de partenariat militaire opérationnel (PMO) : coopération structurelle pilotée par la DSCD ; actions des forces de présence et de souveraineté[14] ; plans de coopération opérationnelle, en l'occurrence avec les pays d'Afrique de l'Ouest ; actions du Centre de Préparation à l'Engagement Opérationnel (CPEO) ; coopérations en opération avec les détachements interarmes (DIA) fournis par les forces. Ces activités contribuent à former à des degrés divers des dizaines de milliers de personnels par an. Elles enregistrent cependant des résultats mitigés dans la mesure où, dans une posture de conseil, elles s'adressent souvent à des armées dont les failles – notamment politiques et sociétales – entravent structurellement leur fonctionnement comme institution et, *in fine*, leur efficacité[15].

Dans la pratique, en BSS, l'interopérabilité reste à un niveau de coordination, effective *a minima*. L'interopérabilité est réalisée en premier lieu au niveau des états-majors comme celui de la Force conjointe G5 Sahel (FC-G5S), par nos officiers de liaison qui y tiennent une place centrale dans les travaux de planification (le CEM est un colonel français). Le récent mécanisme de 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 de

renseignements et un poste de commandement conjoint – doit renforcer cette coordination. En second lieu, elle s'effectue de façon croissante au niveau des unités partenaires avec les formations du CPEO en amont des opérations et celles prodiguées par les DIA insérés. Ces dernières initiatives autorisent des opérations conjointes. Cependant, les attaques massives des camps militaires, comme celui des forces nigériennes à Inates, montrent, entre autres choses, les limites de cette coordination.

Cette interopérabilité reste de fait très problématique. Le volet des SIC ne semble pas le plus critique : compte tenu du dénuement de ces forces en la matière, l'interopérabilité consiste surtout, sur un mode dégradé, à établir et maintenir les communications radio. Elle est en revanche victime dans le domaine technique des multiples sources d'équipements des forces locales. C'est surtout dans le champ culturel et dans celui des normes opérationnelles que les défis sont les plus criants. Là encore, elle pâtit de l'éclatement des PMO, tant au niveau global que sur celui des théâtres d'opérations. Ensuite, bon nombre de ces partenariats consistent à enseigner les normes et processus d'état-major occidentaux à des officiers dont la culture est radicalement différente. Surtout, la situation plus générale qui caractérise ces armées d'États faibles ou faillis (niveaux d'attrition élevés, institutions militaires réduites, moral défaillant, etc.), limite l'effet d'une large part de ces coopérations structurelle et opérationnelle à une interopérabilité très circonstancielle, la plus efficace étant probablement la coopération en opérations.

1.2. Une interopérabilité interarmées incontestable mais perfectible

L'interopérabilité interarmées fait l'objet de beaucoup moins de publicité que celle entretenue avec nos partenaires, de sorte qu'il est particulièrement difficile d'en tirer une appréciation d'ensemble en source ouverte. On peut cependant avancer que si elle est incontestable sous de multiples aspects, elle demeure perfectible.

De fait, elle est incontestable parce que démontrée dans les engagements récents et actuels où elle est requise. Elle se concrétise par des échelons interarmées robustes du CPCO aux COMANFOR et par de multiples manifestations d'intégration opérationnelle, au niveau des composantes : opérations de l'ALAT depuis le BPC en Libye, ou plus généralement les appuis aériens quotidiens (ISR, feux ou encore transport) aux unités de l'armée de Terre dans le cadre de Barkhane. Elle est consolidée progressivement depuis 20 ans avec l'élaboration du corpus doctrinal interarmées du CICDE pour ce qui concerne les missions déjà multidomaines, et ces dernières années dans le domaine des SIC, au moins au niveau interarmées, avec et entre les états-majors de haut niveau, avec le déploiement du SIA.

Elle reste cependant fragile et très perfectible. Le maintien de l'interopérabilité des SIC sur un théâtre comme la BSS serait ainsi particulièrement difficile à obtenir[16]. Le principal obstacle reste de l'ordre du culturel et de certaines normes opérationnelles découlant des spécificités des cultures – voire des intérêts – des institutions. Par exemple, dans le domaine d'une opération multidomaine de longue date comme le CAS, après de nombreuses années d'opérations communes en Afghanistan et en Afrique, en dépit de normes identiques OTAN d'origine américaine et des productions du CICDE, les armées de Terre et de l'Air ne partageaient pas encore au milieu de la décennie la même vision des besoins d'échanges d'information entre les acteurs de cette mission (JTAC, aéronefs, PC, etc.) ; l'armée de l'Air et

la Marine n'étaient pas sur le même registre quant à la nécessité de la pratique de l'appui à basse altitude, etc. L'opération Serval aurait été le théâtre de friction entre l'armée de Terre et l'armée de l'Air quant à l'emploi de systèmes de coordination comme le CMD3D. Ces exemples sont probablement plus nombreux et continuent d'entraver l'interopérabilité de niveau intégration.

Enfin, notons que l'interopérabilité avec les Américains, en situation de forte asymétrie capacitaire, vise avant tout à incorporer les éléments de leurs partenaires, dont les nôtres, dans leurs composantes de force au sein d'une unique matrice interarmées américaine, ce qui ne favorise sans doute pas la consolidation de l'interopérabilité interarmées entre les composantes de force nationale.

1.3. L'interopérabilité au profit de l'approche globale en régression ?

L'interopérabilité interministérielle et plus généralement « l'approche globale » ont connu d'innombrables développements à l'occasion de l'engagement en Afghanistan. Elles semblent cependant susciter moins d'intérêt au sein des appareils de force occidentaux ces dernières années avec le « durcissement des postures stratégiques » et le retour de la compétition entre « États puissances ». Elles ne sont par ailleurs que peu mises en pratique au Sahel ou au Levant.

Certes, cette exigence est régulièrement mentionnée dans nos orientations stratégiques de 2012 et de 2017, comme le rappelle le CEMA. Tant l'OTAN que l'UE réaffirment leur rôles respectifs dans ces architectures, au demeurant plus large dans le second cas. Si les priorités américaines ne se situent plus sur ce registre, la préoccupation n'est pas non plus absente de leurs RETEX. L'OTAN puis le CICDE ont produit de nouvelles versions de leurs manuels de doctrine d'action civilo-militaire. Cependant, on est frappé par la fixité des discours depuis les développements de la précédente décennie, le rappel *ad nauseam* du besoin d'accroître la compréhension mutuelle grâce aux échanges et formations, le partage de l'appréciation de situation et la bonne synchronisation des actions militaires sur les perceptions, et l'environnement opérationnel et des activités des acteurs civils, fondé sur des mécanismes de coopération dans la planification, etc.

De fait, dans la pratique, cette interopérabilité semble avoir reculé, au moins chez nos partenaires. Par exemple, le *Center for Army Lessons Learned* américain rappelait en 2016 que le renseignement restait encore trop concentré sur la menace pour permettre une bonne compréhension de la complexité de l'environnement opérationnel ainsi que l'identification et le ciblage des sources d'instabilité. Il pointe également l'inefficacité des opérations civilo-militaires faute de synchronisation avec des acteurs civils mal identifiés tout autant que leurs pratiques, le manque de renseignement sur les attitudes et les perceptions des audiences cibles sapant tout effort d'opérations d'information efficaces[17]. Les unités américaines semblent donc avoir régressé par rapport aux efforts d'acculturation péniblement consentis dans le cadre de la COIN. Sur le plan technique, le *Multinational Capability Development Campaign* (MCDC) rappelle, là encore en 2016 dans son guide sur le partage d'information civilo-militaire, co-dirigé par les Américains et ACT, que « *Current military information sharing architectures, copractices and standards are inconsistent with the ability to rapidly establish or join an information sharing environment* »[18].

En résumé, l'approche globale semble éternellement en devenir. Si les imprécations à bâtir une interopérabilité de conception restent de bon aloi, cette approche relève en fait, là encore, d'une interopérabilité de circonstance que la divergence des chemins suivis par les institutions civiles et militaires s'empresse ensuite de déliter.

2. Les grandes initiatives internationales de construction de l'interopérabilité

Il existe de nombreux cénacles de développement de l'interopérabilité au plan international. Ce sont tout d'abord les structures multilatérales : l'OTAN qui reste l'une des deux grandes puissances normatives militaires mondiales avec l'appareil militaire américain *stricto sensu*, ses mécanismes de développement des doctrines, des standards et des SIC, ses cycles NRF, ses centres spécifiques comme le *Joint Air Power Competence Centre* (JAPCC) ; secondairement les structures de l'UE comme le comité Finabel pour les forces terrestres. Se rajoutent les structures multinationales, comme le MDCD (ancien MIC), le *Combined Joint Operations from the Sea Centre of Excellence* (CJOS COE) et le JMTC qui développent également des TTPs, ou encore le corps de réaction rapide européen (CRR-E). Les accords multinationaux plus restreints comme les initiatives trilatérales FR-US-UK dans le domaine naval et aérien, les forces expéditionnaires telles la *Combined Joint Expeditionary Force* (CJEF) ou encore la JEF britannique qui préparent à des intégrations opérationnelles de circonstances, les jumelages d'unités terrestres, les centres et états-majors nationaux certifiés OTAN comme le CRR-FR ou encore le centre de formation à l'appui aérien de Nancy, viennent compléter ces dispositifs.

Il ne s'agit pas dans cette partie de faire la description exhaustive de tous ces éléments, mais d'identifier quelques axes majeurs actuels contribuant à favoriser l'interopérabilité.

2.1. Les avancées de l'OTAN : le Federated Mission Networking

On ne reviendra pas sur le processus de génération des AJP et STANAG sinon pour rappeler qu'il produit de l'interopérabilité « générale » d'ordre culturel et, dans une certaine mesure, normatif opérationnel. En soi, les nombreux engagements tendent à montrer que ces productions sont à elles seules insuffisantes à assurer l'interopérabilité technique et opérationnelle des forces alliées dans la mesure où ces standards peuvent, dans bien des cas, être adaptés par chaque membre ou alors être pris en compte dans des versions différentes. Pleinement consciente de ces limites, l'OTAN s'est engagée depuis 2015 dans le programme du *Federated Mission Networking* (FMN), tirant parti de l'*Afghan Mission Network* réalisé avec succès par l'ISAF et mis en œuvre à partir de 2010. Le FMN recouvre trois volets : une structure de gouvernance et de gestion, un cadre de planification permettant de développer une fédération de réseaux, et les spécifications (architecture, standards) de réseaux proprement dites.

Ces dernières synchronisent de façon extrêmement précise des centaines de standards techniques dans tous les domaines des SIC : STANAG, MIL Standard américains, standards

civils tels ceux du *World Wide Web Consortium* ou encore de l'*International Telecommunications Union*, dans la mesure où les architectes de l'Alliance exploitent autant que faire se peut toutes les normes existantes[19]. La documentation est incrémentalement complétée et corrigée suivant plusieurs développements en spirale, sur une base biannuelle. La spirale 1 concernait les *Core Enterprise Services* principales (systèmes d'exploitation, registres, messagerie, outils collaboratifs, *full motion video*, etc. Voir annexe 1 résumant l'articulation d'un SIC). Avec la troisième, produite en novembre 2018, le FMN couvre également des domaines fonctionnels comme le partage des données et la gestion de la recherche en JISR, la tenue de situation, la *Recognized Air Picture*, le MEDEVAC ou encore certains domaines logistiques. Il développe également la sécurité, un peu négligée jusque-là, avec le *Protected Core Networking*.

Chaque spirale est certifiée tout d'abord par un *Coalition Verification and Validation Environment* (CV2E) combinant de multiples laboratoires – industriels notamment – puis est testée dans les exercices de l'OTAN. L'un de ces exercices majeurs est le *Coalition Warrior Interoperability eXercise* (CWIX), la vaste plate-forme d'expérimentation des SIC. C'est lors de ce dernier exercice, en septembre 2019, que le système d'information des armées (SIA) semble avoir démontré sa compatibilité avec les standards FMN[20]. Enfin, le FMN est appliqué dans les missions opérationnelles. Logiquement, le processus FMN est synchronisé avec celui de la génération de la *NATO Response Force* dont il norme les services C4ISR[21].

Au-delà des réseaux OTAN proprement dits, FMN offre donc la méthode et les spécifications permettant aux pays membres engagés sur un théâtre de développer au plus vite l'interopérabilité de circonstance nécessaire entre leurs réseaux. Le FMN est donc un processus complet, évolutif et qui a vocation à s'étendre à de multiples communautés d'intérêt, notamment au niveau tactique[22], à transiter vers le *cloud computing* (voir ci-dessous) et à développer des standards de cyberdéfense[23]. Il convient de moduler cependant ces conclusions. Si le FMN reste incontestablement une référence, l'interopérabilité visée n'en reste pas moins un objectif élusif dans la mesure où tout dépend des investissements nationaux pour maintenir cette fédération. À bien des égards, le projet FMN ne déroge pas au schéma bien établi depuis deux décennies avec NCW/NNEC : des concepts et architectures initialement poussés par les Américains, que leurs grands alliés européens adaptent et corrigent en fonction de leurs moyens et que les autres alliés adoptent à des degrés divers.

Dans la mesure où les pays membres participent pleinement sous la direction des instances de l'Alliance à ses mécanismes de gouvernance et de management et aux différents groupes de travail, ces développements en spirale représentent un enjeu très important, notamment pour les ensembles de standards poussés par les industriels américains et européens.

2.2. Les initiatives européennes : la coopération structurée permanente

Il ne rentre pas dans l'ambition de cette note de décrire dans le détail la « coopération structurée permanente » (CSP ou PESCO en anglais). Une synthèse de ses programmes est proposée en annexe 2. On se contentera de rappeler que la CSP, permise par les provisions du traité de Lisbonne, a été actée par le Conseil européen en décembre 2017. Cette relance des velléités de développement d'une forme d'Europe de la défense est motivée par le partage d'une série de préoccupations : la résurgence de la menace russe, les inquiétudes quant à la

pérennité des engagements américains et le besoin de « resserrer les rangs » européens après le vote du Brexit. Elle représente un cadre flexible, mais néanmoins contraignant, dans lequel les États membres coopèrent en clusters sur des projets capacitaires, constituant un « microcosme d'intégration différenciée »[24].

Cela précisé, la CSP est surtout indissociable de l'autre grande initiative consistant à créer un Fonds Européen de Défense, dans le cadre du futur budget de l'UE. La commission avait proposé qu'il soit abondé à hauteur de 13 Mds€ sur la période 2021-2027 mais la Finlande, qui préside l'UE, a déjà annoncé la réduction de moitié de ce financement. Beaucoup d'incertitudes subsistent quant aux 7 Mds€ restant auxquels s'opposent plusieurs pays-membres, dans un contexte où la disparition de la contribution britannique se combine bien entendu à la crise[25]. Bon nombre de ces projets n'aboutiront donc pas. L'autre grande faille de la CSP est qu'elle reste principalement une plate-forme de programmes de RDT&E, découplée des éventuels volets d'acquisition nationale des systèmes développés. Elle représente donc un risque pour les industriels. Cependant, même dispersée et, à terme, réduite dans ses réalisations, elle fournira probablement un vecteur de développement capacitaire, un moyen de soutenir les BITD nationales et de partager les coûts de développement de toute une série de systèmes.

Son effet sur l'interopérabilité reste difficile à mesurer à ce stade. La nature des différents clusters laisse penser qu'elle devrait l'améliorer concernant à la fois certaines capacités stratégiques (espace, défense antimissile par exemple), les opérations sur le continent et la dissuasion face au grand Est, notamment en termes de soutien et de protection. En revanche, l'essentiel de nos partenaires dans ces clusters, à l'exception de la Belgique et dans une moindre mesure les Pays-Bas, sont précisément des pays peu enclins à participer aux OPEX impliquant des opérations de combat. En la matière, l'absence du Royaume-Uni et du Danemark (exempté de participation à la politique de défense européenne) se fait cruellement sentir.

2.3. L'approche américaine : le Mission Partner Environment

En 2015, un mémo signé par les 4 principaux « commandants » opérationnels géographiques (AFRICOM, EUCOM, CENTCOM et INDOPACOM) et l'USSOCOM (le « *15 stars memo* ») demande à l'OSD tout le financement et le soutien nécessaires pour créer, enfin, un réseau commun multinational de partage de l'information, ce que ne permettent pas les multiples enclaves CENTRIXS évoquées *supra*. Le *Chief Information Officer* (CIO) du DOD met donc en place le projet de *Mission Partner Environment* (MPE), rebaptisé MPE-*Information Sharing* (MPE-IS). Deux configurations doivent coexister : d'une part, le *MPE Enduring*, permanent, de niveau stratégique, pour les travaux de planification et autres efforts de partage de l'information asynchrone, intégré avec le *Joint Information Environment* américain ; d'autre part, le *MPE Episodic*, pour une mission donnée, dans lequel les partenaires de coalition sont élevés au niveau de « *peer* » et doivent pouvoir opérer avec leurs propres systèmes. Concrètement, le MPE uniformise et met à disposition des partenaires toute une série de CES et met en place un *Virtual Data Center* par COCOM permettant de gérer de multiples enclaves CENTRIXS avec des passerelles multiniveaux. Le projet s'étale de 2017 à 2024. Début 2019, le CIO a désigné l'Air Force comme agent d'exécution du développement de ce MPE.

EUCOM a été le premier commandement à déployer le MPE que le vaste exercice *Joint Warfighting Assessment* (JWA) 18 de l'Army a permis de tester, avec succès selon les Américains[26]. L'interopérabilité aurait été bien réalisée avec les PC britannique, canadien et français (7ème brigade). Sur cette base, JWA a permis également de valider un autre système, le « *Common Operational Picture Shop* » permettant de partager les données de situation entre les systèmes C2 des nations participantes. Ce système utilise tout particulièrement le protocole *NATO friendly force information* (NFFI) employé par le FMN ce qui permet de penser que l'interopérabilité concernant le suivi des unités alliées est bien assurée.

2.4. L'Initiative Européenne d'Intervention (IEI)

L'IEI, lancée par le président de la République en septembre 2017, rassemble neuf partenaires : Danemark, Estonie, Espagne, Belgique, Finlande, Pays-Bas, Portugal, Royaume-Uni et plus récemment, Allemagne. Visant à faciliter l'interopérabilité de circonstance, elle s'inscrit avant tout dans le champ culturel puisqu'elle vise à créer une « culture stratégique commune » via des travaux communs de prospective, de planification, de doctrine et de RETEX. En l'état, l'IEI se traduit avant tout par des échanges aux niveaux ministériel et état-major, via *les Military European Strategic Talks* (MEST) lancés en 2018, dans le cadre desquels les partenaires partagent des analyses régionales ou thématiques et du RETEX. L'IEI interroge cependant quant à son ambition : une convergence de « cultures stratégiques » – résultats de la géographie, de l'Histoire et de la culture politique de chaque pays – ne se décrète ni ne se réalise par des échanges d'information et des travaux d'état-major même si ces derniers peuvent s'avérer fort utiles, justement pour affiner et gérer ces différences de cultures.

2.5. La tendance aux intégrations pérennes ciblées

Compte tenu des difficultés à réaliser des interopérabilités de conception avec un grand nombre de partenaires, la période est au renforcement des projets ciblés, très stratégiques, d'interopérabilité par l'intégration opérationnelle « *by design* » qu'il convient de différencier des intégrations de circonstance auxquelles préparent les multiples forces multinationales (CJEF, JEF UK, etc.). Elle est jusque-là limitée à quelques *battlegroups* de l'UE, et à la communité des systèmes. En témoigne bien entendu le programme CAMO par lequel l'armée de Terre belge va pleinement adopter la doctrine et les équipements Scorpion.

L'Allemagne fournit clairement l'archétype de ce modèle, au moins dans le domaine terrestre[27]. Berlin manifeste ainsi la volonté depuis 2014 de constituer une « armée d'ancrage » pour les autres petites puissances militaires européennes en s'appropriant le *Framework Nation Concept* (FNC) otanien, dans le cadre des mécanismes de planification capacitaire de l'Alliance. L'intégration la plus achevée est en cours de réalisation avec les Pays-Bas. Citons notamment celle de la brigade d'assaut aéromobile néerlandaise dans la division des forces de réaction rapides allemandes, celle des unités de chars, la compatibilité ou l'interchangeabilité de nombreux éléments de maintenance et même l'intégration système avec le *Tactical Edge Networking* (TEN). Signé en juin 2019, TEN vise à l'intégration (doctrines, TTPs, équipements communs, etc.) des SIC terrestres du *Digitilisation of Land Based Operations* (D-LBO) allemand et FOXTROT néerlandais jusqu'au niveau plate-forme, y com-

pris en ce qui concerne la sécurité et le cyber. La première unité équipée est planifiée pour 2024[28]. Les deux partenaires prévoient d'y consacrer 12 Mds€ entre 2019 et 2030. Des initiatives d'intégration ont aussi été lancées avec la Roumanie, la République tchèque et la Lituanie. La Belgique a exprimé le souhait de rester interopérable avec ce TEN puisque son objectif est de bâtir « *un pont solide entre ce partenariat franco-belge et le duo germano-hollandais* »[29]. Dans ce contexte, l'US Army et la Bundeswehr ont signé une déclaration de vision stratégique en octobre 2019 visant à pouvoir pleinement intégrer des brigades et divisions allemandes respectivement dans des divisions et corps américains et vice versa. Le texte prévoit notamment la « coordination » des SIC et des procédures de recherche et de partage du renseignement, la « compatibilité » des fonctions de surveillance et de reconnaissance, l'interchangeabilité des munitions et le développement de chaînes feux en réseau[30].

Les intégrations ciblées s'articulent aussi autour des vastes programmes dans le domaine aérien dans la mesure où les systèmes actuels comme le F-35 et plus encore les programmes SCAF ou Tempest constituent de véritables « systèmes de systèmes » : leur adoption n'a plus rien à voir avec l'acquisition d'une unique plate-forme de la génération précédente, qu'une armée de l'air pouvait incorporer selon ses normes, mais engerbe dorénavant aussi les munitions, le soutien, les politiques de gestion des données, etc. On s'achemine ainsi vers des « bulles » F-35, SCAF ou Tempest qui constitueront l'essentiel des capacités engagement / combat et un élément C2ISR majeur de chaque force aérienne impliquée.

Plusieurs autres initiatives sont en cours comme celles du *Maritime Theatre Missile Defence Forum*, mis sur pied en 2004 et rassemblant les 11 nations européennes et américaines disposant de capacités antimissiles navales. Le projet *Framework Architecture 2030+* vise ainsi à développer les processus, modèles de données, standards d'interface (etc.) communs pour permettre l'engagement multiplateforme entre les navires des nations participantes, à l'image de ce que seuls les bâtiments Aegis de l'US Navy parviennent à réaliser avec l'architecture *Naval Integrated Fire Control – Counter-Air* (NIFC-CA).

3. Les facteurs conditionnant le futur de l'interopérabilité

3.1. Les facteurs stratégiques : nos partenaires à l'heure de la grande crise

Ces facteurs stratégiques sont évidemment à considérer à l'aune de la crise majeure liée à la pandémie COVID-19. Cette crise étant loin de son aboutissement, il est encore bien trop tôt pour en tirer des conclusions claires. On peut cependant se risquer à en esquisser quelques contours. Le principal est qu'elle ne semble pas, en l'état de son déroulement, présenter de ruptures encore clairement identifiables dans le champ stratégique mais elle semble en marche pour en accentuer les lignes de fractures.

3.1.1. Des menaces et risques toujours aussi vifs

Une telle crise du système international n'affaiblit en rien les menaces, bien au contraire. Elle exacerbe les tensions entre les superpuissances américaine et chinoise. La crise écono-

mique que traversent à des degrés divers toutes les puissances, est certes susceptible de réduire leurs moyens mais elle peut tout autant pousser aux aventures sur fond de galvanisation des nationalismes, surtout si les capacités dissuasives occidentales étaient réduites. La crise ne semble pas non plus, en l'état, compromettre les capacités des djihadistes au Sahel ou au Levant. Elle sera en revanche de nature à affaiblir plus encore les puissances locales en première ligne de leur endiguement. En effet, même si l'Afrique semble relativement épargnée par la pandémie, les effets de cette dernière sur le commerce international, notamment sur le coût des denrées alimentaires, risquent d'être redoutables. Elle ne remet pas en cause les risques majeurs, environnementaux notamment. Ceux liés au réchauffement climatique, par exemple en matière d'incendies d'ampleur catastrophique comme les ont connus l'Australie et la Californie, justifiant un regain d'intérêt pour les engagements de secours d'urgence, restent bien présents.

Pour faire face à ces menaces et risques, le panorama des partenariats opérationnels n'est en rien amélioré par la crise.

3.1.2. L'indispensable partenariat avec les États-Unis : une inquiétante variable

En théorie, le contexte stratégique devrait plaider pour un renforcement de l'interopérabilité avec les États-Unis. C'est en tout cas la position de l'*establishment* militaire américain. En témoignent par exemple, les accords trilatéraux US-UK-FRA ou encore les efforts relatifs au MPE déjà évoqués. L'un des éléments clés de la doctrine des opérations multidomaines réside précisément dans le soutien que les alliés pourront fournir aux déploiements rapides des forces américaines en cas de crise. Plus stratégiquement, l'attachement des alliés représente en réalité un enjeu permanent de la guerre d'influence mondiale que se livrent les États-Unis d'une part, la Russie et la Chine d'autre part[31].

Pour autant, des tendances à la divergence avec les Américains se font jour depuis une décennie. Depuis la Libye en 2011, l'engagement américain est passé du statut de confortable postulat à celui d'inquiétante variable. En rupture avec ses prédécesseurs, le Président Trump ne manifeste qu'un intérêt limité pour les équilibres stratégiques, entretient une vision purement transactionnelle de ses relations avec ses partenaires et se focalise entièrement sur la compétition économique, replaçant les alliés au même niveau que les opposants. Or, le locataire à la Maison-Blanche semble être le reflet d'une évolution structurelle interne en faveur d'un relatif désengagement des États-Unis des responsabilités mondiales qu'ils entendaient assumer jusqu'à récemment.

L'impact de la crise en cours reste encore incertain. Les niveaux records de l'endettement fédéral générés par le soutien budgétaire à la remise à flot de l'économie américaine pourraient entraîner un resserrement important des crédits de défense, au moins à partir de 2022[32]. À partir de là, toutes les options semblent ouvertes, d'un élagage des engagements non prioritaires avec focalisation sur la dissuasion de la Chine et de la Russie à un mouvement de retrait stratégique nettement plus marqué[33]. Il est d'ores et déjà possible d'envisager à la fois une réduction de l'interventionnisme militaire et une sollicitation accrue des alliés, dont bien entendu la France. Le maintien de la participation américaine aux opérations en BSS, pour l'instant confirmé, apparaît donc d'autant plus incertain qu'il était déjà remis en cause par le secrétaire à la Défense Mark Esper en février 2020[34]. Un scénario plus grave de rupture profonde doit également être envisagé. Tous les observateurs s'accordent

en effet sur la profondeur inédite des lignes de fracture parcourant la population américaine et que la présidence Trump a largement contribué à creuser. Le jeu institutionnel, polarisé comme jamais, en est déjà gravement affecté. On ne peut dès lors exclure, par exemple à l'occasion de la prochaine élection présidentielle, tout particulièrement si ses résultats sont peu tranchés, une crise politique et sociale majeure. Un tel scénario pourrait avoir pour effet, sur le plan stratégique, de paralyser entièrement l'appareil décisionnel américain. Il pourrait alors ouvrir la perspective à d'autres scénarios, incluant des « prises de risques » accrues de la part d'autres puissances si les garanties de sécurité et l'aptitude dissuasive américaines étaient durablement affectées.

3.1.3. L'incertitude des partenariats européens

La crise devrait aussi selon toute logique affecter les positions et capacités des grands partenaires européens. La situation actuelle reste marquée par de multiples lignes de faille aux effets contradictoires : le resserrement des Européens compte tenu des incertitudes stratégiques quant aux engagements de Washington mais aussi de la compétition industrielle accrue avec la BITD américaine tendrait à consolider les efforts communs de stratégie capacitaire, au travers de l'OTAN comme de la CSP.

Dans ce contexte, les nuages s'accumulent sur la position du Royaume-Uni qui reste notre plus proche allié en matière de capacités, d'intérêts stratégiques dans une moindre mesure, et en tout cas de culture stratégique. Le budget de la défense s'inscrit actuellement dans une forte hausse devant le ramener proche des 2% du PIB. Si les Britanniques peuvent apparaître sensiblement marginalisés au sein de l'OTAN compte tenu du Brexit, l'investissement dans le F-35 ou dans la recréation de leur aéronavale leur garantit une place de choix dans les coalitions au côté des Américains. Ils disposent aussi d'une capacité de *Framework Nation* avec la *Joint Expeditionary Force* à laquelle les 8 pays d'Europe du Nord peuvent contribuer. Cependant, le *National Audit Office* vient d'estimer que le plan d'équipement 2019 à 10 ans ne prend pas en compte le risque de sous-financement estimé dans une fourchette de 2 à 7%. La crise vient achever de rebattre les cartes. La nouvelle revue de défense, dont les conclusions sont repoussées en 2021, pourrait ainsi aboutir à un plafonnement voire une baisse des crédits. Or, compte tenu des vastes chantiers aux dépenses peu compressibles (comme le SNLE *Dreadnought*), il n'est pas évident que les Britanniques puissent maintenir à terme le niveau de cohérence interarmées de leur force.

Le poids de l'Allemagne s'en trouve donc renforcé, du moins en théorie. Elle devient le partenaire privilégié de bon nombre de pays d'Europe centrale et de l'est, hormis la Pologne qui privilégie son partenariat avec les États-Unis. Le concept de « nation-cadre » et les initiatives d'intégration déjà évoquées de même que les efforts de remontée en puissance capacitaire que sanctionne une nouvelle hausse significative du budget de la défense, vont clairement dans ce sens. Les observateurs doutent cependant fortement que l'évolution du paysage politique, avec une nouvelle Coalition en 2018 remettant en cause les efforts faits sur la défense, de même que la profondeur des défis capacitaires à relever par ses forces (recrutement, disponibilité), permette à l'Allemagne de réaliser les priorités affichées[35]. Ce qui rend la coopération avec la France, qui cumule les premières forces opérationnelles et BITD du continent, tout autant nécessaire qu'elle est difficilement gérable compte tenu de nos divergences géostratégiques et de nos domaines de compétition. L'une de ces divergences réside

dans la primauté accordée par l'Allemagne, dans ses initiatives de coopération, aux intérêts de sa BITD par rapport aux objectifs stratégiques et capacitaires militaires.

Les effets de la crise sur ces partenariats sont encore incertains. Sur le plan stratégique, elle ne devrait en outre selon toute vraisemblance pas remettre en cause la ligne de fracture entre puissances interventionnistes, au premier rang desquelles restent la France et le Royaume-Uni, et les puissances ne préparant leurs moyens que pour la défense de leurs intérêts vitaux et rétives à tout recours à la force, au premier rang desquelles se renforce l'Allemagne.

3.2. Les ruptures technologiques dans le domaine des SIC

Les avancées technologiques que connaissent les systèmes d'information et de communication sont susceptibles de changer fondamentalement l'interopérabilité technique. Les capacités qu'ils autorisent devraient par ailleurs avoir un impact important sur l'interopérabilité normative opérationnelle.

Cette section distingue ces éléments en abordant tout d'abord la question spécifique de la première couche d'un SIC, les communications, puis en développant l'évolution vers le « *cloud* » qui affecte toutes les autres couches.

3.2.1. L'interopérabilité des communications

A. L'ère de la radio logicielle

Les moyens de transmission évoluent vers une flexibilité accrue dans l'utilisation du spectre électromagnétique. Cette flexibilité permet d'optimiser les communications dans un spectre toujours plus congestionné par le nombre d'émissions, de contourner les menaces de guerre électronique et, précisément, d'améliorer l'interopérabilité.

Cette évolution découle de la numérisation lancée dans les années 1990. Pour mémoire, jusque-là, les matériels analogiques étaient conçus pour utiliser une unique forme d'onde[36]. Les systèmes numérisés gèrent une large part de cette forme d'onde par un processeur programmable et un logiciel. Ces radios logicielles (ou « *Software-Defined Radio* » – SDR) peuvent ainsi communiquer sur plusieurs formes d'onde, utilisées en fonction des correspondants. Certes, cette radio logicielle n'est plus à proprement parler une innovation. Le premier programme à en exploiter la technologie a été le *Joint Tactical Radio System* (JTRS) américain à la fin des années 1990. Une architecture de communication logicielle, le *Software Communications Architecture* (SCA), a été développée et continue d'être mise à jour précisément pour offrir un cadre commun de développement de la partie logiciel de ces radios. Après 20 ans de vicissitudes et de déceptions, cette technologie semble sortie de l'ornière[37]. Le PR4G de Thalès est lui aussi une SDR. Les partenaires européens (France, Italie, Espagne, Finlande, Allemagne dernièrement) se sont dotés de leur propre programme, *European Secure Software Defined Radio* (ESSOR) géré par l'OCCAR, pris en compte par la CSP. ESSOR consiste à développer une architecture ainsi qu'une forme d'onde haut débit. Son architecture est basée sur la SCA américaine[38]. Elle est mise en œuvre par le programme COmmunications Numériques TACtiques et de Théâtre (CONTACT) de Thalès qui doit incré-

mentalement remplacer les postes PR4G et autres postes de transmission UHF des armées. SDR oblige, les postes CONTACT continueront de prendre en compte aussi la forme d'onde PR4G. Les technologies continuent d'évoluer, la logique « *software-defined* » a été étendue à la gestion du réseau, plus uniquement aux transmissions d'un équipement, ouvrant l'ère du « *Software-Defined Networking* » (SDN).

Cette interopérabilité des transmissions tactiques devrait donc s'en trouver grandement facilitée. Elle n'est pas pour autant garantie et pourrait rester un défi. Celui-ci réside dans l'harmonisation des multiples versions de ces architectures logicielles dans un système où la complexité des technologies réduit l'aptitude des opérateurs (mais ne l'annule pas, voir ci-dessous) à compenser eux-mêmes ces défaillances d'interopérabilité, les plaçant en consommateurs d'un service.

Lors d'une expérimentation *Bold Quest* (expérimentation menée à White Sands impliquant des nouvelles technologies utilisées entre autres pour les feux et le CAS), en 2014, l'interopérabilité entre JTAC et aéronefs s'était avérée impossible précisément en raison d'une incompatibilité des versions logicielles. Seuls deux sous-officiers français, déployés au titre de leur (unique) expertise des réseaux DACAS dans l'hexagone, sont parvenus à obtenir la liaison avec les Harrier des *Marines*, en paramétrant eux-mêmes les postes radio, au grand étonnement de leurs homologues américains et de l'aréopage des représentants de Harris et d'autres industriels présents[39].

B. Les nouvelles architectures spatiales

Autre élément d'importance, l'interconnexion croissante permet également le développement d'architectures aérospatiales intégrant les communications par relais aéroportés au-delà de la ligne de vue et celles fournies par les communications par satellite. Ces dernières gagnent non seulement en efficacité mais aussi en résilience avec l'investissement des orbites basses et médianes par des constellations de minisatellites qui offrent un débit et un temps de latence nettement améliorés par rapport aux constellations classiques en orbite géostationnaire.

C. Le développement des réseaux 5G

En matière de communications cellulaires, la mise en œuvre de la 5G promet une rupture encore plus importante que celle apportée par la 4G. Elle offrira un débit de 10 à 20 fois plus important que cette dernière pour un temps de latence réduit dans le même ordre de grandeur, offrant le substrat à l'Internet des objets (IoT), car elle sera en mesure d'interconnecter des milliers de fois plus d'éléments que la 4G. Ses applications militaires sont encore en cours d'exploration, mais il est logique que la technologie soit largement employée. Elle fait désormais partie des 10 technologies majeures du chef de la R&D du Pentagone. Dans la mesure où la 5G monte en fréquence (elle utilisera soit des bandes de 1 à 6 GHz, soit des bandes millimétriques entre 24 et 100 GHz, contre 2,6 GHz au maximum pour la 4G), sa portée est plus courte, à puissance équivalente, que les systèmes mobiles précédents mais, outre les performances de *networking* attendues, le caractère directionnel des émissions les rend peu vulnérables à l'interception et au brouillage (elles sont en revanche plus sujettes aux perturbations atmosphériques). Parmi les utilisations d'ores et déjà évoquées figurent les réseaux « locaux » : « smart bases », réseaux tactiques courte portée de capteurs, de drones et de robots, par exemple au sein de *clouds* tactiques. La logistique ou encore l'entraînement font aussi parties des domaines devant largement bénéficier de la 5G

et de l'IoT qu'elle permet[40]. Son emploi ne s'arrête pas là. Indissociable des technologies de SDN évoquées ci-dessus et de l'intelligence artificielle, la 5G permettra de « virtualiser » plusieurs réseaux de nature et de fonctions différentes. Un réseau 5G sera aussi, entre autres choses, beaucoup plus ouvert que les précédents. Un cœur de réseau 5G pourra ainsi représenter le réseau de contrôle d'autres systèmes de transmission de plus bas débit[41]. La problématique de l'interopérabilité reste encore à étudier mais on peut donc avancer que, théoriquement, la technologie 5G est un remarquable vecteur pour l'améliorer. Elle dépendra cependant bien sur des standards retenus par les différents pays, d'où l'enjeu que constituent les efforts de la Chine (Huawei et consorts) pour exporter sa technologie, la plus mature, et ceux des Américains pour les entraver. Elle dépendra également des bandes de fréquences utilisées. Par exemple, alors que les États-Unis misent sur les ondes millimétriques (en raison de la faible disponibilité commerciale des fréquences plus basses, déjà utilisées par les systèmes EHF gouvernementaux), le reste du monde se concentre sur les bandes de moins de 6 GHz[42].

3.2.2. La nouvelle ère de l'info-valorisation : Cloud et approche data-centric

L'avenir des SIC est, comme dans les secteurs civils, au *« cloud computing »* qui consiste *stricto sensu* à partager, mutualiser les ressources informatiques[43]. Cette transition vers le *cloud* est déjà une réalité pour les SIC stratégiques, en particulier chez les Américains depuis 10 ans où le nombre de *clouds* a explosé. Le programme JEDI vise ainsi à mettre de l'ordre dans ce foisonnement en créant un *cloud* général unique, que viendront compléter des *clouds* spécifiques[44]. Le FMN de l'OTAN fait également appel à ces technologies. Celles-ci vont s'étendre aux ramifications tactiques, sur les plates-formes voire leurs munitions, se déclinant ainsi en « *combat clouds* » ou « *tactical clouds* ». L'Air Combat Command américain le définit comme « *un réseau maillé global pour la distribution des données et le partage de l'information dans un espace de combat, où chaque utilisateur, plate-forme ou nœud autorisé contribue et reçoit en toute transparence l'information essentielle et est en mesure de l'utiliser dans toute la gamme des opérations militaires* »[45].

En fait, le *cloud* renouvelle la problématique du *Network Centric Warfare* à l'ère du « big data », caractérisé par ses 5V : volume, « vélocité » (leur écoulement en flux continu), variété (dans leur formatage), véracité et valeur. Cette transformation est envisageable du fait des capacités grandissantes des capteurs et de stockage des données sur les plates-formes et des futurs outils embarqués d'extraction, de traitement semi-automatisé, de « fusion » de données hétérogènes et d'analyse reposant sur les solutions d'intelligence artificielle. Le *cloud* tactique doit ainsi permettre aux plates-formes et unités d'accéder à un outil autrefois uniquement disponible aux opérateurs de niveau stratégique[46]. Les Américains sont évidemment en pointe dans le développement incrémental de ces technologies : *Fusion Warfare* déjà présente sur le F-35, CloudONE de l'*Airborne Battle Management System* (ABMS), le système C2 tactique futur de l'Air Force, désigné comme pilote de l'intégration des SIC tactiques des forces américaines, développements équivalents au sein de la Navy et de l'Army. Les armées françaises ne sont pas en reste. Dans son *Ambition numérique*, 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 cœur du futur combat en Cloud »*[47]. Le SCAF sera ainsi un *« système de systèmes intégrant, au sein d'un véritable Cloud, des senseurs et des effecteurs de différentes natures et de différentes générations »*[48].

La question qui se pose alors est l'interopérabilité de ces multiples *clouds* émergents. Sur le plan technique, le défi apparaît moindre que sur la précédente génération de SIC, puisque bon nombre de technologies utilisées sont principalement civiles. Or, le monde commercial est caractérisé par une grande convergence de normes et de protocoles entre les acteurs du secteur : Amazon, Microsoft, Google et même leurs homologues chinois. Le niveau d'interopérabilité est tel que pour une entreprise, la bascule d'une solution à l'autre (par exemple, Microsoft vers Alibaba) ne nécessite que quelques jours de travail[49]. Cela étant, ces technologies commerciales sont surtout transposables pour les *Core Enterprise Services* (CES) et des applications fonctionnelles basiques. Bon nombre de communautés opérationnelles requièrent toujours des applications militaires dédiées en mesure de prendre en compte la complexité (donc l'imprévisibilité) et la fluidité d'un environnement opérationnel, bien plus contraignantes que celles d'un environnement commercial aux facteurs bien cernés. C'est en particulier le cas des techniques d'intelligence artificielle qui doivent aider à la prise de décision et/ou fournir le cerveau des futurs systèmes autonomes. Les technologies commerciales, qu'il s'agisse de systèmes *rules-based* ou d'apprentissage machine, ne sont pas adaptées à ces environnements opérationnels complexes[50].

La capacité d'un *cloud* à exploiter le *big data* repose en outre sur une stratégie de gestion des données opérationnelles. Les Américains mettent ainsi en exergue la transition vers un environnement *Data-Centric*[51]. Ces *Data strategies* consistent à enregistrer les sources de données, à précisément cataloguer les données et à les décrire avec des métadonnées et des informations de contexte, fondées sur un glossaire commun, enfin à assurer les mesures de protection de ces données et la gestion des accès[52]. Le développement de ces stratégies s'effectue le plus souvent, chez les Américains au moins, par armée, en même temps que le volet technique du *cloud*. Il y a donc tout lieu de penser que la mise en œuvre de ces stratégies constituera un défi de plus pour l'interopérabilité, tant multinationale qu'interarmées.

Enfin, les évolutions technologiques caractérisant ces SIC, tout comme les procédés d'attaque ou de défense électronique qui les affectent ou les protègent, impliquent également une intégration croissante du domaine cyber au niveau tactique. De plus, parmi les données des capteurs, le ROEM et la surveillance électronique vont occuper une place de plus en plus critique. Or, ce sont précisément des données dont le partage multinational est des plus restreint.

Au final, si les CES des SIC, fondés sur les technologies commerciales, laissent augurer une facilitation de l'interopérabilité, au moins pour la coordination, par exemple en planification, il est probable que les exigences associées aux données et applications opérationnelles les plus pointues, notamment nécessaires pour la symbiose tactique, représentent un obstacle majeur pour le développement de l'interopérabilité future.

3.3. Les facteurs opérationnels

3.3.1. Les formes symbiotiques du combat comme résultantes de ces évolutions technologiques

Ces avancées de la mise en réseau et de l'infovalorisation impriment des changements opérationnels significatifs qui représentent un facteur cardinal pour l'interopérabilité. Elles per-

mettent en effet de passer à l'intégration opérationnelle au plus bas niveau tactique voire au fonctionnement intégré des systèmes d'armes et d'information, qualifié dans cette étude de « symbiose ». Il s'agit bien là d'une évolution générique postulée par la théorie de la NCW et pas uniquement d'un concept américain.

Dans le domaine des opérations terrestres, cette évolution mène à abaisser délibérément les échelons où se pratique l'interopérabilité multinationale dans les doctrines, qui continuent de les fixer au niveau de la brigade voire du GTIA – alors même que le volume des déploiements en OPEX amène d'ores et déjà la pratique des intégrations opérationnelles de niveau sous-GTIA[53].

Cette évolution va permettre très probablement une distribution de la fonction C2 au niveau tactique. C'est tout particulièrement le cas des opérations aériennes : elles sont actuellement conduites selon le principe du contrôle centralisé des opérations (au niveau des structures de conduite du JFACC, ce que l'on appelait auparavant le CAOC) et de l'exécution décentralisée au niveau des AWACS et équivalent, des centres terrestres de détection et de contrôle, etc. Or, dans les cas où de multiples opérations tactiques doivent être gérées simultanément, cette organisation apparaît trop centralisée pour réagir de façon adéquate et saisir les opportunités. Elle ne permet pas d'exploiter au mieux la perception des opérateurs tactiques, souvent supérieure à celle du JFACC. Elle rend de plus le C2 vulnérable aux effets de décapitation (isolement du JFACC de ses nœuds tactiques par la guerre cyber-électronique par exemple). Les nouvelles technologies offriront donc la possibilité de décentraliser ce contrôle au niveau des plates-formes devenant des nœuds C2ISR, y compris les futurs appareils de combat, en fonction des circonstances et des missions (notamment pour le CAS ou certaines missions d'interdiction comme le ciblage d'opportunité et le *Strike Coordination and Reconnaissance*). L'ABMS de l'Air Force va clairement dans ce sens. Le programme d'*Alliance Future Surveillance and Control* (AFSC) de l'OTAN qui doit combiner 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[54], pourrait suivre le même chemin, bien que cela reste à confirmer. Cette évolution constituera très certainement un défi pour maintenir l'interopérabilité avec les autres composantes.

Avec la fusion des données des capteurs, elle se traduira également par le développement des formes de combat collaboratif entre les différentes plates-formes effecteur/ISR mais aussi entre ces plates-formes et leurs munitions, incluant des missiles maraudeurs remplissant certaines fonctions identiques à celles des drones. Dans le domaine aérien, le F-35 représente une première étape de cette capacité de *fusion warfare* et préfigure l'évolution vers la capacité – on n'ose plus dire appareil – *Next Generation Air Dominance* dans le cadre de l'ABMS. L'armée de l'Air inscrit le combat collaboratif connecté au cœur de la modernisation de ses capacités actuelles devant constituer à moyen terme un Système Global de Combat Aérien (SGCA), dont le programme Connect@aéro doit assurer les interconnexions, et bien entendu à terme au cœur du SCAF.

3.3.2. Le « multidomaine », au croisement de la symbiose tactique et du durcissement des postures, un paradigme problématique

Le développement des opérations « multidomaines » ou « interdomaines » est consubstantiel de ce niveau supérieur d'interopérabilité. Le sujet ayant déjà été traité dans le cadre de

cet observatoire, cette note ne reviendra pas sur les fondamentaux de ce concept[55]. L'évolution vers le multidomaine est aussi à considérer à l'aune de l'évolution des menaces, du « durcissement des postures » et des besoins doctrinaux en découlant. Ainsi, le besoin d'une capacité à « manœuvrer » dans les différents domaines, à créer et exploiter des fenêtres de supériorité dans le dispositif adverse, qu'autorise la synergie multidomaine, est dicté par le renforcement des capacités d'interdiction adverses dans chacun de ces domaines.

Il peut cependant exister une importante contradiction entre la logique très inclusive du multidomaine et les développements pratiques de l'interopérabilité multinationale. En effet, le multidomaine peut être considéré d'une façon étroite comme pluriel, chaque composante de milieu (terre, air, mer) développant ses propres bulles multidomaines en intégrant l'appui spatial et les opérations cyber. Dans ce cas, l'interopérabilité multinationale est facilitée. En revanche, si l'on considère le multidomaine comme un cadre unique, d'une façon plus exhaustive, il s'inscrit dans la même logique que l'intégration opérationnelle interarmées. Transposé au plan multinational, il exigerait alors d'intégrer des dispositifs déjà interarmées. Or, comme nous l'avons vu, les initiatives d'intégration s'effectuent avant tout par composantes de milieu. On peine à imaginer, par exemple, les forces belges, écartelées entre des intégrations américaines et françaises, en mesure de réaliser aisément des opérations multidomaines avec chacun de ses grands partenaires. C'est d'ailleurs l'un des principaux défis identifiés par le général Pierre Gérard, le CEMAT belge[56].

Autrement dit, le multidomaine dans la plénitude de son acception reste avant tout une problématique d'interopérabilité au sein de la matrice d'intégration interarmées que constituent les quelques grandes puissances militaires.

3.3.3. D'autres changements impulsés par le durcissement des postures

D'autres évolutions capacitaires et opérationnelles vont aussi façonner les besoins d'interopérabilité. L'une des plus importantes réside dans l'allongement considérable des portées des systèmes de feux terrestres dans la profondeur (voir la note 12). À titre d'exemple, la *Field Artillery* américaine va connaître dans la prochaine décennie un doublement de portée de ses canons, roquettes guidées et missiles tactiques. Cette évolution change considérablement les modalités de l'interopérabilité avec les opérations aériennes d'interdiction dans la mesure où les zones de profondeur opérationnelle tendent à converger.

Un autre facteur est le recours croissant à la guerre électronique et, dans le futur, aux opérations cyber tactiques. En témoignent les nouvelles capacités offertes par un appareil comme le F-35. Or, ces domaines sont parmi les plus sensibles en matière de partage de l'information. Cette évolution devrait logiquement accroître les contraintes d'ordre stratégique sur l'interopérabilité.

3.4. L'accélération et la flexibilisation du développement capacitaire américain

Pour améliorer l'efficience de la modernisation de leurs forces, accélérer cette dernière face à la Chine et à la Russie et remédier aux manques récurrents d'interopérabilité de leurs forces, les Américains renforcent considérablement le recours aux architectures modulaires et aux méthodes du *small business* les plus flexibles.

3.4.1. Les architectures ouvertes modulaires

Les « architectures ouvertes modulaires » combinent deux aspects : d'une part, la modularité d'un système, qui permet d'adapter certaines de ses composantes en fonction du besoin sans changer l'ensemble du système, la gestion des charges utiles et celle de la plate-forme devenant distinctes ; d'autre part, des standards « ouverts », par opposition aux standards « propriétaires » dont une entreprise conserve toute la propriété intellectuelle. Bon nombre de systèmes obéissent déjà à cette logique. Pour autant, si chaque industriel adopte sa propre architecture « ouverte », on recrée *de facto* un problème d'interopérabilité important. L'exemple des navires de lutte antiaérienne et antimissile est parlant. Comme le déplore un planificateur de la Marine allemande : « *36 navires non américains à capacité de défense aérienne [...] utilisent sept systèmes de gestion de combat entièrement différents, quatre familles de radars différentes et deux familles de missiles différentes. Bien qu'ils soient tous conçus comme une technologie à architecture ouverte, l'interopérabilité de leur système est nulle, sauf par liaison de données tactiques* »[57].

Tout tient donc dans la portée de ces architectures. Or, les Américains basculent massivement sur ce modèle. La Navy a été la première à le mettre en œuvre pour les systèmes de détection et de combat de ses quatre classes de sous-marins. L'OSD en préconise la mise en œuvre depuis plusieurs années dans le cadre des mesures du *Better Buying Power* déployées par Ashton Carter au début de la décennie 2010. Le recours à ces architectures, sauf exception, est devenu une obligation légale pour tous les programmes d'armements majeurs avec la NDAA 2017 (Section 805). Généralement lancés et sponsorisés par les armées, une quinzaine de standards matériels et/ou logiciels pour systèmes terrestres et aériens, principalement l'avionique et la vétronique, ont été produits ou sont en train d'être produits par les industriels américains, réunis en de vastes consortiums (voir annexe). De natures, portées et cheminements variés, ces architectures fournissent surtout des standards d'interface entre les composantes et les plates-formes, et l'approche pour réaliser et valider les éléments correspondant. Elles exploitent des *Government Reference Architectures* (GRA) permettant un point de référence pour une fonction donnée (par exemple, communications, radars, drones, guerre électronique, systèmes PNT). Ensuite, il existe un effort de convergence de ces standards, géré par le *Defense Standardization Program Office* (DSPO), sanctionné par un mémorandum tri-*services* signés par les chefs d'état-major en janvier 2019, pour les incorporer dans les processus d'acquisition[58].

3.4.2. L'accélération de l'innovation par les « méthodes agiles »

Les Américains sollicitent de façon croissante les entreprises très innovantes de la *high-tech* pour le développement de leurs systèmes d'information, particulièrement par l'entremise de

la *Defense Innovation Unit*. Ces entreprises utilisent les méthodes de « développement agile » et « DevOps » qui intègrent de façon itérative le développement et le test opérationnel des outils. Elles reposent sur une relation étroite entre développeurs et opérationnels, et une forte délégation d'autorité par la hiérarchie. Le *Service* qui recourt le plus massivement à cette approche est l'USAF. La fameuse opération « Kessel Run » a par exemple permis en quelques mois de moderniser ou de sortir de l'ornière toute une série d'applications de planification et de conduite du CAOC d'Al Udeid et se poursuit en tâche d'huile[59]. Si les résultats sont peut-être plus mitigés que certains observateurs le pensaient[60], ils n'en restent pas moins réels et entraînent une évolution des pratiques sur une échelle de plus en plus grande.

3.4.3. Impact de ces développements sur l'interopérabilité

Il est encore trop tôt pour mesurer précisément la portée de cette évolution sur l'interopérabilité des forces américaines. Elle est cependant porteuse de deux impacts clés pour notre interopérabilité.

Tant l'agilité des mécanismes d'innovation, qui procède d'une approche pragmatique *« bottom-up »*, que le recours aux architectures ouvertes modulaires devraient tout d'abord **accélérer le rythme de modernisation** des systèmes d'armes et d'information ce qui mécaniquement pourrait **rendre plus complexe le maintien de l'interopérabilité avec les SIC des partenaires aux évolutions plus lentes**. L'un des inconvénients de l'approche, régulièrement souligné par les rapports du DOT&E concernant les systèmes de la Navy, est que le rythme de modernisation peut être parfois trop rapide pour correctement évaluer les performances de ces systèmes, ce qui peut inclure la certification de leur interopérabilité.

En lien avec le point précédent, ces architectures sont **réservées aux industriels américains et aux filiales américaines des industriels étrangers**. Cela pose forcément beaucoup de problèmes pour les perspectives déjà réduites d'exportation de nos industriels sur les marchés américains. En revanche, il convient de rappeler que les industriels américains, à l'occasion des réductions budgétaires du début de la décennie, se sont résolument tournés vers les marchés export et que le pli a été gardé, même avec l'embellie budgétaire de 2015 à 2020. Ces MOSA devraient donc consolider ces positions en **multipliant les options d'équipements pour les armées clientes**. Autrement dit, cette évolution devrait **élargir les perspectives d'interopérabilité par identité de systèmes et de charges utiles américaines** et réduire la recherche de compatibilité.

Pour autant, vu de l'OTAN, ce que confirmeraient au demeurant les efforts entrepris dans le cadre de la CSP, il semble que cette offensive américaine se heurte à une volonté des pays-membres européens, plus claire encore que par le passé, de préservation de leurs BITD, non seulement de la part de la France mais aussi de ses grands alliés, à l'exception des Britanniques. C'est tout particulièrement le cas des Allemands, qui sont particulièrement organisés pour maîtriser les projets d'architectures SIC (en dépit de l'absence d'un grand industriel spécialisé outre-Rhin) et des Italiens, dont l'influence dans ce domaine est importante. Ceci compromet les perspectives d'exportation de l'ABMS américain, en dehors de quelques composantes, dans le cadre des futures versions du programme ACCS[61].

Partie 3 – Implications pour les armées et recommandations

1. Quelles priorités des efforts d'interopérabilité ?

Les priorités d'interopérabilité dépendent bien évidemment de trois grands paramètres : l'ambition opérationnelle française, les types d'interventions envisageables, enfin les partenariats opérationnels.

1.1. Ambitions et cadres d'engagement

Au premier chef, l'interopérabilité dépend **du chemin que poursuivra la France sur le plan stratégique**. C'est une évidence mais il faut le rappeler.

Dans l'hypothèse d'une dégradation du niveau d'ambition, notamment par la suite d'arbitrages budgétaires défavorables, affectant la volonté comme l'aptitude à la conduite des OPEX, la position stratégique de la France serait ramenée à celle de son positionnement géostratégique comme Finistère occidental d'une Europe stratégiquement tournée vers l'Est. Dans ce contexte, l'interopérabilité principale serait uniquement à maintenir avec les alliés de l'OTAN. Cette configuration n'exigerait pas non plus d'effort massif de développement d'interopérabilité interarmées dans la mesure où nos forces ne constitueraient plus réellement une matrice de coordination ou d'intégration.

Pour le présent exercice, on gardera cependant comme postulat qu'en dépit de la crise anticipée, la France conservera l'ambition et les capacités d'intervenir pour défendre ses intérêts à l'extérieur (et ceux de bon nombre de ses alliés).

Le second paramètre est celui des interventions envisageables. Sur ce plan, la crise ne remet pas en cause les principaux horizons potentiels de ces interventions :

- L'endiguement djihadiste et la gestion de crise en Afrique où la France reste en situation de leadership, qu'elle poursuive ou non Barkhane/Sabre sous sa forme actuelle, ce qui apparaît douteux. La crise sur ce plan est de nature à fragiliser plus encore plusieurs États de la région, démultipliant les risques de gestion de crise ;
- La confrontation avec un éventuel adversaire émergent ou la capacité à réaliser une gestion de crise, sur les pourtours méditerranéens, notamment au Levant et au Moyen-Orient ;

- L'aptitude à dissuader Moscou de tout aventurisme dans ses atterrages, se traduisant par la capacité à effectuer les déploiements les plus massifs des contrats opérationnels à l'Est et dans l'Atlantique ;
- La réponse à une éventuelle menace exercée sur une de nos possessions outre-mer ou de nos ZEE, par exemple à des fins d'intimidation, de coercition, voire d'appropriation, notamment en zone indopacifique.

1.2. La criticité du maintien des partenariats opérationnels

Le troisième paramètre est celui de nos partenariats opérationnels.

Sur ce plan, beaucoup dépend de la variable clé que constituent les niveaux d'engagement américain et britannique. **Le triptyque militaire US-UK-FR reste l'épine dorsale de la capacité d'intervention occidentale**. Rien dans la présente crise ne remet en cause l'impératif à maintenir ces liens privilégiés, bien au contraire. Dans le cas d'une implication américaine future, même si les stratégies directes reposant sur les déploiements massifs de l'Army sont encore moins probables que dans la période récente, les capacités de projection des feux ou encore les « *enablers* » en ISR et en mobilité continueraient d'être déployés en coordination ou en intégration opérationnelle avec leurs partenaires et de représenter l'armature des coalitions. **Dans ce cas, le maintien d'un haut niveau d'interopérabilité avec ces forces continue d'être un impératif.**

Il s'agit, de surcroît, de maintenir ou de renforcer **un quadruple effort d'interopérabilité « ciblée »** :

- **Avec le club des alliés européens interventionnistes** incluant bien entendu le Royaume-Uni déjà évoqué, la Belgique, les Pays-Bas et la Norvège mais aussi le Danemark ;
- **Avec les nations du flanc sud, l'Italie, l'Espagne et la Grèce**. Bien que ces acteurs soient peu interventionnistes, les risques de dégradation des conditions sécuritaires sur le pourtour méditerranéen, notamment au Levant, rendent indispensable la faculté à opérer avec eux ;
- **Secondairement, avec le partenaire allemand comme élément pivot, avec aussi la Pologne et des partenaires externes comme la Suède**, dans la mesure où la France peut être appelée à constituer une part importante d'un éventuel dispositif de dissuasion et de réassurance à l'Est ;
- **Avec nos partenaires africains**, tout particulièrement, sur ce qui reste notre principal théâtre d'opération.

1.3. Le renforcement de l'interopérabilité interarmées comme priorité absolue

Il convient aussi de préparer les scénarios où nos partenaires seraient nettement moins présents et **réduiraient considérablement leur implication militaire extérieure**. Le théâtre afri-

cain semble à ce titre singulièrement exposé. Cette situation renforce alors la nécessité pour la France de pouvoir constituer la nation-cadre d'une coalition limitée, non seulement en Afrique mais aussi sur le pourtour méditerranéen et au Levant. Ses forces constituent donc une matrice interarmées de coordination ou d'intégration de la coalition, sur laquelle viennent se « *plugger* » les autres partenaires.

Même si ce rôle est partagé ou dévolu à un autre allié, le format des coalitions imposera de toutes les façons d'exploiter nos forces avec un maximum d'efficacité. En outre, sur le plan opérationnel, le multidomaine comme symbiose tactique entre composantes de milieu, pour toutes les missions communes, est un impératif pour garantir le maintien de notre aptitude à délivrer des effets compte tenu de la pauvreté quantitative de nos moyens déployables face aux émergents militaires, sans même parler des forces russes.

Dans ces contextes, dont la plausibilité est de plus en plus évidente, l'interopérabilité interarmées doit représenter la priorité absolue de notre stratégie capacitaire.

2. Recommandations

2.1. Interopérabilité internationale

La réflexion sur les priorités d'interopérabilité éclaire **la pertinence des axes d'effort en cours** : Les initiatives trilatérales avec les Américains et Britanniques, qu'il importe de privilégier ; la *Combined Joint Expeditionary Force* (CJEF) avec les Britanniques ; les travaux de l'OTAN qui fournissent un socle commun, notamment au travers du FMN pour les SIC ; les jumelages d'unités avec plusieurs alliés clés (Britanniques, Italiens, Espagnols, Belges) ; l'Eurocorps ; certains des programmes CSP ; l'accroissement de la coopération en opérations en BSS avec nos forces déployées et enfin les projets à visée plus intégratrice comme SCAF ou CAMO.

Il semblerait cependant logique de développer d'autres initiatives. Il en est ainsi du **développement de programmes avec la Suède, la Pologne, les Pays-Bas** (encore peu engagés dans PSC et afin de reboucler avec les programmes déjà en cours avec la Belgique et l'Allemagne), peut-être plus encore **avec le Danemark**. Il pourrait être payant **d'appuyer**, dans le cadre ou le prolongement de CAMO, les **initiatives belges visant à rester interopérable avec les systèmes germano-néerlandais**. Il pourrait être ainsi intéressant de **rejoindre la JEF britannique** en complément de la CJEF. Le développement d'un **groupe amphibie méditerranéen** ferait également sens. Dans le même ordre idée, **des propositions de projets analogues au programme CSP de *co-basing*** dont nous assurons le pilotage, pourraient être lancées avec l'Italie et le Royaume-Uni eu égard à leurs positions stratégiques en Méditerranée si les arrangements spécifiques n'existent pas par ailleurs.

Inversement, si de nombreuses raisons motivent certainement le refus de **participation française à de multiples programmes CSP**, elle apparaîtrait cependant assez logique dans plusieurs de ces initiatives dont l'ambition semble dépasser le cadre capacitaire des participants déclarés. On pense notamment au CUAS (pilote : Italie), au dispositif militaire permettant le déploiement de capacités de secours en cas de catastrophe (pilote : Italie) ou encore

à la capacité de guerre électronique et programme d'interopérabilité pour la future coopération de renseignement, de surveillance et de reconnaissance interarmées (JISR) (pilote : République tchèque).

Nous avons vu que, dans le champ technico-opérationnel des SIC, un niveau minimal de coordination voire d'intégration opérationnelle devrait être facilité par les convergences des CES fondées sur les technologies commerciales. En revanche, le développement des opérations multidomaines impose une intégration système et une symbiose tactique reposant sur des technologies militaires spécifiques. Plusieurs éléments communs comme la SCA pour les transmissions ou encore la convergence partielle entre le MPE américain et le FMN montrent que des réalisations sont faisables à ce niveau. Cependant, il apparaît **difficile d'espérer une interopérabilité sur un spectre large de systèmes**, compte tenu des différences dans les stratégies de données des différents projets. Ces limites putatives induisent un risque de découplage accru quant aux opérations tactiques réalisables en commun, donc à un renforcement des opérations de niche confiées aux forces françaises, au moins dans le domaine aéroterrestre.

2.2. Interopérabilité multidomaine interarmées

2.2.1. Missions concernées

Plusieurs missions sont déjà entreprises selon la logique multidomaine : par essence les opérations aéroportées et amphibies, mais aussi le CAS ou encore la défense sol-air. L'extension de cette logique implique d'étendre les niveaux d'intégration opérationnelle, voire de symbiose entre les éléments de composantes, à de multiples autres missions.

À des degrés divers, la plupart des aptitudes listées dans la revue stratégique de 2017 sont concernées. Cependant, les principales aptitudes devant en priorité faire l'objet d'une interopérabilité multidomaine sont probablement :

- « Collecter, exploiter et diffuser du renseignement » ;
- « Construire, entretenir, partager une situation opérationnelle ». C'est déjà le cas aux niveaux stratégique et opératif, avec le SIA, mais cette aptitude doit également progresser aux niveaux tactiques ;
- « Obtenir et conserver les supériorités terrestre, aérienne et aéromaritime », pour les missions transverses aux différents milieux ;
- « Protéger les forces déployées contre les menaces surface-surface et contre les menaces air-surface et balistiques » ;
- « Frapper dans la profondeur (en territoire ennemi) » ;
- « Appuyer des forces au contact (renseignement, feux et cyber) ».

L'interopérabilité pour réaliser ces différentes aptitudes devrait logiquement reposer sur le développement de capacités intégrées en matière de *counterair* offensif, notamment la SEAD, d'interdiction, incluant les missions de ciblage d'opportunité, de *Time Sensitive Targeting* (TST) et de lutte antinavire. L'ensemble de ces missions implique non seulement l'armée de l'Air, l'aéronavale et les missiles de croisière de la Marine mais aussi les hélicoptères de

combat de l'ALAT voire les feux d'artillerie, surtout dès lors que ces derniers gagneront en portée. Elle implique non seulement les effecteurs mais aussi les organisations de C2 et les capacités ISR. Il s'agirait, notamment, de développer **des capacités intégrées de gestion unique :**

- **Des feux offensifs de l'artillerie**, de l'ALAT et de l'appui par le feu aérien fourni par l'armée de l'Air et la Marine ;
- **De la défense antiaérienne et antimissile**.

La démarche proposée s'inscrit donc dans le prolongement des recommandations avancées dans nos précédents travaux sur la synergie multidomaine et les feux dans la profondeur. À bien des égards, il s'agit donc **d'étendre et d'aller au-delà de l'approche actuelle de « l'intégration Air-Surface ».** La doctrine interarmées éponyme couvre au demeurant bien ce spectre de missions[62].

2.2.2. Démarche capacitaire envisageable

De telles évolutions impliqueraient bien sûr de nombreuses transformations dans le spectre DORESE. Le combat collaboratif multidomaine ne peut constituer à cet égard qu'un EFR, atteignable sur le long terme. À court-moyen terme, il apparaît plus raisonnable de progresser sur l'intégration opérationnelle des unités puis d'envisager éventuellement une fédération des systèmes de combat collaboratif élaborés par chacune des armées.

A. Sur le court-moyen terme, une progression en tache d'huile de l'intégration opérationnelle

Les armées disposent déjà de plusieurs capacités opérant de façon coordonnée : les liaisons de données tactiques comme la L16, mais aussi les systèmes ATLAS pour l'artillerie sol-sol, MARTHA pour la défense sol-air dont les modules CMD3D permettent la déconfliction des intervenants dans la troisième dimension. Ils sont reliés à ce titre à SIC-S, au réseau L16 permettant de disposer de la situation air générée par le SCCOA de l'armée de l'Air, ainsi qu'aux réseaux de la Marine. Cependant, ces outils sont employés pour déconflicter et au mieux coordonner la défense sol-air, l'emploi des drones et hélicoptères, et les feux d'artillerie, mais pas encore pour organiser une capacité intégrée de feux dans la profondeur.

Elles disposent de surcroît **d'un corpus doctrinal interarmées significatif** avec, notamment, les doctrines récentes sur le *commandement des engagements opérationnels hors du territoire national*[63] (CEO) et sur l'ASI qui fournissent déjà de remarquables instruments, pédagogiques et détaillés, prescrivant des arrangements de C2 entre composantes permettant une intégration opérationnelle au moins à haut niveau.

Pour aller au-delà et développer « vers le bas » cette intégration, **une approche incrémentale et *bottom-up*, fondée sur une suite d'expérimentations tactiques, mission par mission,** comme le proposent plusieurs officiers TACP de l'USAF concernant ABMS aux États-Unis, pourrait représenter la voie à exploiter[64].

Pour la développer, il est par exemple possible d'envisager **une extension de la logique DACAS** ce d'autant qu'elle est déjà considérée, à tout le moins dans l'armée de Terre, comme un mode d'action dans le cadre d'une mission qui reste l'appui-feu. Elle procède déjà d'une intégration partielle, via le rôle du JTAC, des réseaux des acteurs de la gestion des feux sol-sol et du contrôle air. On peut aussi envisager **une extension des procédés de conduite en mode collaboratif du processus de TST** associant l'ensemble des composantes au niveau des états-majors interarmées de coalition.

Cependant, **se pose immédiatement la question de la doctrine et des organisations**. Envisager qu'une patrouille de Rafale fournissant du *Non Traditional ISR* « parle » directement à une batterie d'artillerie sur ATLAS est une chose en matière de SIC, mais le défi central demeure celui de la doctrine du C2 : quel doit être le niveau de contrôle de l'engagement, selon quelle organisation, en vertu de quels principes partagés ? Il convient à cet égard tout d'abord de vérifier dans quelle mesure **les doctrines interarmées récentes** nécessiteraient des ajustements pour prendre en compte cette progression vers ce niveau de coopération opérationnelle tactique qui suppose la capacité à intégrer des actions de moyens de différents milieux pour réaliser un même effet tactique. Ces doctrines offrent déjà des outils significatifs, tels que les arrangements « Commandant bénéficiaire/Commandant en appui » qui structurent la doctrine ASI, appelés « relations bénéficiaire/en appui » RBEA dans la doctrine CEO. La logique est de fixer les arrangements RBEA lors de la planification, au niveau opératif, puis de faire jouer, lors de la conduite, ces relations entre les composantes. La doctrine prévoit aussi la possibilité de désigner des chefs de mission interarmées pour des tâches déterminées. La question est de savoir s'il convient de compléter ces dispositifs. Il est probable que la réponse soit positive. Le véritable défi d'une intégration opérationnelle plus poussée en temps proche du réel est en effet de **pouvoir affecter, en vertu du principe de subsidiarité, les autorités de prise de décision au meilleur niveau en fonction du contexte opérationnel.** Il s'agit donc de **flexibiliser et de rendre plus dynamique la délégation** au sein d'une composante ou **le transfert** vers une autre composante **du contrôle tactique des moyens impliqués.**

Se pose aussi la question de **l'information à partager**. En découle, au-delà de la doctrine, le besoin d'élaborer une première 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 concomitants entre les acteurs impliqués.

Ce développement irait de pair avec celui de **l'interopérabilité technique** des éléments de C2, c'est-à-dire avec le développement de l'ensemble des **interfaces « horizontales »** nécessaires, complémentaires des articulations verticales apportées par SIA : entre CAOC/AWACS, porte-avions/Hawkeye/frégates, voire chasseurs utilisés en nœuds tactiques et PC terrestres gérant l'ALAT et les feux. Le développement de ces interfaces nécessite de prendre en compte, au-delà de l'existant, le développement mené en parallèle, car déjà bien engagé, des **nouvelles architectures de chaque armée (SIC-S, Connect@aéro, Axon@V,** voir ci-dessous). À ce niveau, la transition progressive non seulement des unités de l'armée de Terre mais aussi de l'armée de l'Air et de la Marine vers les réseaux radios CONTACT devrait contribuer grandement à évoluer vers cette capacité. Concomitamment, **l'exploitation des méthodes type « DevOps » devrait aussi être explorée pour le développement de l'interopérabilité sélective de ces SIC**.

Des **TTP communes en matière de guerre cyber-électronique** qui constitue un domaine commun aux différentes armées, seraient aussi logiquement à développer.

Enfin, le principal défi auquel se heurte la consolidation de cette intégration opérationnelle réside dans **la formation et l'entraînement**.

Maintenir les savoir-faire en matière de gestion des appuis et les soutiens représente déjà une gageure pour chaque armée. Au-delà de la doctrine, cette intégration devrait faire l'objet de TTPs et donc trouver sa place dans les cursus de formation et dans des exercices interarmées. Ces **exercices interarmées** devraient être plus nombreux qu'ils ne sont actuellement. Une piste pourrait être d'étendre les champs de mission et de développer ou accentuer le caractère interarmées des grands exercices existants. Cette dynamique pourrait exploiter également les couplages déjà effectués entre certains de ces exercices. Par exemple, une nouvelle version du couplage Serpentex (appui aérien, armée de l'Air) / Toll (artillerie, armée Terre) consacrée non seulement à l'appui mais aussi à l'interdiction pourrait peut-être faire sens. Dans son devis capacitaire *Regain the Advantage*, l'amiral Davidson commandant l'USINDOPACOM, entend **mettre en réseau l'ensemble des sites d'entraînement** de ses composantes (Pacific Air Forces, Army Pacific, 3ème et 7ème flottes, etc.)[65]. Il pourrait être intéressant d'orienter nos liaisons afin de suivre le déroulement de cette initiative que le Congrès devrait financer à partir de 2021.

Cependant le coût et la complexité d'organisation de ces exercices ne peuvent en faire l'unique moyen d'amélioration de cette intégration. Un recours accru aux **outils de simulation,** actuellement sous-exploités en raison semble-t-il de la méconnaissance quant à leurs apports[66], serait probablement indispensable dans l'ensemble du cadre de la préparation opérationnelle. L'intégration ne pourra à cet égard que bénéficier des projets visant à établir un socle technique commun et réaliser des simulations distribuées « inter-composantes » au niveau des bases et garnisons. **La fédération des outils employés** par les différentes composantes, pour ce qui concerne les missions considérées, serait peut-être une voie à suivre.

B. Sur le long terme, le développement du combat collaboratif fondé sur la symbiose, entre les éléments de chaque armée

À plus long terme serait donc nécessaire de développer un combat collaboratif interarmées réel, intégrant cette fois, en tant que de besoin, non seulement les systèmes C2 mais aussi les éléments ISR et effecteurs terrestres, aériens et navals (y compris par exemple, les systèmes de drones en *Manned-Unmanned Teaming)* pour les missions considérées.

Cette interopérabilité nécessiterait bien entendu tout d'abord **une doctrine interarmées et des TTPs de combat collaboratif** consolidant le champ normatif ainsi que l'inclusion de ce combat dans **les cursus de formation et les exercices interarmées**, permettant de faire converger les armées sur le plan culturel.

Comme évoqué *supra*, **sur le plan technique et normatif**, chacune des armées est bien engagée dans le développement de sa future architecture :

- 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.

Or, **la convergence de ces projets est nécessaire** pour réaliser ces opérations réellement multiplateformes. Il apparaît donc logique de travailler en amont à **la compatibilité des évolutions de ces architectures de communication,** notamment des futures liaisons de données tactiques que ces projets impliquent et qui remplaceront la génération actuelle. Mais contrairement à une « simple » intégration opérationnelle avec interfaces, cela ne suffit plus.

La démarche nécessiterait donc plus globalement une **synchronisation de ces projets.** Il serait nécessaire de développer une stratégie permettant**, de façon sélective et incrémentale, des gestions de données opérationnelles compatibles,** entre les *clouds* que chacune de ces bulles constitue. Elle serait fondée sur une nouvelle série de ***Joint Mission Thread*** **plus détaillée** guidant en substance les échanges d'information à réaliser entre systèmes tactiques. Sans une harmonisation de ces développements, nécessairement « top down », la symbiose tactique serait impossible.

Enfin, en sus des efforts de convergence décrits ci-dessus, une approche pourrait être de créer de nouvelles organisations intégrées de combat collaboratif multidomaine. Une piste pourrait être par exemple de constituer plusieurs **unités ou centres de mise en œuvre interarmées (ou à vocation interarmées) intégrant feux, guerre cyber-électronique et appui spatial (SATCOM, PNT et ISR)**, un peu sur le modèle des *Multidomain Task Force* que l'US Army met actuellement sur pied.

Annexe 1 RESUME DES PROGRAMMES DE LA CSP

La CSP a donné lieu à trois séries de projets actés en mars puis novembre 2018 et novembre 2019, totalisant désormais 43 projets[67] :

- 10 dans le domaine des infrastructures et systèmes d'entraînement ;
- 6 dans le domaine des armements terrestres ;
- 6 dans le domaine des capacités navales ;
- 4 dans le domaine aérien ;
- 11 dans le domaine du soutien et autres capacités interarmées (santé, logistique, mobilité) ; 8 projets cyber et C4ISR ;
- Enfin 2 projets spatiaux.

La première série de 17 projets a apparemment obéi à une logique allemande très inclusive quant à la participation des États membres. Elle incluait au demeurant bon nombre de projets déjà lancés. Les projets décidés en 2018 et 2019 rassemblent un peu moins de participants et relèvent d'une logique de différentiation plus marquée, initialement plutôt défendue par la France. Les quatre principaux acteurs de la CSP sont dans l'ordre la France (qui participe à 30 projets et en pilote 10, parmi les plus ambitieux, qu'il s'agisse de plates-formes ou de capacités de combat futures), l'Italie, l'Espagne et l'Allemagne, suivis d'un second peloton : Grèce, Roumanie, Belgique, Pays-Bas, Portugal et Pologne.

Annexe 2 LES COUCHES D'UN SYSTEME D'INFORMATION ET DE COMMUNICATION

Tout système SIC se caractérise par un empilement de couches allant des transmissions à l'application gérée par l'utilisateur derrière son écran. On peut les résumer en cinq niveaux :

- Le réseau : l'émission/réception du signal, les systèmes d'adressage physiques organisant les trames de données, les protocoles de réseau organisant les paquets de données à transmettre (par exemple l'*Internet Protocol) ;*
- La première couche propre à l'entité utilisatrice (état-major, entreprises, etc.) : les éléments « physiques » notamment ses serveurs de données et leur virtualisation, etc. ;
- La couche logicielle : le système d'exploitation, le « *middleware* », les fonctionnalités communes à l'ensemble des utilisateurs (authentification, répertoire de messagerie, fonctions de base des outils collaboratifs, etc.) et la synchronisation des échanges. Avec les éléments physiques, elle représente les « *Core Enterprise Services* » (CES) fournis à l'entité ;
- La couche des données, leur nature mais aussi la façon dont elles sont structurées pour être exploitables. Une partie de ces données est organisée de façon ségréguée selon différentes « communautés d'intérêts » (que constituent par exemple les participants d'une fonction opérationnelle) ;
- Enfin, la couche des applications de l'utilisateur.

Annexe 3 LES PRINCIPALES ARCHITECTURES OUVERTES MODULAIRES AMERICAINES

Les principaux standards des *Modular Open Systems Architecture* (MOSA) américains sont[68] :

- **Future Airborne Capability Environment (FACE),** le plus ancien, le plus large quant à son *scope* et à la participation industrielle (l'« Open Group »), initialement sponsorisé par la Navy et l'Army, et concernant les interfaces logicielles en avionique[69] ;
- **Sensor Open Systems Architecture (SOSA),** incubé dans FACE, initié par l'Air Force, concerne les interfaces logicielles et physiques pour tous les types de capteurs, systèmes de GE et de communication. C'est autour de SOSA que s'organise la convergence des différents autres standards, y compris dans le domaine terrestre[70] ;
- Ces standards qui convergent sur SOSA sont par exemple le **Hardware Open Systems Technologies (HOST**) impulsé par la Navy, mis en œuvre sur de nouveaux composants du F-35, et le **C4ISR/EW Modular Open Suite of Standards (CMOSS),** impulsé par l'Army, mis en œuvre par exemple sur le système aéroporté de guerre électronique ou sur le système de situation tactique *Joint Battle Command –Platform* (JBC-P)[71] ;
- L'autre grand standard est l'**Open Mission Systems (OMS),** spécifié par l'Air Force concernant le transfert et les formats de données pour l'avionique comme les systèmes des centres d'opérations. Il dérive des standards utilisés pour les systèmes de drone, **Universal Command and Control Interface (UCI).**
- Le **Vehicular Integration for C4ISR/EW Interoperability (VICTORY)** sponsorisé par l'Army, est l'un des autres standards de vétronique ;
- Enfin, le SCA concernant les radios logicielles.

Références

[1] NATO Consultation, Command and Control (C3) Agency, *NATO Network Enabled Capability Feasibility Study, Executive Summary : Version 2.0*, October 2005 – http://www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf

[2] JP 1.

[3] Les États-Unis envisagent la synergie à double titre : tout d'abord sous l'angle interarmées, interalliés et interministériel, ensuite sous l'angle interdomaine, devenu multidomaine. La notion de synergie pose toutefois problème. D'une part, la synergie est une finalité recherchée même aux autres niveaux (elle est d'ailleurs synonyme « d'action coordonnée » dans bon nombre de définitions générales). D'autre part, la notion de multidomaine relève déjà d'un cas particulier d'application de cette synergie.

[4] EMAA / B.PLANS, Concept exploratoire, *Combat collaboratif aérien connecté,* Avril 2020, n° 00501068/ARM/EMAA/SCPA/BPLANS/NP

[5] Christopher G. Pernin et alii, « Targeted Interoperability: a New Imperative for Multinational Operations », RAND : Santa Monica, CA, 2019, p. 71 – https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2075/ RAND_RR2075.pdf

[6] Xavier Vavasseur, « U.S., French Navies Conduct Dual-Carrier Ops in Mediterranean », *Naval News*, 3 mars 2020 – https://www.navalnews.com/naval-news/2020/03/u-s-french-navies-conduct-dual-carrier-ops-in-mediterranean/

[7] Voir par exemple le dossier de *Cols Bleus* – https://www.colsbleus.fr/articles/10553

[8] Lire par exemple, *Allied Interoperability & Coordination Guide*, CJOS COE Version 1.0, novembre 2018 – http://www.cjoscoe.org/infosite/wp-content/uploads/2018/10/Allied-Interoperability-and-Coordination-Guide.pdf

[9] GCA (2S) Éric Margail, « Interopérabilité, on peut encore s'améliorer », Blog *Theatrum Belli,* 8 juillet 2019 – https://theatrum-belli.com/interoperabilite-on-peut-encore-sameliorer/

[10] Propos entendu lors du *Brown Bag Seminar* de l'IFRI, 16 mars 2020.

[11] Expérience directe de l'auteur.

[12] Karen DeYoung, Greg Miller, « Allies Guided Rebel 'Pincer' Assault on Tripoli », *Washington Post*, 22 août 2011.

[13] *Audition du général Christophe Gomart, directeur du renseignement militaire, sur le projet de loi relatif au renseignement*, Commission de la défense nationale et des forces armées, Compte rendu n° 49, 25 mars 2015 – http://www.assemblee-nationale.fr/14/cr-cdef/14-15/c1415049.asp

[14] Elie Tenenbaum, avec Morgan Paglia et Nathalie Ruffié, « Confettis d'empire ou points d'appui ? L'avenir de la stratégie française de présence et de souveraineté », Ifri, *Focus stratégique*, février 2020.

[15] Aline Leboeuf, « Coopérer avec les armées africaines », Ifri, *Focus stratégique*, octobre 2017.

[16] Chef Opérations du GTRS MONNA CASALE, Chef du BOI du 53e RT, « Opération Barkhane, un défi permanent », *Transmetteurs*, n° 10 – juin 2016, p. 24.

[17] Center for Army Lessons Learned, *Multinational Interoperability Reference Guide*, juillet 2016, pp. 77-80.

[18] Multinational Capability Development Campaign (MCDC), Federated Mission Networking (FMN) Mission Partner Environment (MPE) Civilian-Military (FMCM) Information Sharing Guidebook, p. 1.

[19] *Federated Mission Networking, Spiral 3 Standards Profile,* 21 novembre 2018 – https://storage.nisp.nw3.dk/20181118_Final_FMN_Spiral_3_Standards_Profile_Bundle.pdf

[20] Ministère des Armées, « Le système d'information des armées (SIA) à l'heure du standard FMN de l'OTAN », 10 septembre 2019 – https://www.defense.gouv.fr/dga/actualite/le-systeme-d-information-des-armees-sia-a-l-heure-du-standard-fmn-de-l-otan

[21] Detlef Janezic, NATO Communications and Information Agency, *FMN for Coalition Operations*, présentation à l'AFCEA, Bonn, DEU, 22-23 juin 2016 – https://www.afcea.de/fileadmin/user_upload/Sonderveranstaltungen/FA_mit_FueUstgKdoBw/13-NCIA-FMN1.pdf

[22] *Marianne R. Brannsten, Frank T. Johnsen, Trude H. Bloebaum, Ketil Lund, Norwegian Defence Research Establishment (FFI), Towards Federated Mission Networking in the Tactical Domain, 2015 – https://publications.ffi.no/ nb/item/asset/dspace:4084/1302683.pdf*

[23] « Network Management & Cyber Defense (NMCD) for Federated Mission Networking (FMN) », NATO STO, 2020-02-16 – https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=531

[24] Steven Blockmans & Dylan Macchiarini Crosson, « Differentiated Integration within PESCO – Clusters and Convergence in EU Defence », CEPS, n° 2019/04, décembre 2019, p. 23 – https://www.ceps.eu/wp-content/uploads/ 2019/12/RR2019_04_Differentiated-integration-within-PESCO.pdf

[25] Nicolas Gros-Verheyde, « Le Fonds européen de défense rapiécé. Est-ce grave docteur ? », Bruxelles2, 18 décembre 2019 – https://www.bruxelles2.eu/2019/12/le-fonds-europeen-de-defense-rapiece-est-ce-grave-docteur/

[26] Center for Army Lessons Learned, *Multinational Joint Forcible Entry Operations Blue Flag-Joint Warfighting Assessment 2018*, CALL 19-3, décembre 2018 – https://usacac.army.mil/organizations/mccoe/call/publication/19-03

[27] Jean-Jacques Patry, « La stratégie d'influence de la Heer allemande peut-elle être un modèle d'inspiration pour l'adT française ? », FRS, Observatoire de l'armée de Terre 2035, 2019, non publié.

[28] *DEU/NLD update on Tactical Edge Networking*, présentation au WInnComm Europe, Berlin, 16 mai 2019 – https://www.wirelessinnovation.org/assets/Proceedings/2019Europe/TS0.1_20190516_TEN%20Wireless%20Comms%20Forum.pdf

[29] Avec la volonté de l'institutionnaliser au sein de la « coopération structurée permanente » : Nathan Gain, « CAMO : derrière l'équipement la construction d'un modèle d'interopérabilité : Interview du général Marc Thys commandant de la composante terrestre belge », forcesoperations.com, 25 septembre 2019 – https://forcesoperations.com/ camo-derriere-lequipement-la-construction-dun-modele-dinteroperabilite/.

[30] Alexandre Vissoky, « Latest Developments on German Interoperability Efforts », Finabel – European Army Interoperability Centre, 12 novembre 2019 – https://finabel.org/latest-developments-on-german-interoperability-efforts/

[31] Propos entendus lors de la Private roundtable « U.S. Defense Innovation and Implications for Transatlantic Allies », with Kathryn Harris, Senior Advisor to U.S. Vice Chairman of the Joint Chiefs of Staff, German Marshall Fund, 23 mai 2018.

[32] Theresa Hitchens, « DoD Budget Cuts Likely As $4 Trillion Deficit Looms », *Breaking Defense*, 27 avril 2020 – https://breakingdefense.com/2020/04/dod-budget-cuts-likely-as-4-trillion-deficit-looms/

[33] Kathleen H. Hicks, Joseph P. Federici, *Getting to Less? Exploring the Press for Less in America's Defense Commitments*, CSIS Briefs, Center for Strategic and International Studies, 16 janvier 2020, et articles suivants – https://www.csis.org/analysis/getting-less-exploring-press-less-americas-defense-commitments

[34] Eric Schmitt, « Terrorism Threat in West Africa Soars as U.S. Weighs Troop Cuts », *The New York Times*, 27 février 2020 – https://www.nytimes.com/2020/02/27/world/africa/terrorism-west-africa.html

[35] Jean-Jacques Patry, *op. cit.* ; Gaëlle Winter, « Le redressement capacitaire de la Bundeswehr : un parcours du combattant », FRS, *Recherches & Documents*, n° 06/2019, 10 juillet 2019 – https://www.frstrategie.org/publications/recherches-et-documents/redressement-capacitaire-bundeswehr-un-parcours-combattant-2019

[36] La forme d'onde recouvre la bande de fréquence utilisée et les multiples caractéristiques de l'émission (filtrage, modulation, chiffrement etc.).

[37] Steve Bernier, Mathieu Michaud-Rancourt, François Levesque, Juan Pablo Zamora Zapata, *The Enduring Myths of the Software Communications Architecture,* NordiaSoft White Paper, 2017 – https://www.viavisolutions.com/en-us/literature/enduring-myths-software-communications-architecture-sca-white-paper-en.pdf

[38] « ESSOR – EUROPEAN SECURE SOFTWARE DEFINED RADIO », site de l'OCCAR – http://www.occar.int/programmes/essor

[39] Entretien avec les intéressés, réalisé dans le cadre de l'ETO DACAS, 2016.

[40] Jack L. Burbank, *Leveraging 5G Networks for Tactical Army Communications: The Good, The Bad, and The Ugly*, U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – C5ISR CENTER, 7 octobre 2019 – https://futurenetworks.ieee.org/images/files/pdf/FirstResponder/2019/Jack-Burbank.pdf

[41] Julianne Simpson, « 5G Offers Opportunity for Improved Allied and Coalition Communications », *SIGNAL Magazine*, 20 mai 2020 – https://www.afcea.org/content/5g-offers-opportunity-improved-allied-and-coalition-communications

[42] Defense Innovation Board, *The 5G Ecosystem: Risks & Opportunities For DoD*, avril 2019.

[43] L'une des nombreuses définitions, émanant du *National Institute of Standards and Technology* américain, désigne le cloud comme « *un modèle permettant un accès réseau omniprésent, pratique et à la demande à un pool partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement fournies et mises à disposition avec un minimum d'effort de gestion ou d'interaction avec le fournisseur de services* ». Un cloud se compose de cinq caractéristiques essentielles : service à la demande, accès de l'utilisateur aux ressources par le réseau, mise en commun de ces ressources avec d'autres utilisateurs, flexibilité de ces ressources et service mesurable. Il comprend plusieurs modèles de service

qui désignent ce qui est effectivement partagé : IaaS (*infrastructure as a service*) quand le partage concerne le réseau et les infrastructures (serveurs notamment). C'est le plus courant actuellement. Le partage peut s'étendre aux plates-formes informatiques, à leurs systèmes d'exploitation et logiciels de base : c'est le PaaS (*Platform as a service*). Enfin le partage peut porter sur les données elles-mêmes et les applications utilisées par l'opérateur : c'est le SaaS (*Software as a service*) qui est techniquement le modèle le plus simple.

[44] *DoD Cloud Strategy*, décembre 2018 – https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF

[45] Air Combat Command, *Combat Cloud Operating Concept*, cité dans : Major Jacob Hess *et alii*, *The Combat Cloud Enabling Multidomain Command and Control across the Range of Military Operations*, Wright Flyer Paper n° 65, Air University, mars 2017, p. 1 – https://media.defense.gov/2019/Mar/01/2002095278/-1/-1/0/WF_0065_HESS_COMBAT_CLOUD.PDF

[46] Office of Naval Research, *Data Focused Naval Tactical Cloud (DF-NTC)*, ONR Information Package, 24 juin 2014 – https://www.onr.navy.mil/~/media/Files/Funding-Announcements/BAA/2014/14-011-Attachment-0001.ashx

[47] MINARM, *Ambition numérique du ministère des Armées,* DICoD – Bureau des éditions – décembre 2017, p. 9 – https://www.defense.gouv.fr/content/download/522541/8762895/Ambition

[48] Général Denis Mercier, « Les opérations aériennes et le cyber : de l'analogie à la synergie », *Res Militaris*, hors-série « Cybersécurité », juillet 2015 – http://resmilitaris.net/ressources/10205/53/res_militaris_article_gaa_mercier_les_op_rations_a_riennes_et_le_cyber.pdf

[49] Entretien avec un ingénieur informatique d'une entreprise de publicité, directement engagé dans ces travaux.

[50] Entretien avec un représentant industriel national au sein de l'OTAN.

[51] Martin E. Dempsey, Chairman of the Joint Chiefs of Staff, *Joint Information Environment*, 22 janvier 2013 – http://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf

[52] Voir par exemple Maj Gen Kim Crider, Air Force Chief Data Officer, *Air Force Data Strategy*, non daté, https://nova.afceachapters.org/file/30916/download?token=GhynNWKP ou Office of Naval Research, Data Focused Naval Tactical Cloud (DF-NTC), ONR Information Package, 24 juin 2014 – https://www.onr.navy.mil/-/media/Files/Funding-Announcements/BAA/2014/14-011-Attachment-0001.ashx

[53] « Parler la même langue tactique », entretien avec le lieutenant-colonel Bertrand, *Terre Information Magazine*, n° 292, mars 2018, p. 10 – https://www.defense.gouv.fr/web-documentaire/nosallies/assets/files/dossier-nos-allies.pdf

[54] Entretien avec un représentant industriel national au sein de l'OTAN.

[55] Qu'il suffise ici de rappeler notre définition de la notion, à savoir « *l'emploi complémentaire plutôt que l'utilisation additive de capacités ISR, de C2, effectrices ou de soutien dans différents domaines (milieux terre, air, mer, espace ainsi que le domaine cyber), de manière à ce que chacune améliore l'efficacité et compense les vulnérabilités des autres, en conduite, au niveau tactique, réalisé le cas échéant transversalement aux composantes de force* ».

[56] « The CaMo Programme: A Strategic Partnership to Modernize the Belgian Army's Motorized Capacity », Interview: Major General Pierre Gérard, FinabelPost, 20 mars 2020 – https://finabel.org/interview-major-general-pierre-gerard/

[57] « Interoperability by Design: The Future of Naval Fleet Collaboration », entretien avec le Commander Andreas Uhl, Defense IQ, Surface Warships Event, 28-30 janvier 2020 – https://www.defenceiq.com/events-surfacewarships/downloads/interoperability-by-design-the-future-of-naval-fleet-collaboration?-ty-m

[58] Secretary of the Army, Secretary of the Navy, Secretary of the Air Force, *Modular Open Systems Approaches for our Weapon Systems Is a Warfighting Imperative*, Memorandum for Service Acquisition Executives and Program Executive Officers, 7 janvier 2019 – https://www.dsp.dla.mil/Portals/26/Documents/PolicyAndGuidance/Memo-Modular_Open_Systems_Approach.pdf

[59] By Steve Kelman, « Why Kessel Run is such a Big Deal », FCW, 12 février 2019 – https://fcw.com/blogs/lectern/2019/02/kelman-kessel-run-usaf-big-deal.aspx

[60] B. T. Kenner, *Too Agile? – DevOps Software Development Challenges in a Military Environment*, Master's thesis, 2019 – https://scholarcommons.sc.edu/etd/5396

[61] Entretien avec un représentant industriel national au sein de l'OTAN.

[62] *Intégration Air-Surface*, *Air-Surface Integration* (ASI), Doctrine interarmées DIA-3.0.3_ASI (2017), N°134/ARM/CICDE/NP du 7 juillet 2017.

[63] Commandement des engagements opérationnels hors du territoire national, Doctrine interarmées DIA-3.0_CEO_ L1_HTN (2019), N° 127/ARM/CICDE/NP du 17 juillet 2019.

[64] Paul Birch, Ray Reeves & Brad Dewees, « Build ABMS From Bottom-up, For The Joint Force », *Breaking Defense*, 13 mai 2020 – https://breakingdefense.com/2020/05/build-abms-from-bottom-up-for-the-joint-force/

[65] National Defense Authorization Act (NDAA) 2020, Section 1253 Assessment, *Executive Summary, Regain the Advantage, U. S. Indo-Pacific Command's (USINDOPACOM) Investment Plan for Implementing the National Defense Strategy Fiscal Years 2022-2026* – https://int.nyt.com/data/documenthelper/6864-national-defense-strategy-summ/8851517f5e10106bc3b1/optimized/full.pdf

[66] Groupe Armées DGA Industrie pour la Simulation, Collèges des Armées et de la DGA, *Préparer les engagements futurs par un juste recours à la simulation*, septembre 2015 – https://www.christophe-assens.fr/app/download/ 13928238624/20150327-PLAQUETTE+SIMULATION-2015.pdf?t=1484836695

[67] Le tableau actualisé des programmes est disponible sur https://www.consilium.europa.eu/media/41333/pesco-projects-12-nov-2019.pdf

[68] John Bowling, *Open Systems Standards and Agile Acquisition*, AF Life Cycle Management Center, presentation, 25 octobre 2018 – https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2018/systems/Thurs_21359_Bowling.pdf

[69] Dennis Stevens Lockheed Martin Corporation, Jeffry A Howington Rockwell Collins, David Boyett US Army AMRDEC ; Kirk Avery, Lockheed Martin Corporation, *FACE™ Master Class*, présentation, 28 avril 2016 IOA 2016 London, England – https://prod.opengroup.org/sites/default/files/contentimages/face_master_class_presentation_final_v3.pdf & Joyce L. Tokar, PhD, Pyrrhus Software, LLC, *An Examination of Open System Architectures for Avionics Systems – An Update* Air Force FACE™ TIM Paper, mars 2017 – https://www.researchgate.net/publication/315736224_An_Examination_of_Open_System_Architectures_for_Avionics_Systems_-_An_Update

[70] Dr. Steven A. Davidson, Raytheon Space and Airborne Systems, The Sensor Open Systems Architecture (SOSA™) in a Nutshell, présentation, 24 octobre 2018 – https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2018/systems/Thurs_21371_Davidson.pdf

[71] John Keller, « SOSA Open-systems Standards for Military Embedded Computing could Double or Triple the Market », *Military & Aerospace Electronics*, 29 janvier 2019, & « Open-systems Electronics Standards for Military Embedded Computing Gaining Money and Traction », *Military & Aerospace Electronics,* 6 février 2019 – https://www.militaryaerospace.com/computers/article/16722139/opensystems-electronics-standards-for-military-embedded-computing-gaining-money-and-traction