Centre interarmées
de concepts,
de doctrines et
d'expérimentations

Les systèmes d'information et de communication (SIC) en opérations

Doctrine interarmées DIA-6_SIC-OPS(2014)

N° 147/DEF/CICDE/NP du 24 juin 2014

Amendée le 16 janvier 2016

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE
DE LA DÉFENSE

Avertissement

Ce document de Doctrine a été élaboré par le Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE). Il est promulgué et rendu public par le Directeur du CICDE, dans le cadre de ses missions de développement et expérimentation de la doctrine interarmées dans un contexte national ou multinational, et de participation aux études et recherches au niveau interministériel.

Il a été conçu et rédigé par un collège d'experts affectés au CICDE : c'est un document de Doctrine et non un acte juridique ; il n'a en particulier aucune portée réglementaire.

Ainsi qu'il est exposé aux § 107 à 111 du document-cadre DC_001(A)_DOCTRINE(2013) pour la doctrine en général, le contenu de ce document sert de référence commune, donne à la réflexion un cadre analytique rigoureux et contribue à définir un langage et des méthodes partagés par tous ceux qui ont pour tâche d'élaborer ou d'exécuter des plans, des missions ou des ordres. Il ne saurait donc en rien affecter l'autorité ni limiter la responsabilité du commandement, que ce soit dans le domaine de l'organisation des forces ou dans celui de la conception et de l'exécution des missions.

Intitulée *Les systèmes d'information et de communication (SIC) en opérations*, la Doctrine interarmées (DIA)-6_SIC-OPS(2014) respecte les prescriptions de l'*Allied Administrative Publication (AAP) 47(A)* intitulée *Allied Joint Doctrine Development*). Elle applique également les règles décrites dans le *Lexique des règles typographiques en usage à l'Imprimerie nationale* (LRTUIN, *ISBN 978-2-7433-0482-9*) dont l'essentiel est disponible sur le site Internet www.imprimerienationale.fr ainsi que les prescriptions de l'Académie française. La jaquette de ce document a été réalisée par le Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE).

Attention : la seule version de référence de ce document est la copie électronique mise en ligne sur les sites Intradef (http://www.portail-cicde.intradef.gouv.fr) et internet (http://www.cicde.defense.gouv.fr) du CICDE.

Directeur de la publication

Vice-amiral Arnaud de TARLÉ

21 Place Joffre-BP 31
75 700 PARIS SP 07
Téléphone du secrétariat : 01.44.42.83.31
Fax du secrétariat : 01.44.42.82.72

Rédacteur en chef

Colonel (air) Laurent AUBIGNY

Auteurs

Document collaboratif placé sous la direction du Colonel (terre) Jérôme PELLISTRANDI
[Amendements apportés par le Colonel (terre) Olivier THIBESARD]

Conception graphique

Premier maître Philippe JEANVOINE

Crédits photographiques

Ministère de la Défense

Imprimé par

EDIACA
Section IMPRESSION
76 rue de la Talaudière-BP 508
42007 SAINT-ÉTIENNE cedex 1
Tél : 04 77 95 33 21 ou 04 77 95 33 25

Dépôt légal
Juin 2014

ISBN 978-2-11-138554-2

DIA-6_SIC-OPS(2014)

Les systèmes d'information et de communication (SIC) en opérations

N° 147/DEF/CICDE/NP du 24 juin 2014

Amendée le 16 janvier 2016

(PAGE VIERGE)

Lettre de promulgation

Paris, le 24 juin 2014

N°147/DEF/CICDE/NP

Objet : Promulgation de la doctrine interarmées (DIA)-6_SIC-OPS(2014).

Références :

La doctrine interarmées (DIA)-6_SIC-OPS(2014), les systèmes d'information et de communication (SIC) en opérations, en date du 24 juin 2014 est promulguée.

Vice-amiral Arnaud de TARLÉ
Directeur du Centre interarmées de concepts,
de doctrines et d'expérimentations
(CICDE)

(PAGE VIERGE)

Récapitulatif des amendements

1. Ce tableau constitue le recueil de tous les amendements proposés par les lecteurs, quels que soient leur origine et leur rang, transmis au Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE) en s'inspirant du tableau proposé en annexe B (voir page 81).

2. Les amendements validés par le CICDE sont inscrits **en rouge** dans le tableau ci-dessous dans leur ordre chronologique de prise en compte.

3. Les amendements pris en compte figurent **en violet** dans la nouvelle version.

4. Le numéro administratif figurant au bas de la première de couverture et la fausse couverture est corrigé **(en caractères romains, gras, rouge)** par ajout de la mention : ***« amendé(e) le jour/mois/année. »***

5. La version électronique du texte de référence interarmées amendé remplace la version antérieure dans toutes les bases de données informatiques.

N°	Amendement	Origine	Date de validité
1	**Révision du document en 2015**	**CICDE**	**16 janvier 2016**
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			

(PAGE VIERGE)

Références

a. *Concept d'emploi des forces* **CIA-01**, septembre 2013.

b. **AJP 6**, *Allied joint doctrine for communications and information systems*, avril 2011.

c. **MC 0593/9 Draft**, *minimum level of command and Control C2*, juillet 2011.

d. **STANAG 5048** -*The minimum scale of connectivity for communication and information systems for NATO land forces*.

e. **DIA-3(A)_CEO(2014)**, commandement des engagements opérationnels, n° 151/DEF/CICDE/DR du 25 juin 2014.

f. Arrêté du 30 novembre 2011 *portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale*.

g. Instruction interministérielle relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI) n° 910/SGDSN/ANSSI du 22 octobre 2013.

h. Instruction n°2100/SGDN/SSD/DR du 01/12/1975 *relative à l'application en France du système de sécurité de l'OTAN.*

i. *Politique de sécurité des systèmes d'information des armées* (**PSSI-A**) n° D-13-009808/DEF/EMA/CPI/SSI/DR du 1er août 2013.

j. *Directive d'assignation des fréquences et de gestion des sites et des servitudes radioélectriques au sein du ministère de la défense*, n° 900004/DEF/DIRISI/SCOE/DIVOPS de janvier 2010.

k. *Politique du système d'information du ministère de la défense*, version 6 du 31 janvier 2013 transmise par lettre n° 02776/DEF/CAB/CC5A du 28 mars 2013.

l. *Politique de l'informatique en nuage du ministère de la défense*, version du 7 février 2014 transmise par lettre n°90/DEF/DGSIC/SDS/NP du 7 février 2014.

m. Directive DGSIC n°18 *relative à l'organisation du domaine des fréquences* du 11 juillet 2011.

n. **PIA-6.4.3_*FrOpS* (2014)**, politique générale d'emploi du réseau des opérations *FrOpS*, n°2217/DEF/EMA/CPCO/CDT/DR du 17 juin 2014.

o. **PIA-6.2_SATCOM(2015)**, les communications satellitaires (à paraître sous timbre du Commandement interarmées de l'espace).

Préface

1. Les SIC sont étroitement liés à l'organisation générale du commandement opérationnel. Les architectures SIC sont ainsi définies sur les bases de l'organisation du commandement retenue pour la conduite d'une opération et des besoins en services et en échanges.

2. Les SIC assurent principalement la mise à disposition des informations par le transport via les systèmes de communication (SC). Les SIC permettent d'élaborer, d'échanger, de stocker, d'agréger l'information opérationnelle via certains systèmes d'information (SI) déployés, entre des états-majors en métropole jusqu'au plus petit élément tactique projeté sur un théâtre.

3. La complexité croissante des architectures, les évolutions technologiques rapides et l'accroissement exponentiel des échanges d'informations caractérisent les opérations actuelles. Le champ d'action des SIC s'accroît en raison de l'augmentation des besoins en informations

de natures différentes, du tempo des activités militaires, de l'expansion de la numérisation des systèmes d'armes et de l'interopérabilité des équipements.

4. Les SIC doivent également répondre aux exigences des opérations multinationales, en particulier conduites par l'OTAN, l'UE ou une coalition ad hoc, imposant une convergence technique et doctrinale.

5. Le CPCO J6 assume au niveau stratégique un rôle central dans la conception et la conduite des opérations tant nationales qu'en coalition. Il s'appuie sur l'expertise technique de la DIRISI et sur les armées et services qui mettent en œuvre les SIC opérationnels.

6. Les dispositifs SIC projetés en opération s'appuient sur les systèmes permanents et s'inscrivent dans une continuité temps de paix-temps de crise.

7. Les enjeux majeurs de la période à venir concernent :

   a. La supériorité informationnelle pour une optimisation du commandement et de la conduite des opérations.

   b. La sécurisation de l'information et plus largement la cyber défense des SIC.

   c. La capacité de traitement et d'échange de l'information.

8. Ces enjeux doivent désormais impérativement être intégrés dès la planification d'une opération. Ils doivent être maîtrisés par l'ensemble des échelons de commandement.

9. Ce document s'adresse principalement à :

   a. La chaîne opérationnelle interarmées, afin de lui apporter les éléments de compréhension nécessaires à la planification et à la conduite des SIC en opération.

   b. Aux armées, directions et services chargés de mettre en œuvre les SIC.

   c. Aux utilisateurs des SIC en opérations ou en préparation opérationnelle.

10. Ce document a pour objectif de :

   a. Présenter les grands principes régissant les SIC en opération.

   b. Définir les responsabilités pour la conception, la mise en œuvre et la conduite des SIC en opérations.

   c. Présenter l'emploi des SIC opérationnels.

11. Les SIC liés à la mise en œuvre de la dissuasion nucléaire ainsi que les Systèmes d'Information Scientifiques et Techniques (SIST) sous la responsabilité de la DGA, sont exclus du périmètre de la DIA 6.

Fiches pour le lecteur pressé
Généralités sur les SIC en opérations

Approche générale et principes généraux

1. Un SIC, Système d'Information et de Communication, est un système intégré d'appui au commandement destiné à fournir dans les délais requis aux autorités et à leur état-major les données nécessaires à la planification, à la conduite et au contrôle de leurs activités. Le SIC intègre le personnel, les équipements, l'organisation, les procédures, les liaisons et les éléments de doctrine (définition DC-004 Glossaire Interarmées de Terminologie Opérationnelle de 2013). Au sein des SIC, on distingue :

   a. Les SC, Systèmes de Communication (ou *Communication Systems)*, qui sont l'ensemble de matériels, de méthodes et de procédures, et le cas échéant de personnes, organisé pour accomplir des fonctions de **transfert d'informations** (cf. *AAP 31 (2010)).*

   b. Les SI, Systèmes d'Information (*Information Systems),* qui sont l'ensemble de matériels, de méthodes, de procédures et, le cas échéant, de personnes, organisé pour accomplir des fonctions déterminées de **traitement d'informations** (cf. *AAP-31 (2010)).*

2. Les SIC sont présents dans toutes les fonctions stratégiques identifiées par le LBDSN de 2013. Ils sont essentiels dans la planification et la conduite des opérations (prise de décision, tempo, réactivité, supériorité informationnelle, optimisation des capacités, interopérabilité avec nos alliés…) et dans l'exécution des missions permanentes confiées aux armées. Ils concourent à toutes les actions majeures à accomplir au cours d'un engagement opérationnel (commander, préparer l'intervention, intervenir) et irriguent les huit fonctions interarmées[1] identifiées par la doctrine OTAN[2].

3. Les SIC reposent sur :

   a. Les Systèmes de communication (SC), permettant le transport des flux d'information à travers des réseaux de télécommunications fixes ou mobiles, déployables en opération.

   b. Les Systèmes d'Information (SI), assurant le management de l'information et son stockage.

   c. La Sécurité des systèmes d'information (SSI ou cyber protection) permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, et des services que ces systèmes offrent ou qu'ils rendent accessibles.

4. La mise en œuvre des SIC s'appuie sur des principes génériques comme le juste besoin, le raccordement du bas par le haut, la fiabilité et la sécurité. L'ensemble de ces principes se décline en actions techniques à conduire à différents échelons. Le management de l'information est indissociable des SIC ; il s'appuie, au sein des états-majors notamment, sur une organisation, du personnel et des procédures permettant la valorisation des informations et l'optimisation des flux de données échangées.

5. La cybersécurité, ou maîtrise du cyberespace, est essentielle dans la mise en œuvre des SIC, à travers un éventail d'actions, de procédures et d'équipements, combinant la cyber protection et la cyberdéfense pour renforcer la sécurité du traitement de l'information tout en permettant des actions offensives.

6. Le Système d'Information (SI) du ministère de la défense se décline en :

   a. Systèmes d'information opérationnels et de communication (SIOC), placés sous la responsabilité du chef d'état-major des armées.

---

1 Commandement, renseignement, feux, manœuvre et mouvement, protection, soutien, influence, CIMIC. (cf. DEF).
2 Cf. *AJP*-01 *Allied Joint Doctrine.*

b. Systèmes d'information scientifiques et techniques (SIST), placés sous la responsabilité du délégué général pour l'armement.

c. Systèmes d'information, d'administration et de gestion (SIAG), placés sous la responsabilité du secrétaire général pour l'administration.

Les SIC des armées

7. Les SIC des armées comprennent des SIC d'infrastructure et des SIC mobiles ou déployables permettant la constitution de réseaux couvrant l'ensemble des besoins opérationnels.

8. Aux niveaux stratégique et opératif, le réseau SOCRATE[3] mis en œuvre par la DIRISI couvre toutes les implantations en métropole et tous les besoins du ministère.

9. Les réseaux satellitaires et HF (utilisés notamment en secours) permettent le raccordement à grande distance entre le territoire national (métropole et outre-mer) avec les théâtres extérieurs et les bâtiments de la Marine nationale. Ils peuvent être complétés par l'utilisation de services de télécommunications spatiales auprès d'opérateur privés.

10. Pour la conduite des opérations, *FrOpS*, French Operational network up to Secret level, désormais déployé sur tous les théâtres d'opérations sous l'autorité d'emploi du CPCO avec l'appui de la DIRISI et des forces, permet les échanges avec les théâtres et les alliés, dans le respect des règles de confidentialité exigées par le SGDSN et conformes aux directives de l'OTAN. *FrOpS* a vocation à être employé également en opération sur le territoire national et en opération nationale.

11. Aux niveaux opératif et tactique, les armées mettent en œuvre une palette de SC et de SI répondant à leurs besoins propres, avec la recherche d'une interopérabilité sans cesse accrue. Les réseaux de Liaisons de Données Tactiques (LDT), en particulier la liaison 16, viennent compléter les dispositifs existants.

Rôles et responsabilités, commandement, organisation et conduite

12. L'EMA/CPCO/J6 est l'autorité décisionnelle pour la planification, la mise en œuvre et la conduite de la manœuvre des SIC en opérations. Il est conseillé en cela par les EMO d'armées et s'appuie sur l'expertise technique de la DIRISI.

13. La DIRISI est en charge de la mise en œuvre et de l'exploitation des réseaux stratégiques et satellitaires, contribuant ainsi à assurer les services concernés de bout en bout jusqu'aux théâtres.

14. Les EMO d'armée et de service, ainsi que l'EMIA-FE, contribuent dans leur domaine de responsabilité à la préparation et à la conduite de la manœuvre SIC, en particulier par la mise en œuvre de leurs SIC dédiés et par l'expression de leurs besoins en services.

15. Sur un théâtre, le niveau opératif est l'échelon clé pour la coordination des SIC d'une opération. La désignation auprès du commandant de la force d'un COMSICIAT s'impose, dès lors que les engagements prennent une dimension significative en termes de zone géographique, de durée et de moyens projetés, y compris sur le territoire national (où il prend l'appellation de COMSIC IA). Le COMSICIAT, correspondant direct du CPCO/J6, est le responsable de l'organisation et de la conduite des SIC au niveau opératif ainsi que de leur cyberprotection ; il exerce ces responsabilités dès le déclenchement de l'opération. Lors de la phase de planification de l'opération, l'EMA/CPCO désigne une des trois armées comme « armée responsable des SIC » (ARS) ainsi qu'un COMSICIAT qui participe aux travaux de planification avant projection. Durant la phase de projection, le COMSICIAT assure la conduite de la manœuvre des SIC. Il a autorité fonctionnelle sur une équipe J6 au sein de l'état-major opératif (ou de la chaîne nationale au cas où la France n'est pas nation cadre) et sur un groupement de transmissions interarmées (GTRS IA) responsable de la mise en œuvre et de l'exécution de la manœuvre des SIC et de l'appui au commandement au niveau opératif. Le chef du GTRS IA s'appuie sur son centre de mise en œuvre interarmées (CMO IA) pour élaborer les ordres des SIC.

[3] Dès 2017, le réseau DESCARTES, Déploiement des Services de Communication et Architecture des Réseaux de TElécommunication Sécurisés, se substituera à SOCRATE.

16. Dans le cadre des missions conduites par l'OTAN et/ou l'UE, des moyens et des procédures spécifiques permettent le raccordement des moyens nationaux aux réseaux interalliés.

17. Sur le territoire national, la DIRISI joue un rôle essentiel dans le cadre des missions permanentes (PPS, AEM) ou lors de grands évènements (G8, commémorations, etc.) en raccordant les systèmes dédiés mis en œuvre notamment par les armées.

18. Les armées peuvent être amenées à mettre en œuvre des SIC d'un autre ministère dans des missions de défense du territoire national (par exemple des SIC du Ministère de l'Intérieur dans le cadre de l'opération SENTINELLE) ou lors d'opérations extérieures.

(PAGE VIERGE)

Domaine 6 *SIC*

Cliquez sur l'enveloppe pour contacter l'officier chargé du (sous)-domaine au CICDE

Stratégie européenne de sécurité 2003

Concept stratégique de l'OTAN 2010

Livre Blanc sur la défense et la sécurité nationale (LBDSN-2013)

Dissuasion nucléaire: Eléments constitutifs de la doctrine française

Visions politiques

Concept interarmées

MC 0400/3 2012 — NATO CONFIDENTIAL

English — CIA-01 CEF — Concept d'emploi des forces

Cliquez sur le document choisi pour le faire apparaître à l'écran !

Doctrines interarmées

AJP-01 Allied Joint Doctrine

English — DIA-01 DEF — Doctrine d'emploi des forces

AJP-6 CCIS

DIA-6 SIC-OPS

DIA-6.X SIC satellitaire

☆ La ***DIA-6.3*** est abrogée par la ***DIA-3.40***, du sous-domaine ***3.40 Cyberdéfense***

Publications interarmées

PIA-6 SIC

PIA-6.4.1 REMO SYRACUSE

PIA-6.4.2 CCMO SIC du niveau opérati

Réflexions Doctrinales & Concepts Exploratoires

RDIA-2013/001 Réseaux sociaux

Publications de l'EMUE

8665/02 CIS Concept

12737/08 NEC Concept

13537/09 CNO Ops

11702/08 MIL CIS

6630/05 INFO SEC

(PAGE VIERGE)

Sommaire

Page

(PAGE VIERGE)

Chapitre 1
Définitions et principes généraux

101. La DIA 6 a pour objectif de développer un « référentiel commun » pour la préparation, le déploiement et la mise en œuvre des SIC au profit des états-majors et des forces. Elle décrit les principes d'emploi, en tenant compte des capacités et organisations existantes ou sur le point d'être acquises. Cette doctrine doit répondre aux exigences opérationnelles actuelles ou à venir.

102. Les SIC opérationnels sont une clé de la supériorité opérationnelle des forces armées. Les principaux enjeux des SIC mis en œuvre en opération sont :

a. L'autonomie et la résilience : contribuer à l'autonomie nationale de décision puis d'action, en garantissant une situation informationnelle commune et des liaisons permanentes sur des réseaux stratégiques résilients, donnant l'accès aux informations clé, en garantissant leur transmission, leur protection, leur intégrité, leur exploitation et leur diffusion ;

b. L'interopérabilité : permettre le commandement comme nation cadre ou la participation aux opérations interalliées conduites par l'OTAN, l'UE ou une coalition ad hoc, et dans un cadre interministériel ;

c. La maîtrise et la supériorité informationnelle : accroître l'efficacité opérationnelle militaire, en optimisant les capacités propres de maîtrise de l'information à travers une utilisation judicieuse des technologies.

103. Les opérations modernes imposent une uniformité des normes utilisées (autour de l'Internet Protocol notamment), une continuité et un niveau élevé de qualité de service (notion de bout en bout) des SIC depuis les plus hautes autorités militaires jusqu'à l'échelon tactique projeté le plus réduit. Le fonctionnement des SIC opérationnels doit être simple, efficace et résilient. Il doit être assuré dans des environnements hostiles et sous forte menace cybernétique.

104. Le domaine SIC recouvre l'ensemble des fonctions nécessaires à :

a. la conception des architectures SIC, découlant de l'organisation du commandement (C2) et du besoin en échange d'information ;

b. la réalisation, le déploiement et l'emploi des systèmes d'information et de communication ;

c. le transport, le traitement et le management de l'information ;

d. la sécurité des SIC, qui couvre leur protection et leur défense face aux dysfonctionnements et aux attaques potentielles, notamment les cyber menaces ;

e. leur soutien spécifique.

105. Les systèmes d'information et de communication (SIC) du ministère de la défense **sont classés selon leur objet** et se répartissent comme suit :

a. **Les systèmes d'information opérationnels et de communication (SIOC)** placés sous la responsabilité du **chef d'état-major des armées** ;

b. **Les systèmes d'information scientifiques et techniques (SIST)** placés sous la responsabilité du **délégué général pour l'armement**[4] ;

c. **Les systèmes d'information, d'administration et de gestion (SIAG)** placés sous la responsabilité du **secrétaire général pour l'administration**.

Section I − Définitions des termes et concepts

106. Un SIC, Système d'Information et de Communication, est un système intégré d'appui au commandement destiné à fournir dans les délais requis aux autorités et à leurs états-majors les données nécessaires à la planification, à la conduite et au contrôle de leurs activités. Le SIC intègre le personnel, les équipements, l'organisation, les procédures, les liaisons et les éléments de doctrine (définition DC-004 Glossaire Interarmées de Terminologie Opérationnelle de 2013). Au sein des SIC, on distingue :

a. Les SC, Systèmes de Communication (ou *Communication Systems)*, qui sont l'ensemble de matériels, de méthodes et de procédures, et le cas échéant de personnes, organisé pour accomplir des fonctions de **transfert d'informations** (cf. *AAP 31 (2010)) ;* l'*AJP*-6 précise :

(1) un système de communication établit une communication entre ses utilisateurs et englobe notamment les systèmes de transmission, les commutateurs et systèmes utilisateur ;

(2) un système de communication peut également inclure des fonctions de traitement et de stockage dans le cadre du transfert de l'information.

b. Les SI, Systèmes d'Information (Information Systems), qui sont l'ensemble de matériels, de méthodes, de procédures et, le cas échéant, de personnes, organisé pour accomplir des fonctions déterminées de traitement d'informations (cf. AAP-31 (2010))[5.]

107. La distinction SC / SI tend aujourd'hui à s'effacer ; certains équipements modernes combinent en effet les deux fonctions. Certaines radio modernes, par exemple, à l'instar des Smartphone dont la vocation n'est plus uniquement le transfert d'information mais également son traitement, permettent à la fois de transmettre de l'information sous différents modes (phonie, data, flux vidéo), en modes claires ou sécurisés, UHF/VHF/ satellitaire, mais également de se connecter à des réseaux de données tactiques, tout en échangeant les positions de forces via des serveurs de données.

Systèmes de communication (SC)

108. Les systèmes de communication (SC) (systèmes filaires, satellitaires, hertziens et radioélectriques, de commutation et de desserte…), transportent les flux d'informations sous forme analogique ou numérique et regroupent les installations, réseaux et services de télécommunications, fixes ou mobiles, permanents ou temporaires. Un système de communication organise et fédère les moyens de communication et rassemble trois éléments, s'appuyant sur un ensemble de matériels, de méthodes et de procédures, et le cas échéant de personnes, organisées pour accomplir des fonctions de transfert d'informations, permettant ainsi de transmettre l'information entre les utilisateurs:

a. Le support qui réalise effectivement le transport.

b. Le routage, qui oriente vers le bon destinataire.

---

[4] Les SIST, principalement mis en œuvre par la DGA, sont exclus du périmètre de la DIA 6.

[5] La DIA 3.40 Cyber, définit un SI comme, un ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) permettant de **collecter, stocker, traiter et diffuser de l'information**. Dans le cadre de la cyberdéfense, cette définition regroupe tous les systèmes dont le fonctionnement fait appel à des composants informatiques : les systèmes d'information et de communication (SIC), les moyens de télécommunication, les outils informatiques, les systèmes embarqués, la plupart des systèmes d'armes ou de combat, les systèmes d'accès et de gestion technique des bâtiments et les systèmes d'information industriels (dont les Automates programmables industriels (API), les Systèmes numériques de contrôle-commande (SNCC) et les logiciels de supervision et de contrôle *SCADA / Supervisory Control And Data Acquisition* ou Système de contrôle et d'acquisition de données*).*

c. La desserte au profit de l'utilisateur final.

109. Les systèmes de communication regroupent les installations, réseaux support et services de télécommunications, fixes ou mobiles, permanents ou temporaires. Ils permettent les échanges entre les systèmes d'information et délivrent également des services de communication du type :

a. Téléphonie claire et sécurisée.

b. Télécopie claire et sécurisée.

c. Visioconférence claire et sécurisée.

d. Télégraphie claire et sécurisée.

e. Transmissions de données claires et sécurisées (services collaboratifs, vidéo…).

Systèmes d'information (SI):

110. Des systèmes d'information (SI) assurent une fonction de traitement de l'information. Ceux-ci sont dits opérationnels (Système d'information opérationnel et de communication des armées - SIOC) lorsqu'ils sont utilisés à des fins immédiates de combat, logistiques[6] ou d'administration et de gestion (SIAG[7]) lorsqu'ils sont employés pour l'administration courante des forces (ressources humaines, finances, etc.…) y compris lorsqu'ils sont déployés en opération.

111. Un système d'information traite et organise l'information pour délivrer un service (cartographie, messagerie, etc..). Il a ainsi pour fonction en s'appuyant sur un ensemble de matériels, de méthodes, de procédures et, le cas échéant, de personnes, organisé pour accomplir des fonctions déterminées de traitement d'informations, de générer, stocker, traiter, organiser, diffuser et présenter les informations qui lui sont confiées pour remplir un service.

112. Le développement et la mise en œuvre d'un système d'information englobent :

a. Les métiers et processus associés.

b. Les aspects fonctionnels (services à rendre).

c. Les programmes et les applications supportées.

d. Les architectures techniques (réseaux et composants, postes de travail, supports physiques et technologies), qui permettent l'accès ou la gestion de l'ensemble des données ou informations accédées, détenues ou fournies par l'organisation bénéficiaire.

113. Les systèmes d'information opérationnels concourent notamment à :

a. L'exercice du commandement.

b. L'appréciation autonome de situation.

c. La planification, la programmation et la conduite des opérations en mode collaboratif.

d. La mise en réseau des systèmes d'armes.

e. La logistique.

f. L'emploi des systèmes « expert ».

---

6 Les Systèmes d'Information Logistique sont des systèmes d'information opérationnels contribuant aux opérations dans le cadre de la fonction logistique.

7 Les SIL sont classés entre SIAG ou SIOC, suivant le type d'informations qu'ils utilisent.

114. Les Systèmes d'Information sont généralement déployés en réseaux. On distingue ici les réseaux étendus / wide area network (WAN) et les réseaux locaux / local area network (LAN).

a. Le *LAN* d'un Poste de Commandement (PC) ou module de PC, d'un bâtiment ou d'une entité : il est constitué de l'ensemble des moyens connectés, dans une aire géographique réduite, sur un même réseau physique et partageant la même information. Le *LAN* permet notamment l'échange d'information à l'intérieur d'un centre opérations (CO).

b. Le *WAN* est constitué par l'interconnexion de l'ensemble des *LAN* via le réseau de théâtre. L'ensemble des *LAN*[8] d'un niveau de commandement donné constitue le *WAN* de ce niveau (par exemple, le *WAN* division). Le *WAN* intègre les détachements de liaison envoyés auprès d'autres PC ou entités. L'ensemble des *WAN* peut être connecté et constituer le *WAN* de théâtre (par exemple, *NSWAN* ou *NATO Secret Wan*). Le *WAN* permet la circulation de l'information sur de grandes élongations, voire sur l'ensemble du théâtre et répond ainsi aux contraintes de lacunarité.

Cybersécurité

115. La cybersécurité est l'état recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles[9].

116. Compte-tenu du lien étroit entre la cybersécurité et les SIC, le chapitre 5 de la DIA 6 y est dédié.

Liaison

117. La liaison (au sens des SIC) est le contact établi au moyen de systèmes de communication entre éléments appartenant à un même ensemble de forces, facilitant une compréhension mutuelle et une unicité de buts et d'actions. Elle est un moyen permettant à un élément d'une force de communiquer avec l'échelon supérieur, les échelons subordonnés, les autres éléments de la force, voire des éléments extérieurs à la force ; elle peut être renforcée par l'échange de personnel et des capacités de « *reach-back* »[10] avec les entités parents.

Services

118. Les services (« functional » ou « core services » en terminologie de l'OTAN) sont déclinés principalement sous forme d'outils logiciels d'un système d'information. Ils permettent les échanges de données entre les utilisateurs dans les domaines fonctionnels identifiés (informations, opérationnelles, logistiques[11] ou générales, outils métiers spécifiques, portails, phonie, messageries…). La description précise des services est un élément clé de la définition des moyens SIC nécessaires, dans la mesure où ces services nécessitent une mise en place plus ou moins complexe sur les systèmes déployés.

Informatique en nuage

119. Couramment mise en avant dans le secteur privé et chez nos alliés, l'informatique en nuage « cloud computing » occupe une place croissante dans le paysage global des systèmes d'information et de communication (SIC). Ce nouveau concept consiste à découpler l'usage des SI des problématiques techniques (bases de données, stockage, archivage, maintenance à distance…) qui sont réalisées à travers le « cloud ». L'usager n'a plus alors à se soucier du « cloud » qui est sous la responsabilité (architecture, gestion, maintenance…) d'une autorité technique dédiée. Ce concept permet de minimiser le soutien de proximité, tout en améliorant le service rendu et faciliter l'usage terminal. Il nécessite en revanche une garantie de la qualité des services informatiques ainsi proposés.

---

8 La notion de « *LAN* étendu » s'apparente au concept technique du *WAN* mais vu de l'utilisateur, il se comporte comme un *LAN*.

9 Cf. « Stratégie de la France dans le domaine de la défense de la sécurité des systèmes d'informations »

10 «En soutien arrière », généralement depuis l'entité en base arrière, en métropole.

11 Sans être directement liées à des outils d'information du commandement, ces informations logistiques sont aujourd'hui vitales au maintien de l'activité opérationnelle de nombreux systèmes opérationnels (ex : AMASYS/HARPAGON pour les RAFALE, CINDY/TAURUS pour le HARFANG, REAPER, …).

120. Le ministère s'est engagé dans la voie de la rationalisation de l'hébergement au travers du projet INCAS (Infrastructure Communicante Adaptative et Sécurisée). La typologie des sites et la topologie des réseaux sont désormais définies en fonction de critères géographiques et opérationnels, et non plus en fonction de l'organisation des armées, directions et services.

121. Les acteurs engagés sur les théâtres d'opération doivent disposer d'un accès d'une grande fiabilité à l'espace des informations opérationnelles, à travers leurs systèmes d'information nationaux ou multinationaux, connectés à un cloud dit de théâtre, malgré les contraintes que constituent :

a. La nécessité de pouvoir déployer et adapter des architectures SIC partout dans le monde avec un très faible préavis.

b. La mobilité des acteurs opérationnels et la multiplicité de leurs équipements d'accès au SI.

c. La limitation de bande passante et la latence liée à l'utilisation quasi exclusive de supports de communications satellitaires.

d. Le besoin de fonctionnement en mode déconnecté.

122. La mise en œuvre de cette politique est d'ores et déjà une réalité au travers du déploiement du socle technique commun interarmées (STCIA) et l'irrigation des outils de travail collaboratif qu'il propose au plus bas niveau tactique. La notion de Cloud de théâtre prendra une nouvelle dimension avec le déploiement prochain du système d'informations des armées (SIA).

Section II − Principes de mise en œuvre des SIC en opération

123. L'élaboration d'une architecture SIC opérationnelle et sa mise en œuvre doivent respecter les principes suivants ; leur niveau d'exigence est précisé pour chaque opération et leur mise en œuvre est réalisée soit de façon native pour les équipements, soit à travers une architecture, une organisation ou des procédures spécifiques.

124. **Une mise en réseau adaptée au « juste besoin »** : les acteurs opérationnels bénéficient d'une connectivité adaptée à leurs besoins. La capillarité des SIC doit permettre d'irriguer jusqu'au plus petit élément tactique sur le théâtre en fonction du moment, de la situation et des besoins, assurant ainsi une fluidité de l'échange d'informations entre tous les niveaux déployés.

125. **Du haut vers le bas** : il appartient à l'échelon de commandement supérieur de raccorder ses échelons subordonnés à travers la mise en place de SIC adaptés à la mission. Ce principe cardinal des architectures SIC évolue cependant actuellement sous l'égide de l'OTAN vers une notion de fédération de réseaux à l'aune des récents déploiements en coalition, mais restera central. Le concept de fédération repose sur l'idée que le haut propose des solutions d'interconnexion au bas, fondées sur des prérequis techniques et de classification.

126. **Bout en bout** : il s'agit de pouvoir garantir la continuité des flux d'information depuis l'échelon tactique élémentaire le plus bas jusqu'à l'échelon stratégique de décision au niveau national, en déployant une architecture générale permettant de relier tous les échelons. Ce principe impose des échanges entre les réseaux projetés et les réseaux d'infrastructure de la métropole, l'interconnexion des réseaux des composantes à chaque fois que possible (compatibilité SSI) ainsi que des passerelles entre les réseaux dont les niveaux de confidentialité peuvent être différents, tout en garantissant au commandant d'un théâtre la maîtrise de sa manœuvre SIC. Cette recherche de connectivité globale vise ainsi à un meilleur partage interarmées des données d'une situation opérationnelle.

127. **Interopérabilité :** c'est la capacité de plusieurs systèmes, unités ou organismes à opérer ensemble grâce à la compatibilité de leurs organisations, doctrines, procédures, équipements et relations respectives. L'interopérabilité technique se traduit par la mise en place de procédures opérationnelles, l'application de standards techniques et la mise en place de passerelles pour l'interconnexion des systèmes.

128. **Fiabilité** : les SIC doivent avoir une architecture garantissant un niveau de fiabilité permanent au commandement, pour les échanges d'information de toute nature dont il a besoin. Ce niveau de fiabilité doit être défini entre le commandement et le X6 du niveau concerné afin d'en déduire les moyens indispensables à déployer pour obtenir la fiabilité requise.

129. **Sécurité** : la sécurité des systèmes d'information comprend les politiques et les mesures réglementaires nationales prises pour protéger les SIC ainsi que l'intégrité, la disponibilité et la confidentialité des informations ainsi échangées. En coalition, le concept d'*INFOSEC (Information Security)* se base sur l'application d'un ensemble de mesures de sécurité logique et physique[12] définies notamment par l'OTAN[13] ou l'UE[14].

130. **Confidentialité** : les SIC doivent garantir de bout en bout le niveau de confidentialité requis pour l'information échangée selon les directives reçues du commandement. Cette confidentialité repose sur la mise en œuvre de moyens de chiffrement, de procédures de sécurité et d'accès contrôlé à ces informations, conformément à l'IGI 1300 pour les SIC nationaux.

131. **Intégrité** : l'information transmise ne doit pas être modifiée ou altérée d'une façon non autorisée. Elle ne peut être modifiée que par les personnes en ayant le droit et de façon volontaire.

132. **Disponibilité** : l'information doit être mise à disposition dans des conditions définies d'horaires, de délais et de performances du système qui la délivre.

133. **Redondance** : l'architecture SIC déployée doit dès sa conception et son déploiement, être suffisamment redondante pour pouvoir pallier les incidents techniques ou opérationnels affectant les moyens mis en œuvre : plans de secours, constitution de réserve d'équipements, capacité de projection d'éléments de maintenance et de personnel pour pallier les difficultés rencontrées…

134. **Résilience**[15] : la résilience des systèmes SIC est la capacité globale de l'organisation retenue à pouvoir réagir en cas de difficultés majeures et à continuer à agir efficacement en dépit d'un environnement dégradé. Les systèmes d'information ou de communication doivent ainsi être capable de résister à une panne ou à une attaque afin de minimiser l'impact opérationnel ainsi qu'à recouvrer une efficacité opérationnelle minimale après l'incident. La résilience des SIC nécessite la définition de plans de continuité et de plans de reprise d'activité (PCA/PRA), permettant la continuité de service en cas de problèmes. Le niveau de résilience doit être défini en amont entre le commandement et les responsables SIC.

135. **Réactivité** : le tempo des opérations conditionne la manœuvre des SIC. L'architecture déployée doit répondre à cet impératif de réactivité.

136. **Mobilité** : les SIC opérationnels doivent contribuer à la mobilité des forces projetées grâce au déploiement de dispositifs SIC mobiles capables d'accompagner la force en mouvement et de maintenir la permanence de la liaison.

137. **Agilité** : la garantie et l'optimisation des débits reposent sur une gestion dynamique des flux et de la bande passante. Des priorités sont accordées en fonction de la conduite des opérations. Ces priorités sont définies conjointement par le commandement et la chaîne SIC. Elles peuvent varier dans le temps et dans l'espace**.**

Section III − Les outils et services mis à la disposition du commandement

138. Outre les outils traditionnels (phonie, graphie, messagerie ACP 127,…), on identifie désormais de nouveaux services d'usage courant en opération. Le développement de ces outils s'inscrit dans l'utilisation croissante des pratiques issues du monde Internet. Ils doivent également permettre l'archivage et la traçabilité de tous les échanges et données opérationnelles.

---

12 Les mesures INFOSEC plus techniques sont réparties en deux familles : la sécurité informatique (*Computer Security - COMPUSEC*) et la sécurité des communications (*Communication Security –COMSEC*).

13 La sécurité **physique** (sous la responsabilité du *Headquarters Security Officer - HQSO*) pour le contrôle physique des accès, protection des installations… ; la sécurité **personnel** (sous la responsabilité de l'officier de contrôle COSMIC) pour les habilitations OTAN /FR, réglementations… ; la sécurité des **documents** (sous la responsabilité de l'*Information Control Officer - ICO*) ; la sécurité des **réseaux** (sous la responsabilité de l'*Information Security Officer - InfoSec Officer*), pour l'application des règles SSI et LID 5lutte Informatique Défensive).

14 Les principes de l'*INFOSEC* de l'UE sont dérivés de ceux de l'OTAN.

15 Concept exploratoire interarmées CEIA-3.37_résilience(2011) n°202/DEF/CICDE/NP du 13.12.11

Le portail Web opérationnel

139. L'emploi de portails[16] type web est désormais d'usage courant dans la conduite des opérations. Il permet la mise à disposition de fichiers stockés et accessibles à partir d'une page d'accueil. Pour une force déployée, la publication sur les pages d'un portail Web opérationnel doit obligatoirement répondre au triptyque : modérateur – nombre et nature des destinataires – besoin opérationnel. Le modérateur d'une page d'un portail Web opérationnel est responsable de l'information qu'il publie. Il veille à utiliser un lien vers la source pour une information dont il n'est pas l'origine.

140. Trois types de pages sont disponibles sur un portail Web opérationnel :

a. Page de conduite *top down* : elle comprend les ordres et les directives, l'historique de l'action (*log book*) et les liens importants vers d'autres portails.

b. Pages *bottom up* de situation : ce type de pages permet à une unité de rendre compte de sa disponibilité ou des tâches qui lui ont été déléguées.

c. Pages *info* d'information : elles comprennent les annuaires, la documentation permanente ou quasi-permanente ou des liens vers des sites référents.

Le courrier électronique

141. L'échange de courrier électronique est un des services les plus couramment utilisés, avec une gamme de possibilités très complètes. Les destinataires peuvent être répertoriés soit par des adresses nominatives, soit par des adresses fonctionnelles. La taille des pièces jointes peut cependant être limitée en fonction des caractéristiques du réseau utilisé et des responsabilités des utilisateurs. Il revient à l'utilisateur de vérifier l'adéquation entre le niveau de confidentialité de son document, la protection des réseaux utilisés et le besoin d'en connaître des destinataires.

La Visioconférence (VTC), le Full Motion Video (FMV)

142. L'emploi de la visioconférence permet de :

a. Discuter entre entités distantes en voyant ses interlocuteurs en temps réel avec la possibilité de visualisation simultanée des documents.

b. Visionner et/ou diffuser en temps réel ou réduit, des séquences images issues de différents capteurs (drones, pods aéroportés...) utiles et/ou nécessaires à la conduite d'une opération…

143. Ce type d'outil nécessite une fiabilité exigeante de la liaison, avec une bande passante importante pour le transfert de vidéo en temps réel.

144. Le terme anglais de Full Motion Video (FMV) est aussi utilisé, par extension, pour décrire une capacité de diffusion, de rejeu et de stockage de la vidéo de systèmes de combat (drone, aéronef, véhicule, frégate…), comprenant également les serveurs et systèmes associés ainsi que les standards et mécanismes d'échanges (ajout de métadonnées[17] permettant l'exploitation ultérieure des images).

Les messageries instantanées (« *chat*[18] »)

145. Une messagerie instantanée est un moyen de commandement et de conduite d'une force. Elle peut être mise en place sur des supports radioélectriques classiques (V/UHF ou HF) ou sur des moyens IP classiques. Lorsque toutes les composantes d'une force interarmées en sont dotées et lorsque les élongations ou la situation tactique en justifient l'usage, le « chat » est utilisé de façon préférentielle en place et lieu des moyens « classiques » de conduite, comme la messagerie ACP 127, sous réserve d'une capacité de contrôle de l'identification des

---

16 Le Portail des Opérations Interarmée (POIA) en est un exemple. Le CPCO est directeur du POIA, les services et serveurs étant soutenus par la DIRISI IdF.

17 Une métadonnée est une donnée numérique enrichie permettant de décrire une donnée enregistrée précédemment (ex. : photo géo-référencée).

18 L'équivalent français du terme « *chat* » est le néologisme « clavardage ».

intervenants sur ce *chat*. Il peut dans certains cas, se substituer ou compléter un réseau tactique.

146. On privilégiera les discussions au sein de « salons » thématiques « *chatrooms* », afin de permettre une consultation de l'historique par tout nouveau venu ; les salons permettent les discussions en aparté entre les participants pour préciser certains points. Le nombre et les rôles des salons sont de la responsabilité du commandement. Leur mise en place et leur utilisation[19] supervisées par un modérateur, sont formalisées au sein d'une directive d'emploi.

147. Le niveau de protection des informations qui circulent sur un « chat » est du niveau de protection du système qui l'héberge en tenant compte des capacités d'interconnexion des réseaux de responsabilité différentes. Le « *chat* » se décline pour une opération ou un exercice donné en salons de « *chat* » *(«chatrooms*») dédiés chacun à un domaine ou à un processus (« *targeting* », manœuvre ou management de l'information…).

Section IV − Les SIC d'états-majors en opération

148. Les SIC opérationnels s'intègrent dans les structures d'état-major. Les principes énoncés ci-dessous en précisent l'organisation générale. Afin d'appuyer les opérations qu'il planifie et conduit, tout état-major doit comprendre une fonction SIC complète et solide :

a. **Les SIC :** La fonction SIC intègre le personnel, les équipements, l'organisation, les procédures, les liaisons et les éléments de doctrine. Elle fournit aux autorités et à leurs états-majors les données nécessaires, dans les délais requis, pour planifier, conduire et contrôler leurs activités. Les SIC sont articulés en 4 sous-fonctions :

(1) Le commandement des SIC.

(2) Les Systèmes de Communication (SC).

(3) Les Systèmes d'Information (SI).

(4) Le Soutien Spécialisé de Quartier Général (SSQG), qui fournit l'appui nécessaire à la vie quotidienne et au bon fonctionnement des SIC de l'état-major ; il assure notamment le déploiement technique des SIC, la production d'énergie électrique, le filtrage et la sécurité des ZPC selon les normes retenues. Le juste dimensionnement du SSQG[20] est indispensable pour permettre aux SIC de pouvoir travailler de façon optimum, dans la durée, au profit des EM soutenus.

b. La Cyberprotection[21](cf. Chapitre 5 - Section II).

Section V − Management de l'information

149. L'augmentation exponentielle du volume des informations traitées impose un management de l'information performant.

150. « Le management de l'information est une fonction relevant du commandement et qui consiste à orienter et appuyer le traitement de l'information durant son cycle de vie afin de fournir une information exacte, d'une qualité suffisante, sous la forme voulue et dans les délais requis pour répondre aux besoins d'un état-major » (*the NATO information management policy*, 2007, *NATO/PFP Unclassified*). Le management de l'information consiste donc à aider au recueil

---

19 **Modérateur de l'information - directeur de réseaux/circuits** : Le modérateur de l'information (ou directeur de réseaux/circuits) est l'unité désignée par le commandement pour un moyen donné (*chatroom*, portail ou page *Web*, circuit radio…). Il est le responsable de la mise à disposition ou de la transmission des informations sur les systèmes supports. Au sein de l'unité il est responsable de la direction du moyen qu'il dirige et dont il assure le fonctionnement. Sur un circuit de phonie, cette fonction est assurée par le directeur de réseau.

20 Le SQG de chaque **état-major terrestre** déployé s'articule en 4 sous-fonctions : le commandement du SQG, le SSQG (soutien spécialisé de quartier général), le SVLQG (soutien vie et logistique de quartier général), la protection de PC. Les deux composantes SIC et SQG sont regroupées dans la fonction appui au commandement. **Pour la composante aérienne**, le CMO SIC est constitué de l'ensemble des Escadrons SIC Aéro (ESICAéro) de théâtre (renforcés en tant que de besoin par du personnel DIRISI) chargés du soutien de tous les systèmes spécifiques Air ; le soutien porte aussi bien sur les postes clients spécifiques que sur les radar, en passant par tous les postes et réseaux déployés dans la « bulle Air », c'est-à-dire sur tout le dispositif Air raccordé derrière l'antenne satellitaire reliant à la métropole, y compris ce moyen. **Pour la composante maritime**, l'état-major embarqué bénéficie du soutien fourni sur le bâtiment ; un renforcement temporaire ou un complément d'armement peuvent être alors demandés pour assurer le service courant à bord.

21 Cyberprotection (Sécurité des systèmes d'information - SSI) : ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, et des services que ces systèmes offrent ou qu'ils rendent accessibles (Cf. DIA-3.40_Cyber).

(*collecting*) et à la mise en forme de l'information, à son stockage (*storing*) sur les supports adéquats, afin de la rendre disponible (*displaying*) ou de la transmettre (*disseminating*) selon les règles de sécurité en vigueur et dans le respect du besoin d'en connaître.

151. Afin d'élaborer une architecture SIC opérationnelle, il convient, entre autres, d'identifier la nature des informations véhiculées et de fixer les responsabilités des différents intervenants dans les processus de diffusion puis de les hiérarchiser et d'en définir l'emploi.

152. Pour cela, on distingue deux types d'information :

a. **L'information opérationnelle** : c'est l'information nécessaire à la conduite de mission (*Mission Critical Information* : *MCI*). Elle se décline sous forme verbale (réseau de phonie, téléphonie *IP*, LDT,…), écrite (messagerie, portail *Web*, *chat*), ou sous forme d'actions codées (*LDT*, *AdatP 3*, *Gold*, ….), ou encore visuelle (vidéo, FMV, GHOM,[22]..). Cette information est au cœur des SIC et en impose l'architecture et l'emploi.

b. **L'information générale** : elle englobe l'ensemble des informations non opérationnelles, (non nécessaires dans l'immédiat pour l'accomplissement de la mission).

153. Le Management de l'Information (*Info management*) passe par la mise en place d'une organisation, de personnel, de procédures adaptées et d'outils techniques simples permettant de transmettre les données et de les organiser en vue de les transformer en informations utiles.

154. Le management de l'information est effectué au sein de Cellules de Management de l'Information (CMI), ou également appelées cellules *Information and Knowledge Management* (*IKM*), en coordination avec les utilisateurs opérationnels des systèmes déployés, les administrateurs des systèmes d'information utilisés et appuyé par les personnels SIC en charge des services ou systèmes d'information utilisés.

155. Au sein d'un état-major, la Cellule Management de l'Information (CMI) œuvre au profit des utilisateurs, avec le soutien des SIC. Aux ordres du Chef d'état-major (CEM ou *Chief of Staff - COS*), le responsable du management de l'information (*Info Manager Officer - IMO*) contribue directement à la bonne circulation de l'information tant interne qu'externe et donc à l'efficacité opérationnelle de l'entité concernée. Il doit maîtriser à la fois les capacités offertes par les SIC, l'architecture du C2, mais avant tout le fonctionnement de l'état-major, ses processus et le format des informations opérationnelles. En particulier, l'*IMO* doit connaitre les services ou applications déployés au sein de l'état-major et est en contact permanent avec le X6, le CEM et le CO.

156. Si le management de l'information est désormais une réalité concrète, deux étapes supplémentaires se profilent autour de l'information et auront très vite un impact sur la conduite des SIC en opération :

a. **L'info-valorisation** : qui consiste, à travers une organisation, du personnel et des procédures, à valoriser les informations transmises par un traitement plus élaboré, permettant ainsi d'apporter au commandement une vision la plus complète et la plus pertinente possible de la situation. L'information nécessaire arrive au bon endroit, au bon moment.

b. **L'opération infocentrée** : qui consiste à donner à l'information un caractère central de l'action, notamment dans le cadre de l'approche globale. L'information précédemment valorisée est alors disponible sans délais, accessible et organisée pour répondre à l'ensemble des besoins des forces durant toutes les phases d'une opération et selon le principe du besoin d'en connaître.

157. Dans le concept d'opération infocentrée, toutes les plateformes, les systèmes d'arme, jusqu'au combattant individuel, participent ainsi aux échanges d'informations et de données, en totale transparence et fluidité sur le plan de l'intégration technique. Chaque entité est à la fois capteur, émetteur et producteur d'informations partageables. L'ensemble des forces est interconnecté, permettant la diffusion des informations. Les entités se raccordent selon le principe du « *plug*

[22] Données Géographie, hydrographie, océanographie et météorologie,

and play ». La dominance informationnelle (*Information dominance*) ainsi acquise confère un avantage militaire décisif sur l'adversaire.

Chapitre 2
Les SIC des armées

La connaissance des SIC des armées est aujourd'hui nécessaire pour comprendre les architectures des systèmes déployés, les services qui sont fournis ainsi que l'optimisation de leur emploi. Ce chapitre présente les principaux SIC dans un cadre d'emploi interarmées.

201. Les SIC mis en œuvre par les armées comprennent des SIC permanents d'infrastructure et des SIC mobiles ou déployables. Ils permettent la mise en place de réseaux de natures diverses afin de répondre aux besoins des forces.

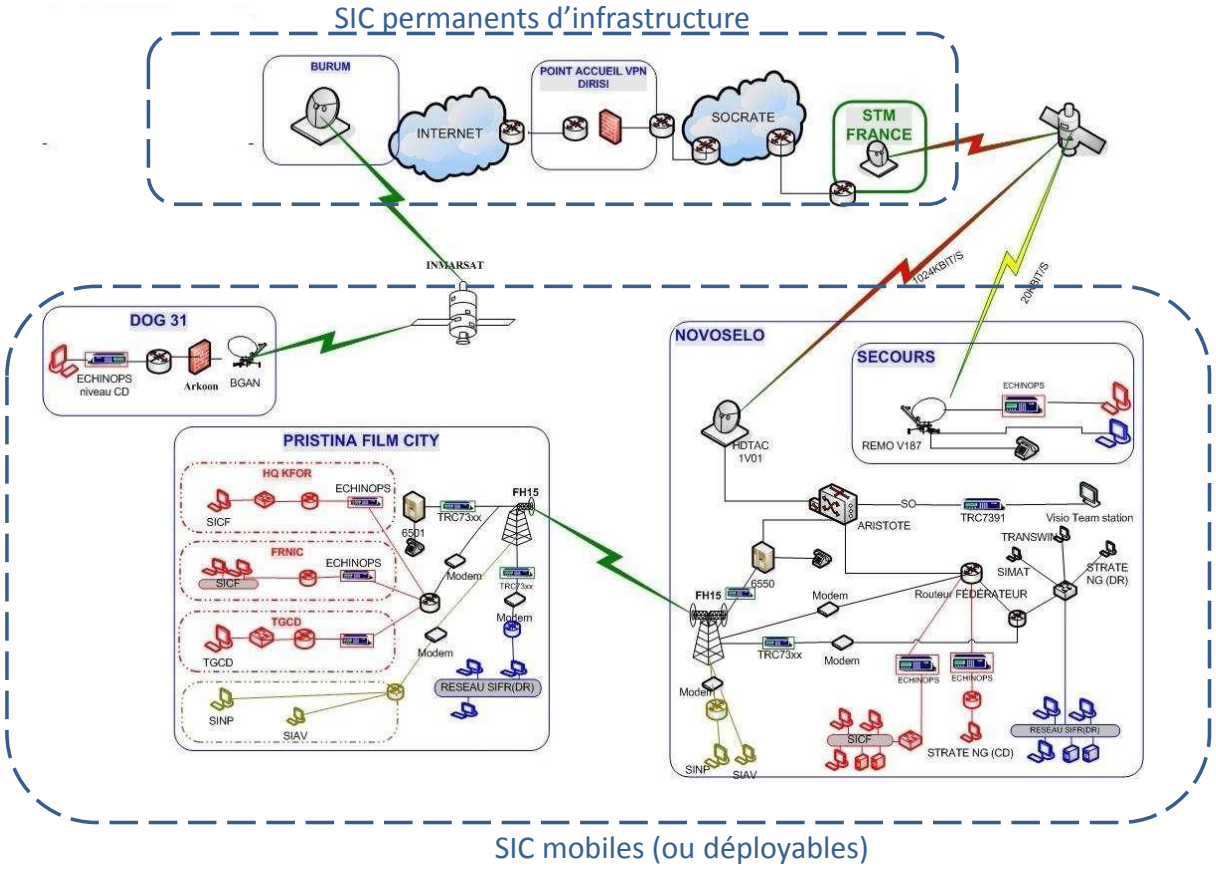

FIG. 1. – *Exemple d'une architecture SIC en opérations.*

Section I − Les SIC des niveaux stratégiques et opératifs

Réseaux d'infrastructure

202. Le système de communication SOCRATE[23], complété par les réseaux de desserte des armées, raccorde toutes les implantations, unités des armées et des services ainsi que de nombreux organismes du ministère. Il fournit les supports de communication en métropole. Réseau privatif de la Défense, conçu dans les années quatre-vingt-dix pour offrir une résistance importante aux menaces du moment, il satisfait les besoins opérationnels les plus variés[24] et les plus contraignants, tout en accueillant également les communications aujourd'hui qualifiées d'usage

[23] Système Opérationnel Constitué des Réseaux des Armées pour les Télécommunications.
[24] Selon les cas, des liens *Virtual Private Network (VPN)* peuvent être mis en place au profit d'une force à partir d'un lien satellitaire civil ou par Internet.

général (téléphonie, transport des flux de données,…). Réseau métropolitain à l'empreinte très vaste, conçu comme un noyau de communications indépendant de la société civile, il a vocation à résister à des agressions sévères sur le territoire national et à maintenir l'ensemble de ses services en cas de crise intérieure généralisée.

203. SOCRATE est opéré par la DIRISI au profit des armées et des services, via le CMO Réseaux implanté à Maisons-Laffitte.

204. DESCARTES, successeur de SOCRATE, doit fournir à partir de 2017 les réseaux du ministère de la défense pour son cœur résilient (cœur stratégique et besoins opérationnels des forces armées en tout temps) et pour l'ensemble des emprises du ministère, un réseau d'usage général pour le fonctionnement courant[25]. Il interconnectera la métropole et les DROM-COM[26]. Ces programmes sont complétés par des projets de desserte[27].

Réseaux satellitaires

205. Les liaisons par satellites sont principalement utilisées pour réaliser les transferts d'information à grande distance, voire intercontinentales entre le territoire national (métropole et outre-mer), les théâtres d'opérations extérieures, et les bâtiments de la Marine nationale. Elles sont également employées par une force déployée sur un terrain compartimenté par des masques empêchant les liaisons directes (par exemple, zones montagneuses, urbaines…) ou sur un théâtre étendu (grandes élongations entre unités du dispositif) ; elles équipent également certains aéronefs. Ces liaisons offrent la possibilité de transmettre tous les types d'informations possibles : voix, données, images fixes et vidéo…

206. Un système de communication par satellite se compose d'un segment spatial comportant des satellites et d'un segment sol (naval, terrestre, aérien) comportant des stations fixes (Favières et France-Sud pour Syracuse III) et des stations mobiles ou déployables. Les stations fixes acheminent l'ensemble du trafic et assurent l'interconnexion des abonnés du système aux différents réseaux de télécommunications militaires et civils. La capacité de communication par satellites offre donc :

a. Des communications indépendantes de la topographie ou des élongations, peu sensibles aux conditions météorologiques[28] et qui permettent de couvrir des espaces lacunaires.

b. Une mise en réseau flexible entre des éléments de nature différente (bâtiments à la mer, bases aériennes projetables, SGTIA, états-majors) et un lien direct vers la destination finale permettant de s'affranchir de déploiements tactiques de relais radio.

c. Une couverture et une disponibilité permettant la circulation montante et descendante des flux d'informations.

207. L'emploi des réseaux satellitaires est supervisé par la DIRISI, sous l'autorité de l'EMA, via le Centre national de mise en œuvre des moyens satellites (CNMO MS) implanté à Maisons-Laffitte.

Le réseau satellitaire SYRACUSE

208. Le système SYRACUSE III met en œuvre 3 satellites de télécommunications en orbite géostationnaire (SYRACUSE 3A, SYRACUSE 3B et SICRAL 2). Le contrôle technique et la gestion sont assurés par le CNMO MS de Maisons-Laffitte.

209. Le système SYRACUSE III fournit des liaisons protégées et durcies face à une agression électromagnétique, couvrant l'essentiel des besoins du C2. Les satellites peuvent assurer une couverture globale, ainsi que des couvertures mobiles régionales et de théâtre, en fonction des besoins opérationnels. Il est complété et partiellement secouru par le satellite franco-italien SICRAL 2 (bande X) et ATHENA – FIDUS (bande Ka).

---

25 Les services suivants seront assurés par DESCARTES : Transport *IP* de bout en bout, téléphonie d'usage général, télécopie d'usage général, transit intersites au profit du contrôle aérien, supervision. Les sites d'usage général ayant un lien avec l'opérationnel bénéficieront d'une capacité limitée SATCOM pour rester connectés aux sites du cœur stratégique (sites dits « noyau dur »). A partir de 2018, le transport des données et de la téléphonie pour l'usage général pour le ministère se fera sur le réseau interministériel de l'Etat (RIE).

26 Départements et Régions d'Outre-mer, Collectivités d'Outre-mer.

27 Réseaux de dessertes *IP* des emprises aériennes (RD*IP*) et la Modernisation des Dessertes *IP* (MODIP) pour le reste des emprises.

28 La météo peut cependant altérer les performances des liaisons satellitaires avec, par exemple, les masques de pluie ou de sable.

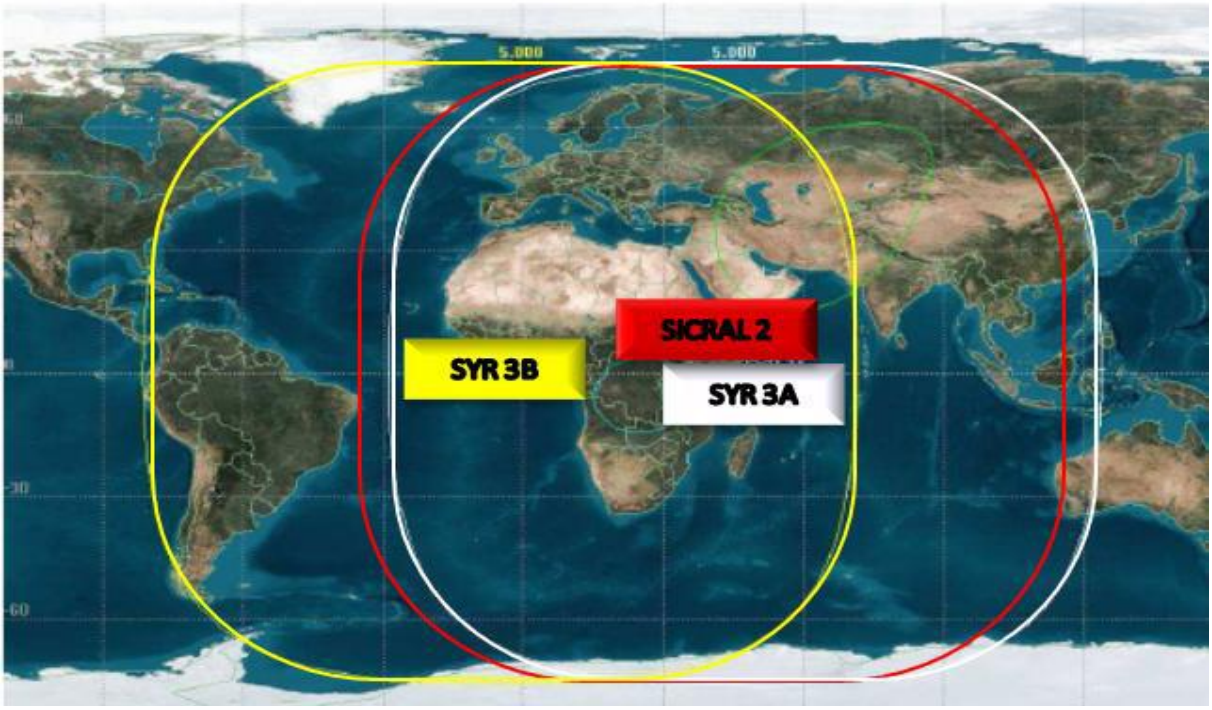

FIG. 2. – *Couverture satellitaire Syracuse III.*

210. Le système SYRACUSE III permet la mise en œuvre de trois types de réseaux, à partir des deux satellites A[29] et B[30], complétés du satellite franco-italien SICRAL 2[31] :

a. Le réseau de transit (RTRAN) constitue le cœur du système Syracuse. Il offre des liaisons point à point protégées contre le brouillage. Ce réseau fédérateur a une capacité dite « durcie ».

b. Le réseau de mobiles (REMO) est rattaché au RTRAN. Il est capable de livrer des services phonie et data à bas débits, jusqu'aux plus bas échelons tactiques en s'appuyant sur des stations satellitaires mobiles comme le VAB VENUS, les stations portables (P) et les valises (V). L'utilisation de ce réseau, dont la ressource est allouée dynamiquement, permet d'offrir un service bas débit à un nombre élevé d'utilisateurs (taux de contention).

c. Le réseau de diffusion (RDIFF) est un véritable complément du RTRAN. Utilisant la technologie « tout *IP* », il est capable de diffuser simultanément la même information à toutes les stations raccordées sous la même couverture (technique VSAT). Caractérisé par des forts débits dans le sens métropole vers les théâtres d'opérations, il permet d'économiser la bande passante allouée au RTRAN en le délestant d'un certain nombre de flux. Ce réseau, qui nécessite des modules additionnels pour certaines stations sol, n'est pas protégé contre le brouillage. Les services mis en œuvre concernent l'*IP*, la téléphonie et la télégraphie.

211. Le système franco-italien SICRAL 2 vient compléter le réseau Syracuse III en utilisant les mêmes stations. Le contrôle technique du satellite SICRAL 2 est assuré par l'Italie. Il offre une capacité supplémentaire (non durcie) d'une couverture globale et d'une couverture régionale. Il offre également une capacité UHF.

212. Le système ATHENA-FIDUS vient en complément du réseau SYRACUSE 3 et SICRAL et offre une capacité en bande Ka. Cette capacité non durcie est répartie en une couverture régionale et 5 spots de théâtre (1000 km de diamètre). Le système COMCEPT est lié au satellite franco-italien ATHENA-FIDUS. Il repose sur un réseau de topologie étoilée. Il a vocation à délester SYRACUSE en transportant les flux INTRADEF, ELINFO et les flux nécessitant une large

[29] Syracuse 3 A lancé en 2005.
[30] Syracuse 3 B lancé en 2006.
[31] Lancé en 2014 et opérationnel en cours d'année. La capacité SYRACUSE étant de 18 répéteurs SHF de 40MHz (dont trois loués à l'OTAN) et 12 répéteurs EHF de 40MHZ, SICRAL 2 apportera un complément de 5 répéteurs SHF.

bande spectrale (flux vidéo montants et descendants, imagerie). L'architecture réalisera chaque fois que possible la redondance d'une station COMCEPT avec une station SYRACUSE, à des fins de résilience générale des réseaux satellitaires. COMCEPT a également vocation à fournir la redondance du noyau dur du réseau DESCARTES.

Les autres réseaux satellitaires

213. D'autres réseaux satellitaires civils (INMARSAT, IRIDIUM[32], GLOBALSTAR, THURAYA,…) peuvent être utilisés pour des informations non protégées en l'absence de systèmes de chiffrement ; leur emploi ne doit pas cependant être privilégié en raison notamment du coût des communications. Ils peuvent être utilisés comme moyens complémentaires, voire redondants des moyens militaires (couverture satellitaire, secours…), lors d'opérations limitées ou dans la phase initiale d'un déploiement (projection des échelons précurseurs),

214. La DIRISI, à travers le projet de contrat cadre ASTEL (Acquisition de Services de Telecom) et l'ESCPC (European Satellite Communication Procurement Cell) de l'agence européenne de défense, assurent la contractualisation des besoins au profit des forces.

215. L'UHF SATCOM apporte également une réponse aux besoins tactiques pour une communauté réduite d'utilisateurs. La ressource (postes radios type PRC 117 et 152 détenus par les armées et le COS, mais aussi accès aux fréquences sur des satellites tiers) est rare ; elle est destinée en priorité aux forces spéciales et aux équipes chargées de la mise en œuvre de l'appui aérien.

Les réseaux en opération

216. Les forces armées ont globalement besoin **d'élaborer, d'échanger, de stocker, d'agréger** des informations **de domaine :**

a. **Non souverain** de niveau maximum *Secret Défense Opération*[33] ou *Mission Secret* – MS[34] (coalition de circonstance), *Secret OTAN* (SO) ou *Secret UE* (SUE) ;

b. **Souverain** de niveau *Confidentiel Défense Spécial France*[35] (CD SF), parfois *Secret Défense Spécial France (SDSF).*

217. Les opérations et exercices utilisant des données opérationnelles classifiées sont conduits sur un réseau[36] *Secret* unique. Ce réseau, est dénommé « *FrOpS* » (« *French Operational network up to Secret level* »). Le CPCO est l'autorité d'emploi de *FrOpS*, la DIRISI en est l'opérateur.

218. *FrOpS* donne accès:

a. A l'ensemble des acteurs militaires nationaux de niveau stratégique et opératif ;

b. Aux théâtres, (niveau opératif, voire tactiques) ;

c. aux réseaux de niveau secret de nos alliés (OTAN, coalitions, pays) par le biais de passerelles sécurisées appelées « passerelles trans-domaine »[37].

219. Les informations souveraines (Spécial France) resteront, pour leur part, traitées sur des réseaux dédiées (Intradef, Intraced CD SF,…) répondant aux exigences nationales de sécurité.

220. L'emploi de ce réseau *FrOpS*, ainsi que le traitement et le management de l'information font l'objet de documents spécifiques.

221. *FrOpS* est donc le réseau de niveau *Secret* dédié aux opérations qui traite d'informations non-souveraines. Il héritera à terme des technologies développées dans le cadre du système d'information des armées (SIA).

---

32 Trois kits Satcom Iridium à bas débit équipent ainsi les deux kits Morphée utilisés pour les Evasan sur Boeing KC 135. Les E 2C *Hawkeye* sont également dotés d'une capacité Satcom Iridium.

33 Ces informations sont échangées avec les alliés qui ont le besoin d'en connaître.

34 Cas de l'Afghan Mission Network (AMN) qui figure un réseau de coalition « ISAF SECRET ».

35 Ces informations sont strictement destinées à du personnel français.

36 Lettre n° D-12-010316/DEF/EMA/CPI/PSIOC/NP du 1er octobre 2012

37 Une passerelle trans-domaine permet l'échange entre deux réseaux de niveau équivalent (ici de « secret » vers « secret ») alors qu'une passerelle inter-niveaux permet l'échange d'informations entre deux réseaux de niveaux distincts (par exemple entre un réseau secret et un réseau restreint).

222. La mise en place de *FrOpS* s'accompagne d'une adaptation des principes de classification des documents qui tous devront porter les mentions suivantes (pour les documents nationaux) :

a. Une mention de classification (SD-O[38] – CD) ou de protection (DR – NP).

b. Une mention de restriction du besoin d'en connaitre : « restreint XXX ».

c. Une mention de communicabilité : « communicable à *liste des pays ou organisation – X Y Z releasable ».*

En l'absence des mentions de restriction ou de communicabilité clairement indiquées, il revient au seul émetteur du document le droit de les définir (ce principe est éventuellement généralisable à d'autres réseaux).

223. INTRADEF et INTERNET OPS sont des réseaux de niveaux respectifs restreint et non protégé utilisés également pour les opérations, notamment parce qu'ils permettent de supporter la plupart des applications logistiques utilisées par la force et parce qu'ils permettent d'entrer en contact avec des acteurs non habilités au niveau Secret Défense Opérations (SD-O) : ONG, fournisseurs, CIMIC, …

Le Système d'Information des Armées (SIA)

224. La mise en œuvre des SIOC a débuté par une première phase de l'informatique. Les armées ont chacune progressivement agrégé des systèmes limités, puis initié des opérations plus importantes. Cette façon de faire a cependant favorisé le cloisonnement des différents systèmes d'information. Au bilan, les principaux systèmes d'armées sont :

a. SICF pour l'armée de terre.

b. SIC 21 pour la marine.

c. Intraced Air et SIC Air pour l'armée de l'air.

225. L'évolution suivante a eu lieu dans les années 2008 avec l'arrivée de l'Intraced sur les niveaux de confidentialité CD SF et Fr NNS (préfigurant *FrOpS*). Les systèmes d'armées et interarmées ont été et sont toujours reliés entre eux par un fédérateur qui garantit le suivi, l'intégrité et la non répudiation de messages entre les SI d'armées. Il offre un service d'annuaire, de chat, de travail collaboratif et de communauté de travail.

226. Le programme SIA a été lancé en 2010-2011, comme un vecteur de mise en cohérence de l'ensemble des SIC du ministère. Le SIA est un système destiné à être utilisé pour la conduite des opérations ; il comprend la mise en cohérence de systèmes existants et la réalisation de composants matériels et/ou logiciels. Il fera appel à une logique de métier et non de milieu, intègrera préférentiellement des COTS[39] mis en œuvre par l'OTAN et sera réalisé selon une logique incrémentale. Le SIA dispose d'une architecture qui garantit le fonctionnement du système sur théâtre d'opération malgré la rupture des liens de communication avec la métropole.

227. Le SIA s'appuie sur les réseaux existants. Il offre à travers un socle les services suivants aux utilisateurs :

a. Service d'annuaire, portail d'accès, travail collaboratifs, bases de données, gestion documentaire.

b. Des modules métiers du domaine C2, Renseignement, Logistique, qui viennent se déployer sur ce socle avec une préférence donnée à la réutilisation de produits de l'OTAN.

228. Cette architecture logicielle sera totalement ou partiellement déployée sur les niveaux de confidentialité :

a. CD SF ;

[38] Secret Défense Opération.
[39] *COTS* : *Commercial off-the-shelf* –composants pris sur étagère.

b. *FrOpS* SD-O ;

c. NP DR ;

d. Confidentiel UE ;

e. Confidentiel coalition de circonstance.

229. Dans la pratique, en métropole, dans les DROM COM, sur les bâtiments de la marine et sur les théâtres d'opération, un panel restreint de bulles informatiques, quasi identiques, sera déployé. Ces bulles se présentent sous la forme de « BOX », appelées aussi « SIA BOX », dont le rôle sera d'offrir aux utilisateurs, l'accès à l'ensemble des services du SIA. La SIA BOX, est une structure qui comprend les serveurs sur lesquels est hébergé l'ensemble des applications informatiques d'un bateau, d'une base aérienne ou d'un PC terrestre. Il s'agit de structures génériques, personnalisées en fonction des besoins de chaque unité. Là encore, les bonnes pratiques issues du monde civil sont progressivement appliquées au monde militaire : les différentes applications sont déployées sur des machines virtuelles regroupées sur des serveurs communs. Ces bulles seront administrées :

a. Par la DIRISI pour la partie Métropole et DROM COM ;

b. Par l'antenne DIRISI Toulon pour la marine nationale ;

c. Par les spécialistes du GTRS déployés sur le théâtre.

230. Les premiers gains espérés seront liés à la rationalisation de l'architecture, de l'administration et du MCO car tous ces matériels et tous ces logiciels seront quasi identiques. Côté utilisateurs, les problèmes d'interopérabilité internes ne devraient pas subsister car toutes les armées utiliseront le même logiciel et le même modèle de données. Les problèmes d'interopérabilité externes, avec l'OTAN seront limités grâce à l'utilisation de COTS issus de cette organisation.

231. Enfin, la sécurité reste une préoccupation permanente et l'architecture d'ensemble est dessinée en conséquence. Le concept de SIA Box répond au besoin de rationalisation physique des architectures des SIOC. Le but est :

a. De fournir un cadre de déploiement SIC simplifié ;

b. De faciliter la tâche des exploitants et administrateurs, en diminuant le nombre de configurations à maîtriser, à déployer et à maintenir ;

c. De faciliter le déploiement par les utilisateurs en opération, en cherchant à réduire les actions finales de paramétrage au strict nécessaire (logique « plug and play »).

232. Pour donner encore plus de souplesse et de modularité au SIA, il a été décidé de mettre en place sur la quasi-totalité des SIA BOX, un « SIA Store » permettant de compléter les applications déployées. Il offrira toutes les facilités de déploiement et de garantie de bon fonctionnement de l'application téléchargée dans l'environnement du poste de travail.

Section II − Les SIC du niveau tactique

233. Les architectures déployées au profit des forces sont notamment caractérisées par leur milieu de déploiement. L'espace de déploiement, par nature hétérogène et complexe, exige des architectures reposant sur toute la gamme de supports existant, du satellite au faisceau hertzien jusqu'au réseau radio tactique pour les plus bas niveaux La rapidité du cycle décisionnel, l'augmentation du tempo opérationnel nécessitent une autonomie dans la conduite de la manœuvre SIC tactique en appui de la manœuvre interarmées.

234. Les réseaux déployés sur un théâtre peuvent être de nature diverse, mettant en œuvre une gamme élargie de supports répondant aux besoins tactiques exprimés. Ils s'appuient, non seulement sur les systèmes satellitaires, mais également sur des réseaux radio (UHF, VHF, HF) et des réseaux s'appuyant sur un maillage des chaînes hertziennes, permettant de couvrir des zones bien déterminées (APOD, base aérienne projetée, Zones de PC ou logistique, axes logistiques…). Ils permettent à travers les stations satellitaires le raccordement vers la métropole et intra-théâtre. Les architectures déployées doivent garantir la mobilité tactique des

unités et autoriser une reconfiguration permanente du dispositif SIC déployé en fonction de la manœuvre.

Les liaisons de données tactiques (LDT)

235. Pour les armées, les LDT sont à la fois intégrées aux systèmes d'armes et contribuent à de nombreux domaines transverses (C2, coordination dans la troisième dimension, contribution à la Common Operational Picture [COP][40], appui aérien numérisé/Digitally Aided Close Air Support [DACAS], etc.) visualisée dans les états-majors. Leur adhérence aux SIC est de plus en plus forte notamment pour les besoins de passerelle et d'élongation. Ainsi, les moyens SIC (radio, communications satellitaires, systèmes d'information, chiffre, réseaux de desserte, etc.) concourent à la mise en œuvre des LDT.

236. Une liaison de données tactiques (LDT) est un moyen d'échange automatique des informations de données tactiques (position, direction et vitesse des pistes amies ou ennemies, ordres de tir, etc.) entre différentes plateformes des trois armées (aéronefs, bâtiments , centres de défense et coordination surface-air, centres de conduite des opérations aériennes fixes et tactiques, systèmes de détection aéroportée, etc.), unités et états-majors en temps réel[41] ou quasi réel[42] au moyen de systèmes de transmission haut débit, sécurisés et très résistants au brouillage.

Pour profiter pleinement des capacités offertes par les LDT, il convient de prendre en compte trois volets complémentaires :

a. L'aspect technique qui comprend, entre autres, des problématiques d'interopérabilité des matériels et d'architecture de réseau ;

b. L'aspect opérationnel qui en organise l'emploi au niveau des différentes plateformes ;

c. L'aspect SSI qui garantit la fiabilité des informations.

237. Les liaisons de données tactiques participent au réseau fédérant les échanges entre composantes en opération. Dans ce cadre, les LDT favorisent l'établissement de la COP et contribuent à améliorer le cycle décisionnel en opérations. Le terme LDT regroupe l'ensemble des protocoles permettant le partage de données tactiques : L1, L11, L11B, L16, LH et VMF, et à terme (2020) la L22.

238. Les LDT permettent notamment :

a. La liaison de commandement : diffusion des ordres et remontée des comptes rendus. ;

b. La liaison de coordination et de partage mutuel : échanges d'informations dans les trois dimensions pour une meilleure perception et une meilleure action globale ;

c. La remontée des tenues de situation opérationnelle[43] (*Recognized Ground Picture - RGP*, *Recognized Maritime Picture - RMP*, *Recognized Air Picture - RAP*) en vue de l'établissement de la COP.

239. La L16[44], interconnectée avec des systèmes de FFT (Friendly Force Tracking)[45], permet de réduire les risques de tirs fratricides en donnant aux systèmes d'armes la position des unités amies. L'émergence à terme d'une messagerie unique et normalisée (de type VMF- messagerie K) pourrait offrir nativement l'interopérabilité entre les systèmes.

240. La liaison 11 est encore utilisable - malgré les contraintes SSI limitant son emploi - dans la constitution de réseaux ad hoc notamment pour les forces navales, terrestres et aériennes. Elle

---

40 L'OTAN utilise désormais davantage l'acronyme CROP (Common Relevant Operational Picture) qui désigne l'ensemble des informations pertinentes de la COP.

41 Qualificatif appliqué à l'acheminement des données ou des informations qui s'effectue sans délai si ce n'est celui de la transmission électronique. Ceci implique que les délais soient presque négligeables.

42 Qualificatif appliqué à l'acheminement des données ou des informations qui s'effectue sans délai si ce n'est celui du traitement automatique et de la transmission électronique. Ceci implique que les délias soient presque négligeables.

43 Voir PIA-3.7_COP(2004).

44 Cf. Guidelines for the employment of the Joint Tactical Data Link 16 (NATO RESTRICTED).

45 Cette interconnexion de la L16 peut faire appel à des outils SIC spécifiques tel que CSI (CRC System Interface), développé par la NCIA (NATO Communications and Information Agency), qui permet l'échange temps réels entre des aéronefs, des navires, des unités terrestres et des C2 qui utilisent des liaisons de données standardisées nationales ou de l'OTAN, notamment les liaisons ATDL-1, L1, L11B et L16.

utilise des supports filaires ou radio. La liaison 22 devrait à terme compléter les LDT actuelles et notamment se substituer à la liaison 11.

241. Aujourd'hui, la liaison 16 est la LDT de référence sur les théâtres d'opération, dans un cadre tant national que multinational. La L16 utilise le poste radio de type *MIDS* (*Multi-Functional Information Distribution System*) pour fournir des services de messagerie spécifique (messagerie J) et de phonie.

242. Contribution des LDT à la COP :

a) Les réseaux multi-liaisons sont la source principale d'établissement de la COP. Les échanges de données en temps réel ou quasi-réel, issus notamment des détections des différents radars, offerts par l'architecture des LDT et fusionnés au bon niveau forment la COP qui informe le commandement sur la situation opérationnelle et augmente sa capacité à décider, à engager des cibles ennemies et à réduire le risque de tirs fratricides. Une conception en amont du réseau multi-liaison est donc indispensable dans le cadre de la gestion et de l'exploitation du champ de bataille numérisé ;

b) Via la COP, les participants disposent d'une vision partagée et unique qui améliore la connaissance de la situation (SA[46]) et l'identification au combat (CID[47]).

243. Une couverture adaptée au théâtre et à la dynamique de l'opération doit être recherchée, dans un cadre espace-temps évolutif.

L'élongation stratégique, opérative et tactique de la L16 est apportée via le protocole *JRE (Joint Range Extension Application Protocol, JREAP)*[48], qui permet de faire transiter la messagerie J de la L16 via un support IP (satellite, réseaux de théâtre, infrastructure). Des passerelles JRE rendent l'intégration à l'architecture L16 relativement aisée pour toutes les unités d'une force réparties sur un théâtre d'opération caractérisé par d'importantes élongations.

[46] Situation Awareness.
[47] Combat Identification.
[48] Le Joint Range Extension Application Protocol –C (JREAP-C) (STANAG 5518 / MilStd 3011) est un protocole de communication développé et exploité dès 2002 par les US pour des besoins opérationnels de transmissions de flux L16 au format IP. Existe aussi au format JREAP-A et B (non utilisé en national).

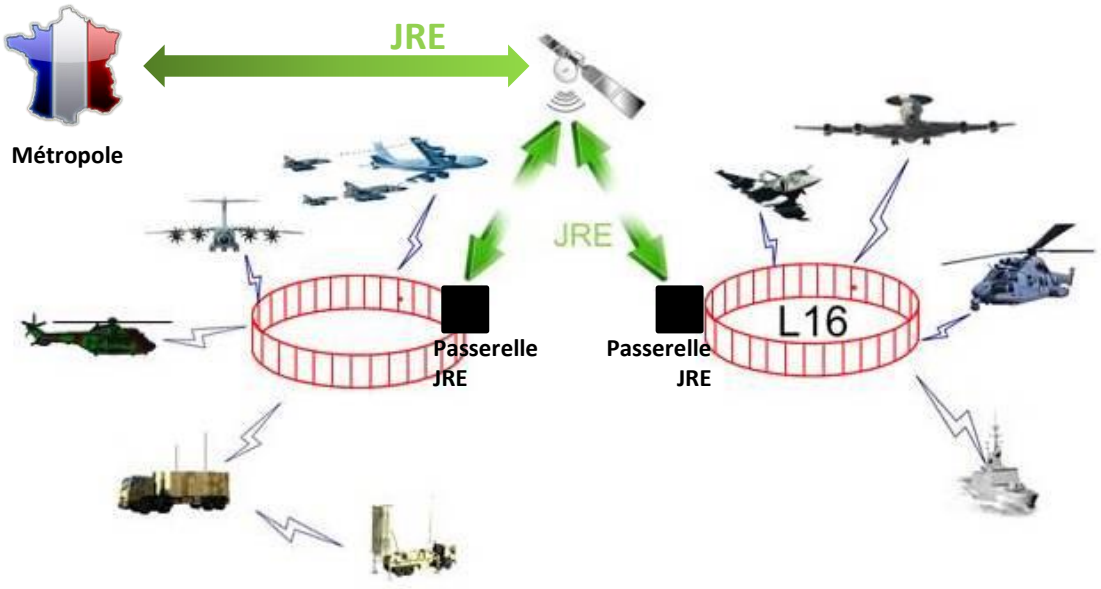

FIG. 3. – *Architecture générale des LDT en projection.*

244. Pour les opérations aériennes se déroulant dans les limites du territoire national, et au titre d'un mandat interarmées, le CDAOA/CNOA/Section LD :

a) Est le garant en temps de paix en FIR[49] France du respect de l'accord transport aérien/défense[50] et de l'absence d'interférence entre réseaux L16 ;

b) Coordonne ces activités avec les cellules de gestion des réseaux L16 des pays limitrophes afin d'éviter toute interférence ;

c) En cas de crise ou de conflit, coordonne avec les organismes de l'aviation civile la levée partielle ou totale des restrictions d'emploi induites par les accords nationaux particuliers, sur ou à partir du territoire.

245. La mise en œuvre des LDT en opération est complexe par nature et relève du seul COMANFOR.

Dans un réseau multi-liaisons, les LDT sont interconnectées et certaines actions dans les systèmes intégrés au réseau ont des conséquences sur les autres liaisons. Cela permet un haut degré d'interopérabilité mais ne permet plus de considérer une LDT de manière autonome mais dans un ensemble de réseaux de liaisons interconnectées. Il est alors indispensable d'avoir une manœuvre d'ensemble des LDT du réseau sous une chaine de commandement identifiée et unique.

La mise en œuvre des LDT repose sur une organisation (qui sera présentée dans une PIA LDT ultérieure) au sein de laquelle le DLM/ICO[51] occupe une place centrale.

246. Lors d'une opération en coalition, il est nécessaire de déployer, au sein de la structure responsable de l'architecture et de la gestion du réseau LDT, un élément de liaison national chargé de l'intégration des moyens français auprès de l'autorité unique d'emploi des liaisons de données tactiques de la coalition (*authority for TDL [Tactical Data Link] employment)*[52].

Il importe alors que la France désigne un DLM/ICO - FR ou LNO LDT, chargé de représenter et de défendre les intérêts nationaux en matière de LDT. Dans la phase de montée en puissance, son rôle est primordial pour assurer la pleine intégration des moyens français dans les réseaux LDT. Il est donc nécessaire que le poste soit armé par un DLM/ICO expérimenté.

---

49 *Flight Information Region.*
50 Accord du 29 juillet 2005 diffusé par note n° 1227/DEF/EMA/PI/BMNF du 24 août 2005 dont les annexes ont été amendées en 2011 et 2014.
51 *Data Link Manager/Interface Control Officer.*
52 Voir l'intégration du GAN (groupe aéronaval) à l'architecture L16 CENTCOM via le CAOC d'Al Udeid au cours de l'opération « BOIS BELLEAU ».

247. Niveaux de confidentialité (liaison et chiffre) :

a. Les LDT n'ont pas de niveau de classification intrinsèque. Le niveau est fixé par le commandant de l'opération. Les équipements LDT sont conçus pour fonctionner jusqu'au niveau SECRET OTAN ;

b. Au niveau national, les demandes de clés MIDS alliées sont adressées à l'AND (Agence Nationale de Distribution) puis les clés sont gérées par la filière CSSI de la DIRISI.

Les SIC de la composante terrestre

248. L'architecture SIC des forces terrestres s'articule autour de deux grandes composantes :

a. **Le réseau de théâtre**, qui assure le transit des communications entre les niveaux 1 (LCC) et 4 (GTIA), voire au-delà, de la composante terrestre. Le réseau de théâtre offre les supports de communication pour les services utilisés par les échelons élevés de la force terrestre (téléphonie, transmission de données et/ou d'image). Le réseau de théâtre permet de s'adapter aux engagements lacunaires et aux élongations au sol ;

b. **Les réseaux de capillarité** (parfois appelés réseaux contraints) qui assurent les communications jusque dans les plus petites entités tactiques déployées sur le champ de bataille, soit du niveau 4 (GTIA) jusqu'au niveau 7 (groupe de combat). Ces réseaux servent de support de communication pour les services des bas échelons tactiques (téléphonie, phonie alternat, transmission de données et/ou d'images).

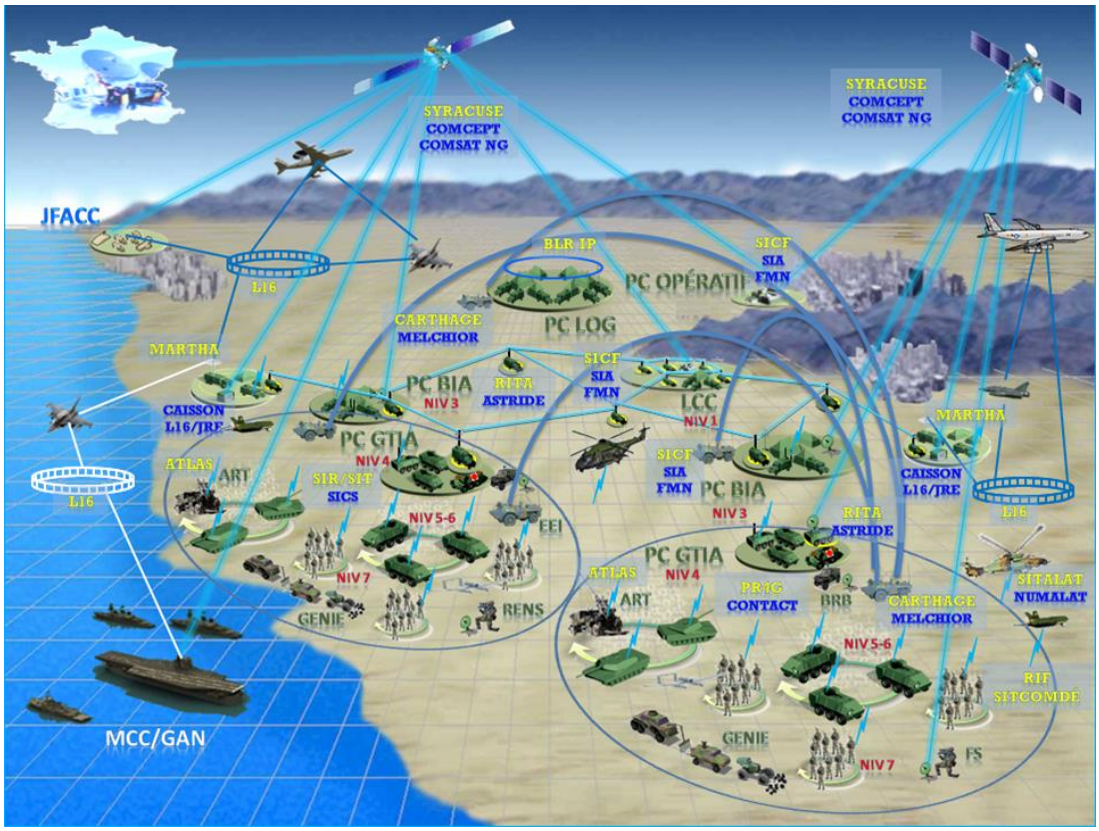

FIG. 5. – *Schéma générique d'un réseau SIC de théâtre.*

249. Les réseaux de capillarité offrent des débits moindres[53] que ceux du réseau de théâtre, mais sont néanmoins adaptés au volume des échanges d'information à ces échelons.

250. Le schéma ci-après présente une synthèse de l'architecture globale actuelle des réseaux des forces terrestres en opération. Ils précisent, pour chaque niveau de commandement, le(s) système(s) de communications utilisé(s) et les systèmes d'information permettant le commandement numérisé à l'échelon considéré.

a. Systèmes d'information (d'ici 2020 avant la mise en place du SIA et du SICS) :

(1) Un réseau *Mission Secret* interconnecté au réseau du PC opératif, pour les PC de niveau 1 à 3. Ce réseau est réalisé par l'outil SICF portant tout ou partie des applicatifs métiers utilisés sur le *FrOpS* si la France est nation cadre à ce niveau (*JChat*, *JOCWATCH*, *IGEOSIT*, etc.) ;

(2) SIR pour les PC de niveaux 4 et 5 (GTIA et SGTIA) ;

(3) Systèmes spécifiques liés à des systèmes d'armes (feux sol-sol, coordination 3D, GE, renseignement, simulation (MARTHA, ATLAS, SILCENT, …) ;

(4) Systèmes d'information terminaux (SIT) qui coexistent pour les niveaux 5 à 7 (SITEL, SITALAT, SIT ComDé, …).

b. Systèmes de communication :

(1) Réseaux satellitaires du type Syracuse et COMCEPT ;

(2) Réseaux satellitaires de type commercial ;

(3) Réseaux radio HF ;

[53] C'est pour cette raison qu'ils sont parfois et à tort appelés réseaux contraints.

(4) Boucle Locale Radio IP ;

(5) Réseaux radio VHF (PR 4G) ;

(6) Réseau RITA 2G avec faisceaux hertziens mobiles, permettant le raccordement et la desserte des différents PC déployés sur un théâtre.

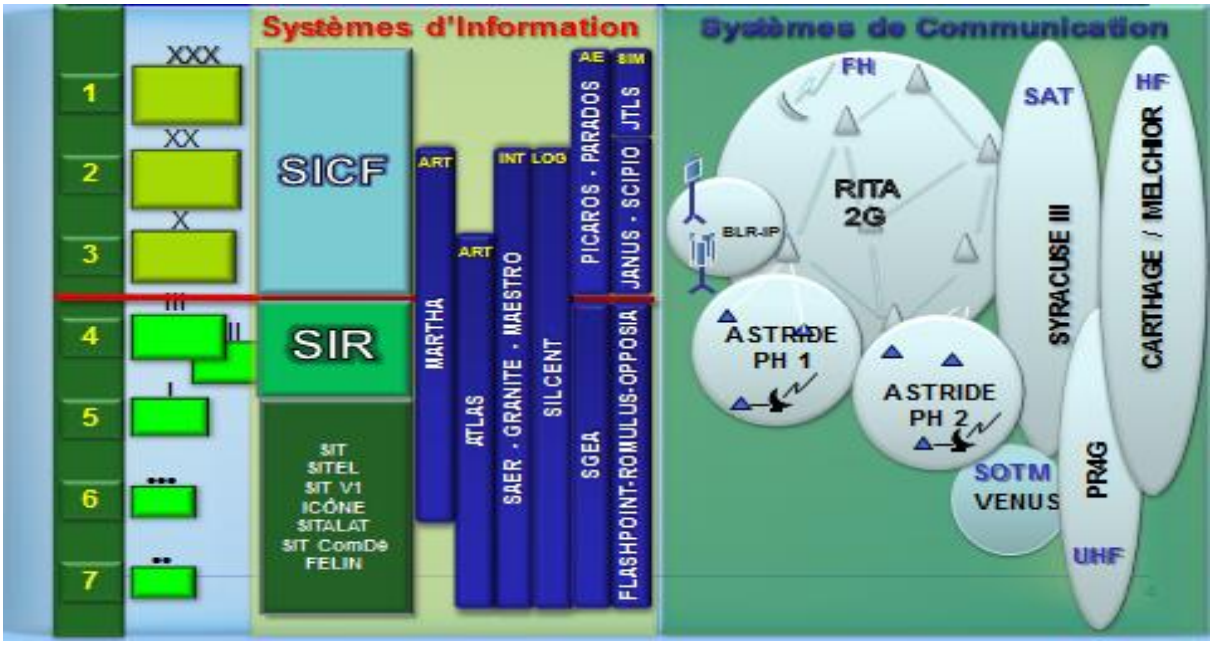

FIG. 6. – *Les SIC actuels de l'armée de Terre*.

251. Cette architecture actuelle est en cours d'évolution. La figure suivante présente ainsi l'architecture future envisagée, s'appuyant principalement sur le programme interarmées SIA. Elle suit les mêmes principes : à chaque échelon correspond un (des) système(s) de communication, servant de support à un (des) système(s) d'information qui sont employés pour le commandement numérisé de l'échelon considéré.

252. Certains systèmes sont d'ores et déjà en service ou en phase de mise en place dans les forces.

FIG. 7. – *Les SIC futurs de l'armée de Terre.*

253. L'architecture du réseau de théâtre peut s'articuler en nœuds de commutation (système RITA 2G[54] et – au niveau 4 – ASTRIDE[55]) raccordés entre eux par des systèmes de communications à vue directe (CHF) ou satellitaires (SYRACUSE ou autre[56]) dans le cas de grandes élongations.

254. En elle-même, cette architecture offre la redondance des liens. Mais de plus, des liaisons radio HF assurent le secours des liaisons. La résilience d'ensemble est donc garantie. En outre, cette architecture permet le raccordement et la desserte des PC, et l'intégration radio des mobiles, sous réserve d'être sous couverture radio. Elle est maillée (localement, dans les Zones de PC - ZPC), sécurisée, mobile et modulaire.

255. Elle offre les avantages d'être techniquement stable, physiquement robuste au champ de bataille et gérée de manière décentralisée par la composante projetée (en termes de supervision et de commandement du réseau).

256. Le choix des supports dépend des conditions d'engagement (situation tactique, phase, lacunarité, géographie de la zone de déploiement, menaces, ressources) et des capacités techniques des systèmes (c'est le rapport débit/portée).

257. La fonction de desserte des PC englobe le déploiement, jusqu'auprès du personnel d'état-major (utilisateur terminal), des matériels d'extrémité nécessaires au travail d'état-major : réseaux de télécommunications (téléphones) et réseaux informatiques (*LAN* et terminaux informatique). La desserte prend en compte les contraintes suivantes :

a. L'intégration, dès la conception, de la mobilité du PC ;

b. La coexistence de plusieurs réseaux physiquement séparés pour séparer des flux de classifications différentes, justifiés par des services de nature différente rendus aux usagers (parfois plusieurs pour un même usager[57]) ;

c. Il y a autant de réseaux de desserte que de réseaux de classifications différentes sur le PC.

Les SIC de la composante marine

258. Les systèmes de communication d'une force navale sont composés :

a. de moyens satellitaires ;

b. de réseaux d'élongation radioélectriques ;

c. de réseaux tactiques de théâtre.

259. Les supports de ces systèmes peuvent être fédérés au sein du réseau *IP* de la force aéronavale, (Réseau d'Interconnexion de la Force d'Action Navale – RIFAN) ou peuvent être exploités de façon indépendante. Les moyens satellitaires permettent à la force aéronavale de disposer de réseaux à haut débit dans un environnement numérisé et s'inscrivent pleinement dans le cadre des opérations en réseau. Le segment radioélectrique y ajoute la résilience, que lui confère un service de télégraphie indépendant des technologies « grand public », sur la quasi-totalité du globe terrestre.

---

54 Réseau Intégré de Transmissions Automatique de 2° Génération.

55 Accès par satellite et transmissions hertzienne au réseau de zone et à l'intranet de l'espace de bataille.

56 Réseau SATCOM COMCEPT.

57 Dans une même cellule d'état-major, des stations informatiques très diverses pourront être déployées, par exemple : le réseau « NATO secret wan » de l'OTAN, le réseau « Mission secret » réalisé grâce au système SICF, le réseau de C2 souverain réalisé par intraced ou SICF CD SF, le réseau pour le soutien national porté par Intradéf ou le réseau non classifié professionnel porté par internet (ELINFO ou fournisseur d'accès [FA]I local).

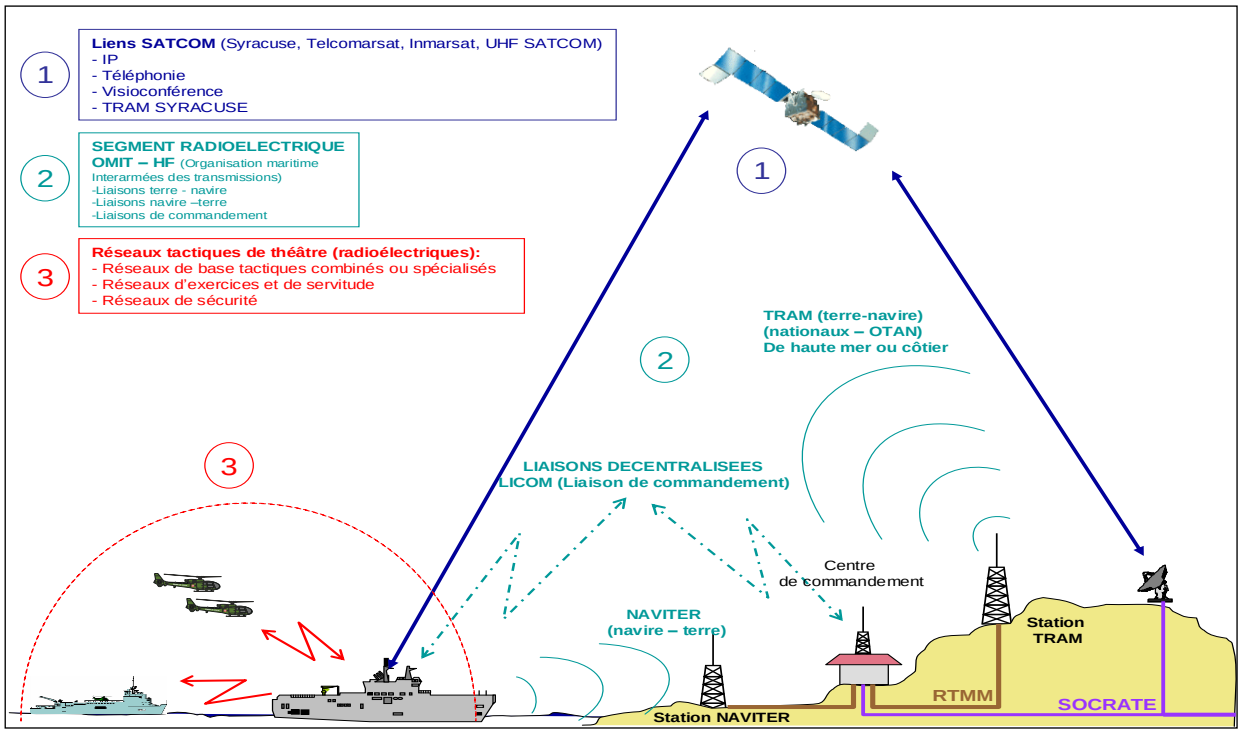

FIG. 8. – ***Les systèmes de communication de la force aéromaritime.***

RIFAN

260. Sur un bâtiment de combat, les systèmes de communication reposent sur des supports dont les niveaux de confidentialité sont assurés de bout en bout. RIFAN fédère ces systèmes de communication et constitue le *WAN*[58] des opérations pour un bâtiment à la mer, permettant l'accès aux services en s'appuyant sur les supports de transmissions HF, UHF, VHF guerre, SATCOM et filaires. La gestion du *WAN* RIFAN et de ses dessertes est assurée par le Centre National de Mise en Œuvre Réseaux (CNMO R) de Toulon en coordination avec les bords.

Les moyens satellitaires.

261. En plus des services classiques de Syracuse, les bâtiments de la marine disposent des services de transmission télégraphique « au fil de l'eau » (Tras59 et Naviter) par moyens satellitaires et de liaisons de commandement point à point entre un centre d'opérations maritimes et un bâtiment (Licom).

262. TELCOMARSAT fédère l'ensemble des offres civiles destinées à compléter les moyens militaires sur les familles de réseaux suivants : VSAT (constellations INTELSAT et EUTELSAT), IRRIDIUM et THURAYA. TELCOMARSAT permet, moyennant finances, de répondre aux besoins des unités non équipées de SYRACUSE ou de fournir un moyen de secours aux unités équipées.

263. INMARSAT dont la couverture est quasi-mondiale (hors pôles, au-delà de 70° de latitude), est un réseau de communication civil mondial complémentaire aux réseaux décrits précédemment.

Les réseaux d'élongation radioélectriques de la marine

264. Au sein de l'organisation mondiale interarmées des transmissions (OMIT, cf. PIA 6.6), les réseaux d'élongation radioélectriques de la marine comprennent des liaisons centralisées, décentralisées nationales, ou encore OTAN entre les bâtiments et la terre et constituent l'Organisation Maritime (OMAR).

[58] *WAN: Wide area Network.*
[59] TRAS : Transmission Radioélectrique en l'Air par Satellite.

Les liaisons des bâtiments

Les TRAM[60] / NAVITER

265. Les TRAM permettent aux unités de recevoir leur trafic télégraphique, au format ACP 127, « au fil de l'eau » ou par vacation hors port base. Ils peuvent être nationaux ou OTAN (cf. nota) et utilisés dans un cadre national ou au profit des forces de l'OTAN. Un TRAM est défini pour une activité ou pour un théâtre. La gestion d'un TRAM est assurée par une autorité qui en assure le contrôle. Les contrôleurs de TRAM sont CECLANT, CECMED, COMAR Manche, COMFOR Dakar, COMFOR Djibouti, COMSUP Saint-Denis-la-Réunion, COMSUP Fort-de–France, COMSUP Nouméa, COMSUP Papeete.

Les Liaisons NAVITER

266. Les liaisons NAVITER (SHIP to SHORE en OTAN) permettent aux unités en mer d'émettre leur trafic via un centre-relais automatique (CRA – Brest ou Toulon). Les CRA assurent l'acheminement, l'aiguillage et la gestion des messages au format « ACP 127 ». Ils sont pour cela connectés aux réseaux de diffusion nationaux et OTAN.

Les liaisons de commandement

267. La LICOM est une liaison de commandement décentralisée, destinée à permettre l'échange direct et en temps réel de communications opérationnelles entre une autorité et une force/ unité à la mer. Elle est baptisée LICOM, suivi de l'implantation géographique de l'autorité. (Ex : LICOM BREST). Une LICOM est activée sur un moyen radioélectrique « classique » ou sur un « chat » par l'autorité sur ordre ou à l'arrivée dans le théâtre (CHOP[61]).

Les liaisons des sous-marins

268. Les communications entre la terre et les sous-marins sont assurées par les émissions LF, VLF, HF et SATCOM SHF (pour les SNA uniquement).

269. Les TRAM sont émis à partir des stations VLF de Rosnay et Sainte-Assise ou LF de Kérlouan et La Régine et permettent aux sous-marins en plongée de recevoir leur trafic télégraphique par l'intermédiaire d'une antenne remorquée (pénétration VLF à la surface de l'eau).

270. ALFOST est coordonnateur des TRAM des sous-marins et des moyens VLF/LF.

Les liaisons de l'aéronautique navale

271. En plus des liaisons classiques « air », les aéronefs de patrouille maritime en mission au-dessus de la mer mettent en œuvre une liaison de commandement tactique (liaison HF télégraphique MATELO[62]) avec leur autorité de contrôle (MACA[63]). CECLANT et CECMED sont les MACA françaises au sein de l'OTAN. À terme, le contrôle opérationnel d'un aéronef équipé de moyens satellitaires (AVIASAT) pourra se faire sur un «*chatroom*» exploité par les MACA nationales ou OTAN.

Le réseau côtier 3G/4G

272. Le réseau côtier 3G/4G permet aux bâtiments non dotés de moyens SATCOM ou radioélectriques et qui opèrent dans la bande côtière (15 à 20 Nautiques) de disposer d'un accès restreint aux systèmes d'informations lorsqu'ils sont en portée d'un relais téléphonique.

---

60 TRAM : Transmission en l'Air à destinataires Multiples.
61 CHOP: *Change of Operational Control.*
62 MATELO: *Maritime Air Telecommunications Organization.*
63 MACA: *Maritime Air Control Authority.*

Les réseaux tactiques de théâtre

273. Les réseaux tactiques de théâtre comprennent les liaisons radioélectriques non énumérées précédemment ou les « *chat* » de niveaux tactiques utilisés au sein de la force aéromaritime (moyens HF, V/UHF). Ils font référence aux circuits des plans de fréquences permanents et sont rappelés pour une opération dans un ordre permanent pour les SIC ou un OPTASK COMMS (APP-11(G)).

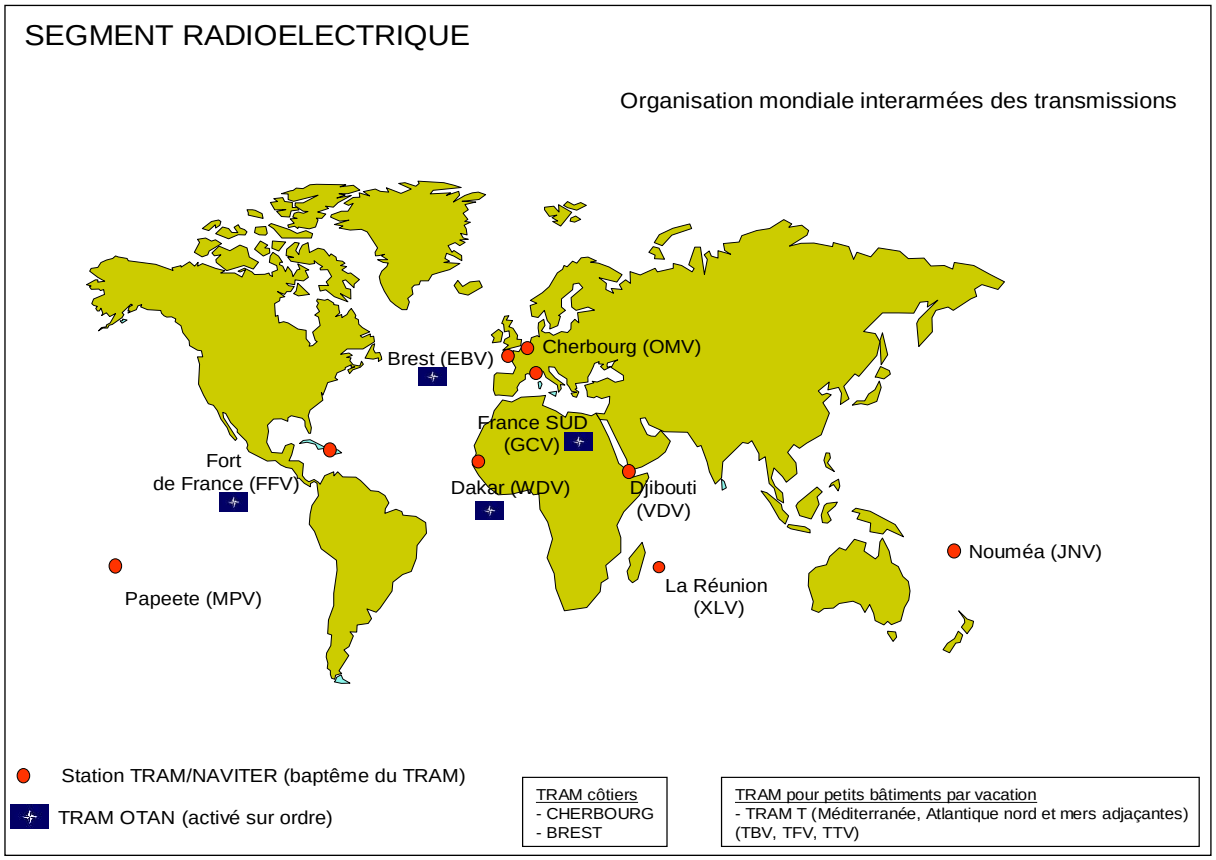

FIG. 9. – *Stations TRAM-NAVITER.*

Nota : Sur demande de l'EMO marine, les TRAM de Brest, Cherbourg Fort-de-France et Dakar peuvent être activés au profit des forces de l'OTAN, conformément à l'ACP 176 NATO Supp 1 France. La désignation d'un TRAM en procédure OTAN se fait sous l'appellation « Broadcast ».

Les SIOC

274. *FrOpS* est le SIOC principal de la Marine sur le segment SECRET, SIC 21 sur le segment CD SF. Ces deux SIOC fournissent, dans le strict respect des règles de sécurité », les services suivants à une force aéromaritime :

a. messagerie formelle ACP 127, informelle et instantanée ;

b. formatage / déformatage de messages (format OTAN AdaTP-3) ;

c. tenue de situation aéromaritime « non temps réel » / interface LDT ;

d. planification de l'activité aéromaritime (planification air limitée) ;

e. visioconférence ;

f. portail de navigation *Web*.

275. SPATIONAV est le SIO de niveau DR, interopérable avec les administrations de l'État et les agences et organisations de l'Union européenne dans le cadre du projet MARSUR (*Maritime Surveillance)* au sein de la communauté *CISE*[64].

276. SIA est l'avenir des SIO de la Marine. Dans un premier temps, l'effort se portera principalement vers l'intégration des modules métiers de SIC 21 vers SIA.

Les SIC de la composante Air

277. La spécificité de la 3ème dimension dans ce domaine résulte de la nécessité du raccordement des réseaux aux informations « temps réel » issues des capteurs et des centres de détection et de contrôle, pour délivrer une situation d'intérêt Air adaptée à la conduite des opérations aériennes.

278. Les SIC Air s'appuient sur le Système de Commandement et de Conduite des Opérations Aérospatiales (SCCOA), qui regroupent les systèmes dont les principales missions sont :

a. la surveillance de l'espace aérien ;

b. le contrôle des vols militaires et gouvernementaux ;

c. le commandement des opérations aériennes et de la défense surface-air.

279. Le SCCOA est notamment constitué d'un ensemble de radars, de systèmes de télécommunications sol-air et de systèmes d'information interconnectés ; ces systèmes sont installés sur les bases aériennes et au sein des centres de détection et de contrôle fixes pour les missions qui s'exercent sur le territoire national[65], notamment la Posture Permanente de Sureté Air (cf. PIA 3.33). Certains systèmes sont mobiles afin de disposer de ces mêmes capacités sur les théâtres d'opération.

280. L'avenir du SCCOA sera marqué par l'arrivée de radars de nouvelle génération, sur la mise au standard OTAN des centres de détection et de contrôle nationaux avec l'arrivée de l'ACCS (Air command and control system) à l'horizon 2015, qui apporteront une capacité essentielle dans le cadre de la PPS et des opérations aériennes.

---

64 *CISE*: *Common Information Sharing Environnement.*

65 Les SIC Air comprennent notamment pour le dispositif permanent activé H24, 7/7 :
- Les **capteurs** constitués par les radars HMA, BA civils et militaires, répartis sur le territoire national, les radars et centres C2 civils et militaires étrangers des pays limitrophes, les informations (pistes, plans de vol) sur l'ensemble du trafic aérien en temps réel survolant le territoire national provenant des centres de contrôle de la DGAC, les systèmes aéroportés, les systèmes tactiques déployés les services interministériels, les services de renseignements nationaux et alliés en amont ;
- **Les liaisons** reliant les centres C2 de la défense aérienne aux organismes précités ;
- **Le système STRIDA** (Système de Traitement et de Représentation des Informations de Défense Aérienne) intégré aux centres C2 (CNOA, CDC) qui établit la synthèse de tous les capteurs pour présenter une piste représentant la position exacte de tout aéronef survolant l'espace aérien national ;
- **Les télécommunications** comportant un système de radio sol-air (MÉTÉOR, bientôt SRSA), un système de téléphonie opérationnelle, un système d'interphonie (LOOP) ;
- **Les liaisons avec les systèmes d'arme** (défense surface air) et **les bases aériennes** (permanence opérationnelle composés de chasseurs, Plots MASA hélicoptère, escadron E-3F, escadron Ravitailleur, …).

FIG. 10. – *Capacités du SCCOA pour le commandement et la conduite d'opérations.*

Les systèmes de communication tactiques

281. Que ce soit en métropole dans le cadre d'exercices, lors des dispositifs particuliers de sûreté aérienne (DPSA) ou en opérations extérieures, le lien entre les Etats-majors métropolitains, les structures de commandements, les détachements Air ou les unités desservies repose essentiellement sur des liaisons satellites militaires de type SYRACUSE et sur des liaisons hertziennes tactiques. Ces liaisons permettent de délivrer l'ensemble des services nécessaires comme les réseaux opérationnels, la vidéo temps réel, la visioconférence, les applications métiers Air ou encore la téléphonie claire et chiffrée.

282. Ces systèmes doivent permettre à l'Armée de l'air de planifier programmer et conduire les opérations depuis ses installations permanentes situées en métropole (Lyon Mont Verdun actuellement).

283. Les opérations aériennes couvrent de vastes territoires. La mise à disposition de réseaux satellitaires constitue bien souvent un préalable à la manœuvre aérienne.

Les systèmes de détection et de contrôle tactiques

284. En application du contrat opérationnel, l'armée de l'air déploie des systèmes de détection et de contrôle tactique, ainsi que des systèmes tactiques d'aide à la navigation aérienne. En renfort de la PPS dans le cadre des dispositifs particuliers de sûreté aérienne ou en opérations extérieures, ces moyens se composent de radar ANGD, Vigie, TACAN, GONIO, CDC-D, C3MV1. Le raccordement de ces moyens est une mission prioritaire pour les SIC déployables de l'armée de l'air.

Les systèmes d'information opérationnels et de communication

285. Les systèmes d'information opérationnels et de communication (SIOC) sont au cœur des opérations aériennes. Déployés au profit des structures C2 (JFACC, C2A2, CNOA, COAIR…), ils contribuent à la manœuvre aérienne globale. Ces structures C2 s'articulent autour des fonctions planification, programmation, conduite et renseignement. Elles nécessitent, en fonction du type d'opération, l'emploi d'applications OTAN et/ou nationales reliées à des d'outils fédérateurs nationaux (SIOC du JFACC Rear et Forward/Harpon) ou multinationaux (ACCS, ICC), interopérables et capables d'opérer avec des réseaux permanent (FrOpS, NS WAN) et/ou alliés déployés (Mission Secret). A terme, ces capacités d'échange entre C2 seront offertes par le programme SIA.

Les systèmes d'information opérationnels des escadrons

286. Au sol, les équipages s'appuient sur des systèmes de planification, de préparation et de restitution de mission pour l'armement et l'aéronef : SLPRM, CINNA3, SPMR2, MELISSA… La performance en vol des aéronefs et de leurs systèmes d'arme, repose en partie sur les SIC qui y sont intégrés : liaisons de données tactiques, liaisons SATCOM….

287. En matière de maintien de condition opérationnelle, des systèmes récents sont associés aux systèmes d'armes et tiennent une place importante dans la régénération du potentiel avion : AMASIS HARPAGON pour le Rafale, Cindy et Taurus pour le drone Harfang, ATAMS pour les M2000 et le Caracal… Le rapatriement vers la métropole des données recueillies est une priorité pour les SIC déployés sur un théâtre.

Les systèmes d'information opérationnels des autres unités

288. D'autres unités déployées (centre de renseignement Air de théâtre, unités de soutien logistique, stations météo déployables…) mettent en œuvre des Systèmes d'information particuliers qui doivent être raccordés aux structures de commandement et de conduite des opérations.

Les liaisons radio

289. Les liaisons radio VHF, UHF et HF complètent le spectre des SIC Air et assurent la communication entre les aéronefs et le sol. Les liaisons HF servent également à la transmission de données.

Supports intranets utilisés

290. Pour mener à bien les opérations, l'Armée de l'air utilise prioritairement, depuis le commandement (JFACC) jusqu'aux unités participant aux opérations, le réseau FrOpS et le réseau de la coalition (Mission Secret).

291. En complément, elle doit également pouvoir utiliser, à tous les niveaux de la composante, le réseau internet (météo, source renseignement ouverte, SI logistiques…).

(PAGE VIERGE)

Chapitre 3
Rôles et responsabilités

Section I − Niveau stratégique (hors FN)

301. Le CEMA, outre ses responsabilités de commandement opérationnel, est autorité qualifiée en Sécurité des Systèmes d'Information (SSI) pour les armées, directions et services relevant de son autorité.

302. **EMA/CPCO/J6** : Le CPCO/J6 est l'autorité décisionnelle garante des architectures et dispositifs SIC destinés à permettre au CEMA d'assurer le commandement opérationnel de l'ensemble des forces françaises en opération. Cette responsabilité peut être déléguée, notamment aux armées pour la Posture Permanente de Sûreté. Le CPCO/J6 s'appuie sur la DIRISI, les EMO d'armée, l'EMIA-FE/J6 pour la définition des architectures SIC tant en phase de planification que de conduite.

303. **EMA/CIE :** le commandement interarmées de l'espace (CIE) commande les capacités militaires spatiales françaises et conseille le CPCO, dans le cadre de la planification et de la conduite des architectures SIC satellitaires civiles et militaires au profit des opérations.

304. **EMA/CPI :** le chef de la division cohérence des programmes interarmées est le représentant de l'autorité qualifiée CEMA. Le centre de cyberprotection des armées (CCPA), placé sous son autorité fonctionnelle, réunit les moyens œuvrant au sein des armées pour permettre au CEMA d'assumer ses responsabilités d'autorité qualifiée en sécurité des systèmes d'information, et en particulier celles relatives à l'homologation de sécurité des systèmes d'information.

305. **EMA/cyber** : l'Officier Général cyberdéfense (OG CYBER), en tant que chef CYBER du CPCO et officier général LID, conduit la défense des systèmes d'information du ministère et exerce une autorité spécialisée sur l'ensemble du domaine cyber en s'appuyant notamment sur les cellules concernées du CPCO, en particulier J6/LID et le CALID (centre d'analyse à la lutte informatique défensive).

306. **EMA/OLID** : L'officier lutte informatique défensive (OLID) central est l'adjoint de l'OG CYBER, ainsi que l'adjoint cyber du CPCO. Il assure le pilotage au quotidien de l'organisation cyberdéfense ainsi qu'en temps de crise.

307. **CALID** : Responsable du volet spécialisé et de l'expertise opérationnelle en matière de lutte informatique défensive, le CALID est le centre opérationnel en charge de la défense des systèmes d'information du ministère. Il met en œuvre une large palette de fonctions, telles que l'anticipation, la surveillance des réseaux, l'analyse de cyberattaque et fournit une capacité d'intervention. Il connaît l'ensemble des systèmes du ministère déclarés auprès de lui lors de la phase d'enrôlement préalable à la mise en service d'un système. Le CALID est placé sous OPCON du Chef Cyber du CPCO, dont il est un bras armé spécialisé. Il est sous le commandement organique de la DIRISI.

308. **Le CALID** émet des directives spécialisées vers les opérateurs de SI et les entités en charge de la cybersécurité.

309. Pour les autres niveaux, l'organisation CYBER qui couvre tous les types de systèmes d'information déployés (SA, *SCADA*[66]….) est décrite dans la doctrine cyberdéfense (DIA 3-40).

310. **DIRISI** : est l'opérateur ministériel des systèmes d'information et de communication (SIC) de la défense ; elle met en œuvre et soutient des réseaux de transmissions d'infrastructure, permanents ou de circonstance, dans un contexte interministériel et Européen. Chargée de la satisfaction des besoins des organismes de la défense, la DIRISI fournit plus particulièrement, à l'intérieur de son périmètre de responsabilité (qui exclut les SIC projetés), les moyens nécessaires à l'exercice du commandement opérationnel du CEMA et, par suite, des commandements opérationnels de théâtre, en milieu national, interallié et multinational.

[66] *Supervisory Control And Data Acquisition* ou Système de contrôle et d'acquisition de données.

311. La DIRISI assure également la satisfaction des besoins SIC liés aux missions permanentes (dissuasion - hors périmètre de la DIA 6 -, PPS Air, AEM, navigation aérienne dans le cadre de la réglementation ciel unique et du système de management de la sécurité, contribution française au *NATINAMDS*[67]…). Elle prolonge également les SI « organiques » sur les théâtres d'opération (SIL, SIRH, SIFIN…). Elle répond aux besoins des armées, directions et services engagés en opérations mais également en exercices. Le soutien aux opérations et au fonctionnement courant est traité simultanément par les mêmes centres nationaux afin de gagner en performance, en résilience, en économies de moyens et surtout une concentration des efforts.

312. La DIRISI appuie les états-majors impliqués dans la planification et la conduite des opérations, le CPCO de l'EMA, l'EMIA/FE, la DRM et les EMO d'armées, notamment lors de travaux de planification stratégique pré décisionnelle et opérationnelle puis, pendant l'engagement, lors des études d'évolutions/restructurations des forces engagées. La DIRISI/SDSSI assure la direction des réseaux de chiffrement des armées et la direction de la gestion des ACSSI.

313. La DIRISI met en œuvre l'Organisation Mondiale Interarmées des Transmissions (OMIT) : réseau militaire national de transit d'infrastructure à couverture mondiale qui permet :

a. d'assurer la permanence des liaisons entre le CEMA et les commandants interarmées outre-mer et à l'étranger et entre la métropole et les commandants des forces projetées ;

b. de servir de point d'ancrage pour les transmissions des forces projetées en opération extérieure, des forces de souveraineté et de présence.

314. En tant qu'expert technique, la DIRISI valide la cohérence technique et SSI (cyberprotection) des architectures proposées par les théâtres et les organismes des armées concernés[68] Dans ce cadre, la DIRISI apporte son soutien technique via :

a. La division opérations pour les travaux de conception et de planification des travaux SIC, en particulier pour la définition et la validation des architectures techniques SIC.

b. Le Centre Opérationnel de la DIRISI, implanté à Maisons-Laffitte, (COD) pour la gestion nationale des incidents et la conduite temps réel (permanence opérationnelle H24). À cet effet, le COD pilote les centres nationaux de mise en œuvre (CNMO[69]) de la DIRISI et coordonne leur action pour la résolution des incidents. Le COD rend compte au CPCO et informe les théâtres de la résolution des incidents.

315. **EMO 6 armées et services** (COS, DRM, SSA, SEA, SCA, …) : structures « miroir » du CPCO, les états-majors opérationnels (EMO) d'armée ou de service ont vocation à soutenir le CPCO dans le commandement opérationnel de leur armée, composante ou service. Pour le domaine SIC, les X6 des EMO sont les interlocuteurs pour la définition, la mise en place, la gestion, l'emploi, le déploiement et le soutien des SIC, notamment pour le raccordement à la chaîne opérationnelle interarmées des moyens interarmées mis en en œuvre par une armée ou un service. Chaque X6 peut être amené à proposer la conception de l'architecture SIC et du dispositif SIC relevant de son niveau ou de sa composante, en coordination avec le CPCO J6 et la DIRISI.

316. Chaque X6 d'EMO arme, si nécessaire et avec les renforcements ad hoc, une cellule LID spécifique et adaptée à son armée ou service, capable d'une part d'évaluer les impacts et, d'autre part, de participer au choix des mesures cyber défensives au regard des conséquences opérationnelles. Ils participent à la préparation opérationnelle de leur composante dans le domaine SIC[70].

---

67 *NATO Integrated Air and Missile Defence System*

68 En particulier le CFT/BTAC, le CSFA/BAAMA, le COS, la DRM, etc.

69 CNMO Systèmes d'Information du Mont-Valérien, Toulon ; CNMO réseaux, à Maisons-Laffitte et à Toulon ; CNMO moyens satellitaires (CNMO MS), à Maisons-Laffitte ; CNMO Intranets (CNMO I) à Rennes, Maisons-Laffitte et Toulon ; CNMO Télécommunications spatiales et Radio (CNMO TSR) à Favières.

70 La complexité croissante des SIC impose un niveau élevé d'expertise et de qualification du personnel ainsi qu'un entraînement régulier, normé et contrôlé de ce dernier sur les matériels mis en œuvre et le déploiement des réseaux SIC dans leur configuration opérationnelle. La définition des normes d'entraînement et le contrôle sont du ressort des armées et services et contribuent ainsi au suivi de la capacité opérationnelle SIC par les EMO. Les exercices interarmées doivent être l'occasion d'entraîner systématiquement les SIC en y incluant également les SIL et les SIAG très consommateurs en bande passante et en débit et dont la mise en œuvre s'avère désormais incontournable en opérations. La DIRISI est associée dans toutes les phases de préparation, de conduite, de soutien et d'analyse après action, aux exercices interarmées mettant en œuvre les SIC.

Section II − Niveau opératif

317. **EMIA-FE J6 :** référent opératif, l'EMIA FE contribue à la mise en œuvre du PC opératif (PCIAT) sur le théâtre d'opération. Ce PCIAT est constitué de modules opératifs générés à partir du vivier défini. Il s'inscrit notamment dans le cadre de l'échelon national d'urgence (ENU) ou de la génération du FHQ au profit de l'Union Européenne. A ce titre, le J6 de l'EMIA FE apporte son expertise dans cette génération ainsi que dans la conception des architectures de théâtre avec la DIRISI pour être soumises au CPCO/J6. Il participe activement au processus de planification opérative dans son domaine et de rédaction des ordres (CONOPS, OPLAN, OCI).

318. Depuis 2009, l'armée de Terre est responsable des SIC de niveau opératif et constitue le noyau clé du GTRS IA. L'armée de l'Air y apporte la connaissance et les SIC nécessaires à la synchronisation des effets dans la 3ème dimension.

319. La DIRISI est J6 pour les forces de souveraineté et de présence, hors opérations pour lesquelles le CPCO/J6 désigne un COMSIC IAT. En cas de déclenchement d'une opération dans la ZRP d'un OPCONer, le directeur DIRISI outre-mer peut assurer immédiatement la fonction de COMSIC IAT tant que le CPCO/J6 n'a pas formellement désigné l'officier qui remplira la fonction. Par la suite, le directeur DIRISI agira en soutien du COMSIC IAT qui sera autorité bénéficiaire[71] (au sens de la DIA-3(A)_CEO(2014)).

320. **COS J6** : Le contrôle politico-militaire des opérations spéciales impose que l'appui SIC qui leur est consacré vise systématiquement l'interopérabilité, la complémentarité et la redondance des architectures. La mise à disposition d'une capacité de transmission d'imagerie / vidéo en temps réel (FMV) et de numérisation aux niveaux opératif et tactique sera recherchée.

321. En amont d'une opération spéciale, la conception des ordres et des architectures est de la responsabilité de l'EM COS, en liaison avec les théâtres ainsi que la DIRISI et le CPCO.

322. Les contraintes d'élongations et d'actions dans la profondeur, l'isolement potentiel d'éléments FS et dans certains cas les limitations d'emport nécessitent de disposer de moyens de communication spécifiques sécurisés jusqu'au plus petits échelons tactiques.

323. Pour une opération spéciale multinationale[72], le raccordement au GCOS ou à un COMANFOR sera au mieux réalisé par des liens satellitaires nationaux relevant de la DIRISI, à défaut par des liens satellitaires ou des moyens d'infrastructure civils via des opérateurs étrangers. Le PC des SOTG français doit garantir son raccordement au Joint Special Operations Task Force (national) / Combined Joint Special Operations Component Command (multinational) et l'établissement d'une liaison nationale avec le COS.

324. Des unités FS sont identifiées pour la mise en œuvre de l'appui SIC aux opérations spéciales. Des formations des forces armées détenant des capacités et / ou des savoir-faire spécifiques peuvent également être intégrées dans la conception d'architectures et les déploiements SIC particuliers nécessitant des compétences extérieures au périmètre du COS et des FS.

COMSICIAT

325. Dès le déclenchement d'une opération multinationale et suivant sa dominante, le CPCO désigne une armée responsable des SIC (ARS)[73]. Sur proposition de cette dernière, le CPCO/J6 désigne le COMSICIAT au titre de l'opération concernée. Le COMSICIAT est le conseiller SIC et cyberprotection du COMANFOR ou du *NCC*[74]France. Il est donc chargé de la coordination de l'ensemble des SIC interarmées nationaux du théâtre, particulièrement dans les domaines de l'emploi, de l'interopérabilité, des LDT et de la cyberprotection. Il assure la fonction d'OLID de théâtre et a autorité sur un OSSI de théâtre.

---

71 Autorité bénéficiaire (*supported commander*) : « Commandant responsable au premier chef de tous les aspects d'une tâche assignée par une autorité militaire de niveau supérieur et qui reçoit des forces ou un autre type de soutien d'un ou de plusieurs commandants en soutien » (DIA-3(A)_CEO(2014), annexe A, page 53).

72 Lorsque la France est nation-cadre, le COS constitue le noyau dur des chaînes de commandement des opérations spéciales de la coalition (SOCC ou JSOTFHQ / CJSOTFHQ). En tant que nation contributrice à la composante des opérations spéciales, des modules FS (SOTG, SOATG) sont détachés dans les structures opérationnelles et des personnel COS sont insérés dans les structures de commandement dont le noyau dur est fourni par une Nation cadre autre que la France.

73 Dans le cadre d'une force maritime internationale, se reporter au paragraphe 334.

74 *National Contingent Commander*

326. Si la France est nation-cadre de l'opération multinationale, le COMSICIAT peut être amené à assurer simultanément les fonctions de Chef du J6 du PC opératif en tant que ACOS J6.

327. Dans le cadre d'une opération nationale, un COMSIC IAT sera désigné par le CPCO/J6.

328. Le COMSICIAT participe aux travaux de planification conduit par le CPCO/J6. Il est le correspondant du CPCO/J6 sur le théâtre. Il assure, en liaison avec lui, le contrôle du déploiement, de la mise en œuvre et des propositions d'adaptation des SIC nationaux et des moyens nécessaires à la chaîne de transmissions vers la France. Selon le principe de subsidiarité, il conduit la manœuvre des SIC nationaux sur le théâtre qui comprend les aspects conception et contrôle de la mise en œuvre. Sur le théâtre, il a la responsabilité fonctionnelle de la manœuvre des SIC nationaux des différentes composantes de l'opération (ACC, MCC, LCC et SOF).

329. Le COMSICIAT apporte son soutien à la cellule management de l'information au profit du *NCC*, dans le cadre de la maîtrise de l'information à des fins d'appréciation autonome de situation.

330. Le COMSICIAT a autorité sur une équipe dédiée pour concevoir les ordres **AUX SIC** et a autorité fonctionnelle sur le GTRS IA. Le chef du GTRS IA est responsable de l'établissement des ordres **DES SIC** que lui propose son CMO IA. L'équipe du COMSIC IAT est composée au minimum de :

a. l'équipe de conception du COMSICIAT (comprenant les compétences SSI-OLID) ;

b. d'une équipe planification (comprenant un officier systèmes de communication et un officier systèmes d'information) ;

c. d'une équipe conduite (comprenant un officier systèmes de communication et un officier systèmes d'information) ;

d. d'un expert en gestion des fréquences[75] ou *frequency manager* ;

e. d'un expert en coordination des LDT[76] ;

f. d'un comptable en charge de la gestion des équipements ressortissant de la chaîne DIRISI *;*

g. d'une cellule cybersécurité (comprenant en particulier le responsable en charge du suivi des équipements spécifiques liés au Chiffre (ACSSI)), qui pilote notamment la lutte informatique défensive sur le théâtre. Une cellule cyber de théâtre peut être également mise en place auprès du COMFOR ou du *NCC* France ou du FRA/*SNR* lorsque des missions de renseignement d'intérêt cyber et des opérations cybernétiques doivent être assurées.

331. Le GTRS IA est armé au niveau du théâtre et appuie le COMSICIAT dans la planification et la conduite de la manœuvre des SIC nationaux avec une capacité de supervision et d'expertise technique, en coordination étroite avec la DIRISI et les entités soutenues.

332. Le chef de corps du GTRS IA est responsable de la conduite de la mise en œuvre des SIC nationaux. Sa mission comporte 2 volets :

a. assurer le commandement, la coordination, la supervision, la gestion comptable et logistique des SIC nationaux ;

b. assurer le suivi de la capacité opérationnelle des SIC nationaux et d'en coordonner les aménagements nécessaires.

333. Le COMSICIAT exerce l'autorité fonctionnelle sur les groupements transmissions (GTRS[77]).

---

75 Il se coordonne avec le gestionnaire de fréquences de la force pour la gestion des fréquences des SIC nationaux.

76 Cf. TUEM COMSICIAT de l'ENU.

77 Mis sur pied à partir d'unités de la BTAC et d'unités SIC de l'armée de l'Air, renforcées éventuellement par le COMIAS et les Services, le GTRS peut également exécuter des missions de soutien spécialisé de quartier général (SSQG).

[NOUVEAU PARAGRAPHE 334.]

334. Pour les opérations maritimes, le commandant des SIC interarmées (COMSIC IA) est par défaut l'officier SIC du bâtiment. Pour une force constitué à la mer, la fonction est assurée par :

a. le N6 de l'état-major lorsque celui-ci est embarqué ;

b. l'officier SIC du bâtiment dont le commandant est le plus ancien.

Section III − Niveau tactique

335. **X6** : Sur les théâtres extérieurs, les X6 sont chargés sous l'autorité technique du COMSICIAT, du déploiement, du contrôle, de la mise en œuvre et de l'adaptation des SIC relevant de leur responsabilité. Ils rendent compte de toutes les évolutions nécessaires, des indisponibilités de service et expriment leurs besoins opérationnels futurs après concertation et coordination avec les X2 et X3 de leur niveau. Ils conduisent la manœuvre SIC en appui de la manœuvre tactique.

336. Ils participent également à la sécurité des SIC en mettant en œuvre les directives SSI/LID reçus.

Section IV – Opérations en coalitions

OTAN

Les SIC de l'OTAN peuvent être classés de la façon suivante :

337. **Les SIC fixes** (ou statiques): ils sont déployés de manière permanente dans les différents états-majors de l'OTAN et dans certaines unités des pays de l'Alliance. Ils sont fournis par l'agence NCIA. Des entités appelées « secteur » livrent les services OTAN au profit des états-majors de la NATO Command Structure.

338. **Les SIC mobiles**[78] : L'Alliance dispose d'un « *NATO CIS Group* » sous OPCOM du SACEUR. Il est déployé dans le cadre d'opérations de l'OTAN, permettant la mise en place d'un réseau spécifique à la mission et interopérable avec les réseaux fixes. Pour le mettre en œuvre, l'Alliance dispose de trois bataillons SIC multinationaux, situés à Wesel (en Allemagne, armé par l'Allemagne, le Danemark, les Pays-Bas et la Grande-Bretagne), à Grazzanise (en Italie armé par les États-Unis, l'Italie, la Roumanie et la Bulgarie) et à Bydgoszcz (en Pologne armé par la Pologne, la République Tchèque, la Slovaquie, la Hongrie, la Lituanie et la Turquie) eux – mêmes subdivisés en six modules SIC projetables (*Deployable CIS Module - DCIS*). Équipées essentiellement de ces *DCIS*, ces unités projetables sont en mesure d'appuyer une opération conduite par l'alliance par le déploiement, l'administration et la gestion d'une architecture SIC et des services délivrés. Chaque bataillon dispose également d'une M&S Coy (*Maintenance and Support Company*).

339. Pour les opérations aériennes, l'OTAN dispose également, dans le cadre du programme *ACCS* (*Air Command and Control System*), d'un *DACCC (Deployable Air Command and Control Center)*, stationné à Poggio Renatico (Italie) et dont la mise en service opérationnelle (*Full Operational Capability)* est prévue en 2014. Il regroupe un *CAOC* déployable (*Deployable Air Operation Centre)* et des moyens de détection et de contrôle déployables, appelé *DARS* (***D****eployable* ***A****ir Operations Center*, ***R****ecognised Air Picture Production Center,* ***S****ensor Fusion Post*).

340. La supervision des réseaux SIC OTAN déployés est effectuée par le *JCCC* (*Joint CIS Control Centre*). La responsabilité de l'OTAN est limitée aux besoins communs à la coalition, les nations restant responsables de leur propre déploiement. L'objectif recherché est de déployer ainsi une « fédération de réseaux » permettant de raccorder des SI de natures diverses et de délivrer des services.

341. En particulier, le concept SIC de l'OTAN pour les forces en opération consiste à déployer un *backbone* OTAN. Ce *backbone* embarque les standards d'interconnexion permettant le raccordement des réseaux OTAN-Nation par l'intermédiaire de passerelles et/ou de points

[78] Un document sur la déployabilité des états-majors de la *NCS* est en cours de rédaction par *ACO.*

d'interconnexion de réseau. En outre, il est préconisé que les mêmes standards soient employés pour l'interconnexion Nation-Nation. L'OTAN déploie son *backbone* et les systèmes d'information (SI) sur ce *backbone* ; l'OTAN fournit à chaque unité directement subordonnée l'accès à ses SI et la connectivité aux points d'interconnexion (PI). Concrètement, le PI est réalisé sur un nœud du *backbone* OTAN, équipé d'une passerelle *INM* (*Interface with Nations Module*), selon les principes :

a. L'échelon supérieur fournit le PI à l'échelon subordonné.

b. L'unité qui appuie, fournit la connexion à l'unité appuyée.

Cette logique de raccordement est différente de celle appliquée en France ou dans l'UE où « le haut raccorde le bas ».

342. L'OTAN peut faire appel à un opérateur privé pour prendre le relais, voire étendre l'architecture SIC déployé.

343. Les SIC fournis par les nations en soutien d'une opération conduite par l'OTAN : l'interopérabilité de ces moyens avec les SIC mobiles ou fixes pour permettre l'échange d'information doit être recherchée. Un processus d'homologation est préalable à toute interconnexion physique.

344. Si la France est désignée « nation cadre », les besoins SIC seront pris en compte lors des conférences de génération de forces, sous la tutelle du CPCO J6.

345. Les unités SIC françaises projetables se connectent aux unités du *NATO CIS Group* au travers de passerelles *INM*, les réseaux de desserte restant à charge nationale.

UE

346. La France participe régulièrement à la préparation de l'alerte de l'Union Européenne, à travers la mise sur pied du BG 1500 et les tours d'alerte OHQ et FHQ.

347. À ce titre, elle est en mesure d'assurer le commandement à travers l'OHQ ainsi qu'un FHQ déployé (*FHQ Deployed*) sur un théâtre. Désignée nation-cadre, elle fournit alors le noyau-clé de cet OHQ situé au Mont-Valérien, le commandement du FHQ ou PC de Force ainsi que l'armement de ses principaux éléments subordonnés. Pour la partie SIC, la France occupe de ce fait les fonctions d'ACOS J6 de l'OHQ et de chef J6 du FHQ. Le *FHQ Deployed* est raccordé à l'OHQ désigné et au *FHQ Homebase* si celui-ci est activé.

348. Toute opération de l'UE sortant du cadre alerte BG 1500 devra être précédée d'une planification et d'un processus de génération de force. Outre les SIC financés et déployés par l'UE, une chaîne SIC Spécial France sera logiquement déployée au profit du commandement de la structure *NCC*.

~~349.~~ *PARAGRAPHE A SUPPRIMER DANS VERSION FINALE* ~~Dans le cadre d'une opération multinationale hors OTAN/UE, les principes restent identiques.~~

Section V – Opérations nationales

350. Les principes restent identiques, avec une chaîne unique COMISICIAT/J6.

351. **Points d'appui DIRISI** : la DIRISI dispose de directions locales (DL) en outre-mer contribuant à l'OMIT, réparties sur la planète, dans les DROM-COM, ou dans des pays ayant signé des accords de défense avec la France. Ces DL, outre leur mission nominale locale permanente, contribuent au raccordement SIC de forces projetées dans le cadre d'une opération, au travers de leurs stations satellites d'infrastructure ou de leurs stations d'émission/réception forte puissance HF. Elles appuient la montée en puissance de l'EMIA de la zone en PCIAT et participent à l'armement du J6 du PCIAT.

Section VI – Territoire national – Espaces de souveraineté / MISSINT[79]

352. **PPS :** La DIRISI joue un rôle essentiel dans le cadre de la PPS en raccordant au quotidien les SIC dédiés mis en œuvre par les armées. Elle concourt directement à la maîtrise du SMS (Système de management de la sécurité). La DIRISI est en charge de la mise à disposition du réseau support, mais c'est l'armée de l'air qui est responsable et garante du fonctionnement et du soutien des systèmes de surveillance, de détection et contrôle. Il s'agit des dispositifs d'alerte (permanence opérationnelle) et du réseau maillé de radars (haute, moyenne et basse altitude, militaires et civils, nationaux et OTAN) soutenus par les armées : équipements SIC des centres de détection et de contrôle ainsi que du centre national des opérations aériennes complétés par d'éventuels moyens tactiques qui sont mis en œuvre par le CSFA/BA.AMA/SIC.

353. **Action de l'État en mer** : dans le cadre de leurs missions au titre de l'action de l'état en mer (AEM), les unités de la marine utilisent les moyens SIC classiques dont ils sont équipés pour communiquer avec les centres opérationnels de la marine, en particulier, dans le cadre des commandements de zones maritimes : le N6 (CECLANT, CECMED, COMAR MANCHE, ALINDIEN) assure la fonction de COMSICIA pour les opérations aéromaritimes de leurs théâtres respectifs en particulier dans le cadre des interactions avec les autres administrations. La DIRISI soutient et supervise au quotidien les SIC déployés dans les sémaphores et tous ceux contribuant à l'action de l'État en mer. Les administrations (Marine nationale, affaires maritimes, douanes, police, gendarmerie, sécurité civile) coopèrent aux missions de l'action de l'État en mer sous les ordres du préfet maritime.

a. SPATIONAV est le système d'information qui permet à ces administrations de coordonner leur action. Il est déployé dans les sémaphores, les centres opérationnels de la marine et ceux des douanes et dans les centres de recherche et de sauvetage en mer. Le système a vocation à terme à s'interconnecter au système européen EUROSUR.

b. EUROSUR est le système d'information de l'agence FRONTEX en charge de l'immigration clandestine pour les administrations européennes chargées de la lutte contre les trafics illicites (immigration clandestine en particulier) aux frontières terrestres et maritimes de l'espace Schengen.

c. À terme, également, le projet fédérateur CISE (Common information sharing environnent) rassemblera l'ensemble des systèmes d'information développés par les différentes agences de l'Union Européenne (FRONTEX, *EMSA*[80], *ESA*[81], *EDA*[82]). EUROSUR intégré à CISE fournira la situation navale de référence à la fonction garde côte.

354. **MISSINT/grands événements** : la DIRISI est l'acteur essentiel dans le fonctionnement des SIC quand une MISSINT est déclenchée. Le dispositif SIC d'infrastructure maintenu en permanence par la DIRISI est complété par des dispositifs déployés par tout ou partie des trois armées. La planification d'une MISSINT, la définition des réseaux et des systèmes mis en œuvre sont décidés par le J6 du CPCO. La mise en œuvre des SIC ainsi déployés sur le terrain relève de la responsabilité du COMSIC IA désigné pour la circonstance par le CPCO.

355. Selon l'opération, une armée sera désignée responsable des SIC. Le CPCO/J6 désignera un COMSIC IA parmi les armées ou la DIRISI.

a. La planification SIC peut se faire dans un cadre interministériel, au sein de groupes de travail au sein desquels le COMSICIA coordonne l'action des composantes engagées pour l'événement et identifie les synergies éventuelles.

b. La mission du COMSICIA, placé sous les ordres de l'Autorité Interarmées de Coordination (AIC) est alors de s'assurer de la cohérence de l'ensemble des SIC interarmées nationaux du dispositif mis en place, particulièrement dans les domaines de l'emploi, de l'interopérabilité, de la sécurité et de la gestion des fréquences.

---

79 MISsions INTérieures.
80 *EMSA: European maritime Safety agency*.
81 *ESA: European spatial agency.*
82 *EDA: European defence agency*.

c. En coordination avec le DZSIC[83], relevant de la préfecture, le COMSICIA fait définir, en liaison avec le CPCO/J6, les architectures, assure le déploiement, intègre les systèmes d'information nécessaires à la conduite du dispositif interarmées mis en place au sein du PC opératif préfectoral et des PC déportés et en conduit le soutien. La chaine LID centrale peut assurer la défense des systèmes d'informations déployés.

d. Chaque composante en charge d'un dispositif particulier désigne un COMTACSIC responsable de la mise en place des SIC « tactiques » associés.

[83] Directeur de Zone Sic.

Chapitre 4
La planification et la conduite des SIC en opérations

Dans le cadre du processus de planification et de conduite des opérations, une compréhension claire de la manœuvre des SIC est nécessaire pour en assurer le succès. Cette manœuvre concerne toute la chaîne de commandement et doit prendre en compte le temps, l'ampleur et la complexité de l'opération à conduire.

Section I − Planification de l'architecture SIC

CPCO

401. **Le CPCO/J6** assume, sans délégation, le commandement stratégique des SIC en opérations sous l'autorité du chef du CPCO représenté par le chef Cyber du CPCO. Pour exercer ce commandement, il s'appuie sur la DIRISI, les armées et les services et organismes spécialisés.

a. Il désigne un COMSICIAT (OPEX) ou un COMSICIA (OPINT) dès la phase de planification, à qui il donne le cadre du déploiement à réaliser (objectifs opérationnels ; C2, effets à obtenir, …) à décliner en ordres SIC.

b. Le COMSICIAT (ou COMSICIA) participe à la définition des architectures SIC nécessaires à la structure du C2, des systèmes de PC ainsi que les besoins en liaisons, réseaux et services des différents niveaux de commandement, en liaison avec la DIRISI et les EMO d'armée, l'EMIA FE, le COS, la DRM, les différents services (SSA, SEA, SCA,…). Ce travail s'effectue de façon itérative.

c. La DIRISI, avec l'appui des EMO, définit techniquement les architectures et les soumet à la validation opérationnelle du CPCO/J6, en précisant les solutions techniques préférentielles, les recommandations et les réserves.

d. Le CPCO/J6 valide les architectures. Il fixe les priorités et les exigences particulières qu'il estime nécessaires pour l'opération, en vérifiant la cohérence des besoins SIC avec les capacités disponibles. Il prend en compte la menace cyber dès cette phase et s'assure de la nécessaire résilience des réseaux.

e. Il fait assurer les coordinations nationales ou internationales en termes de spectre radioélectrique.

402. Le COMSICIAT désigné, avec toute ou partie de son équipe et du commandant de GTRS IA, est directement associé aux études SIC préparant l'engagement, apportant ainsi son expertise, afin d'être en mesure d'assurer d'emblée et dans les meilleures conditions de préparation ses fonctions sur le théâtre. Il est appelé en renfort auprès du J6 du CPCO ou du X6 de l'EMO dès sa désignation. Un noyau SIC devra être projeté dès la mise en place sur le théâtre d'opération des éléments précurseurs de la force.

403. Tête de chaîne de la cyberdéfense pour les théâtres d'opération, le CPCO/J6 coordonne l'action des différents COMSICIAT et OSSI de théâtres et fait appliquer par leur intermédiaire les directives et mesures de protection des différents réseaux et respecter les règles d'emploi des différents moyens de communication. Le CPCO/J6 contribue, en liaison avec les COMSICIAT, à la lutte informatique défensive au profit des réseaux déployés. Pour mener à bien ces actions LID, il s'appuie sur les états-majors opérationnels d'armée (EMO), les commandements opérationnels permanents et de circonstance, le COD DIRISI et les capacités des unités spécialisées dédiées (CALID, C2LID d'armées, SOC, GIR).

404. Le CPCO/J6 peut également demander le déploiement d'un réseau civil en appui de la force soit en autorisant une contractualisation locale par le COMSICIAT, soit à partir des ressources du ministère. Dans ce dernier cas, selon une procédure programmatique spécifique, un opérateur national peut satisfaire un besoin en réseau sur un théâtre d'opérations après étude de faisabilité.

DIRISI

405. La DIRISI appuie les états-majors impliqués dans la planification et la conduite des opérations, le CPCO de l'EMA, l'EMIA/FE et les EMO d'armées, notamment lors de travaux de planification stratégique pré -décisionnelle et opérationnelle puis, pendant l'engagement, lors des études d'évolutions/restructurations des forces engagées.

406. Elle est le point de contact unique pour toute demande de SIC de circonstance dépassant la capacité déléguée au théâtre. Elle étudie la validité des architectures sur le plan technique et de la réglementation SSI, fournit notamment le chiffre et les adresses *IP* nécessaires et réalise les liens, en particulier satellitaires (attribution de la bande passante, détermination des fréquences d'émission-réception, et mise à disposition des équipements de chiffrement)... La DIVOPS de la DIRISI constitue l'interlocuteur privilégié des états-majors et des forces, au sein de la DIRISI et propose des options au CPCO/J6 en lien avec les EMO pour décision.

407. À ce titre, elle est particulièrement chargée :

a. **Avant** l'engagement des forces :

(1) De participer aux processus de planification opérationnelle pour les exercices et les opérations, en liaison avec les acteurs interarmées et d'armées.

(2) De proposer au CPCO et organiser le cas échéant des plates-formes de validation et de mise en condition opérationnelles (MECO).

(3) De valider techniquement les architectures proposées par les armées et les COMSICIA ou COMSICIAT, en particulier, les architectures SATCOM (segment sol et spatial).

(4) De traduire en ordres techniques vers la chaîne DIRISI sa contribution aux exercices et opérations, préparer les dossiers et architectures au profit du COD pour la conduite des opérations.

(5) De faire préparer les matériels de sa responsabilité (câblage, informatique, moyens SAT civils légers) à déployer, pour mettre en place le dispositif SIC.

(6) De piloter la manœuvre des réseaux satellites (allocation des ressources et couverture des théâtres).

(7) De gérer la réserve SIC stratégique mis en place par le CPCO au CNSO.

(8) De participer à la manœuvre logistique en contribuant au prépositionnement sur le théâtre d'une réserve opérationnelle de théâtre (ROT) mise au profit du COMSICIAT.

(9) D'ordonner l'acheminement en avance de phase des ACSSI nécessaires à l'ensemble des SIC déployés.

b. **Pendant** l'engagement des forces :

(1) De répondre aux besoins des forces et leur apporter une assistance en cours d'action.

(2) D'appuyer la chaîne exploitation dans la résolution des incidents.

(3) D'accompagner les évolutions d'architectures liées aux évolutions des théâtres d'opération.

(4) De diriger les réseaux de chiffrement déployés.

(5) De conseiller le CPCO et les théâtres sur l'emploi des moyens SATCOM civils afin de contrôler les dépenses de communications.

c. **Durant** le désengagement des forces : d'accompagner la manœuvre de désengagement sous l'angle logistique (comptabilité, cession, destruction, retour du matériel en métropole).

d. **Après** l'action :

(1) D'effectuer le retour d'expérience SIC (pour les exercices et les opérations).

(2) De régénérer ou réformer les matériels revenus des théâtres et de reverser les matériels loués (moyens SAT légers).

(3) De faire évoluer et participer à l'évolution des procédures et de la doctrine SIC, sur la base de ce retour d'expérience.

408. Pour réaliser ces missions, la DIRISI dispose de structures nationales pour la mise en œuvre et le soutien des SIC de son périmètre de responsabilité :

a. les entités de la DC DIRISI et ses services centraux ;

b. les centres nationaux (COD, CNMO, SOC, CNGF, CNSO, …) ;

c. les DIRISI locales, en métropole, outre-mer et à l'étranger ;

d. les CIRISI, sous OPCON direct du SCOE en cas de déclenchement d'une opération.

L'EMIA-FE

409. Il assure, avec l'appui de la DIRISI et des armées :

a. l'expression des besoins SIC, dont les besoins en services de l'état-major opératif et l'étude de l'architecture SIC de théâtre lorsqu'il est déployé en tant que PC de force ;

b. l'étude et l'adaptation des architectures qui lui sont confiées, au cours des différentes phases de planification, dans le cadre de la préparation de l'engagement considéré.

Ces actions seront menées en liaison avec le COMSIC IAT si ce dernier a été désigné.

Les EMO d'armées

410. **L'armée de terre** : l'EMOT/G6 participe aux travaux de planification avant l'engagement des forces. S'appuyant sur le dispositif d'alerte défini par la PIA 7.0.1, l'armée de terre est en mesure de déployer dans des délais contraints[84] un nœud d'entrée de théâtre en fournissant le noyau dur du CCMO SIC interarmées et est chargée, de par son contrat opérationnel, d'armer l'essentiel des SIC du niveau opératif.

411. L'EMOT/G6 conduit la mise en œuvre des moyens SIC qu'il déploie jusqu'au niveau tactique. Pour cela, il déploie des unités adaptées, les groupements transmissions (GTRS) (du niveau régiment ou bataillon) et sous-groupements transmissions (SGTRS) (du niveau unité élémentaire ou section), qui peuvent englober le cas échéant les renforts issus des autres armées. Ces GTRS reçoivent leurs ordres fonctionnels de l'échelon opératif (COMSIC IAT).

412. Seule détentrice de moyens spécifiques majeurs comme les stations THD[85] ou BLR-IP, l'armée de terre peut renforcer occasionnellement d'autres armées, selon les ordres reçus du CPCO.

413. **La marine** : L'EMO/N6 est le bureau chargé de la préparation des SIC en opérations, en centralisant avec les OPCONers les expressions de besoins et en référant au CPCO/J6 la disponibilité des capacités SIC embarquées. Il assure l'interface avec le CPCO J6 dans la planification des opérations mettant en œuvre des moyens de la marine. L'é tu de technique de

[84] Délai de 72 h depuis la sortie de quartier.
[85] L'armée de terre met en œuvre 9 stations THD, dont 1 au profit de l'armée de l'air.

la faisabilité des besoins exprimés par les contrôleurs opérationnels, la validation des solutions techniques et la conception des architectures SIC relève de la DIRISI/SCOE/DIVOPS. Elle s'appuie sur le CIRISI de rattachement pour le déploiement des architectures et le gréement des bâtiments.

414. **L'armée de l'air** : L'EMO/A6 est l'unique interlocuteur du CPCO J6 pour la planification et la conduite des opérations de l'armée de l'air. Dans ce cadre, il établit, au vue des orientations définies par la partie A35, l'expression de besoin fonctionnel, qu'il s'agisse du déploiement de centres C2 (*JFACC*, CAOC, AOCC, …), de bases aériennes projetables ou de Détachements Air. Ce besoin est ensuite traduit en termes d'architectures SIC par l'Antenne Projection du CSFA/BAAMA/SIC, en charge de l'établissement des demandes de prestations vers la DIRISI/SCOE/DIV-OPS. Assurant la gouvernance générale de la fonction SIC opérationnelle de l'armée de l'air, l'EMO A6 établit, sous couvert du chef d'état-major du CDAOA, les arbitrages entre les différents besoins exprimés auprès du commandement des forces aériennes (CFA) lorsque la ressource requise s'avère insuffisante. Le périmètre d'actions directes de l'EMO A6 couvre les domaines suivants :

a. Opérations extérieures : les architectures établies s'articulent autour de structures C2 en charge des fonctions planification, programmation, conduite, renseignement et soutien. Elles nécessitent, en fonction du type d'opération, l'emploi d'applications nationales et/ou OTAN reliées à des outils fédérateurs nationaux (*JFACC Rear*, *JFACC Forward*/Harpon – COCCA[86]) ou multinationaux (*ACCS*, *ICC*,…), interopérables et capables d'opérer avec des réseaux permanent (*FrOpS, NS WAN*) et/ou de circonstance (*Mission Secret*).

b. Missions intérieures : il s'agit de mettre en place des architectures de circonstance destinées à renforcer les capacités des moyens de surveillance, de contrôle et de défense aérienne relevant de la Posture Permanente de Sûreté au profit d'évènements particuliers (Dispositifs Particuliers de Sûreté Aérienne), d'activités aériennes particulières ou de missions de la sécurité civile. Ces architectures relient les centres C2 Air (CNOA/CARS de Lyon Mont Verdun, CNDA de Cinq Mars La Pile, CDC/ARS) aux systèmes de surveillance (civils ou militaires), systèmes de défense sol/air (SAMP-T, Frégate, …) et autres centres C2 interarmées et interministériels.

~~415.~~ *PARAGRAPHE A SUPPRIMER DANS VERSION FINALE* ~~De manière générale, la préparation, la mise en œuvre, le soutien et le repli de l'ensemble des moyens tactiques SIC Air déployés en métropole et sur les théâtres d'opérations extérieurs sont assurés par le Groupement Tactique des Systèmes d'Information et de Communications AEROnautiques 10.805 d'Evreux (GTSICAERO 10.805). Ce groupement détient les capacités SIC nécessaires au transit (stations satellites de théâtre…), à la desserte (câblage tactique), au déploiement des réseaux informatiques nécessaires à la conduite des opérations aériennes (SI communs et SI opérationnels Air), ainsi qu'au déploiement/mise en œuvre et soutien des moyens de contrôle, navigation et surveillance (CNS),~~

416. *PARAGRAPHE A SUPPRIMER DANS VERSION FINALE* ~~Les personnels SIC nécessaires sont fournis par le GTSICAéro (déploiement immédiat, noyau dur) et sont renforcés, en phase stabilisée, par des renforts issus des autres unités de l'armée de l'air ou de la DIRISI.~~

Facteurs clé de la planification

Conditions de la planification

417. **Définition du C2** : les choix politico-stratégiques retenus dans la planification d'une opération débouchent sur un dispositif de commandement dit « C2 » (*Command and Control*). Une des finalités des SIC est d'accroître l'efficience de cette architecture C2 ainsi définie, qui conditionne d'emblée et de manière décisive les systèmes, liaisons et applications à déployer. Ces applications doivent apporter aux états-majors des services de bout en bout.

418. **Ampleur et type d'opération à conduire :** il s'agit d'analyser la taille de la force, les élongations envisagées sur le théâtre, le nombre de sites distants, les volumes des échanges à réaliser avec les autres membres d'une coalition, la couverture satellitaire disponible… Les opérations conduites par la France se font principalement dans des zones géographiques

[86] Centre Opérationnel de Commandement de la Composante Aérienne de niveau 1.

couvertes par les moyens satellitaires nationaux, qui assurent dès lors le rôle de lien principal entre le théâtre et la métropole, mais aussi en intra-théâtre.

419. L'étude SIC est aussi conditionnée par les besoins en informations exprimés par les états-majors et unités déployés. Ce processus appelé « *Information Exchange Requirement* (*IER*)» est impératif pour bâtir une architecture à même de rendre les services requis. À défaut, des modifications en conduite sont nécessaires pour faire coïncider les services déployés avec le besoin opérationnel.

420. **Contraintes** : La conduite simultanée de plusieurs opérations peut conduire à des difficultés tant en matière de disponibilité de moyens SIC que de débit utilisables (notamment pour les transmissions satellitaires). Le partage capacitaire doit être ainsi arbitré au CPCO, en s'appuyant sur l'expertise technique de la DIRISI et sur les EMO d'armées disposant de la connaissance précise des moyens disponibles. Une bascule des moyens peut être conduite sous couvert du CPCO en y associant étroitement les COMSICIAT/J6 concernés et en coordination avec leurs autorités de théâtre.

421. Le déploiement de l'architecture C2 retenue et donc du système SIC, se fera de façon séquentielle en fonction du mode de projection. Il est essentiel d'avoir un projet d'architecture le plus conforme aux besoins, réaliste et adaptable en fonction des évolutions envisageables du théâtre et du contexte politico-militaire. La projection des matériels SIC s'inscrit dans la manœuvre logistique globale d'acheminement des moyens de la Force sur les théâtres d'opération. A ce titre, une priorisation pertinente de la projection des moyens SIC revêt une importance essentielle pour la montée en puissance de la force déployée.

422. Un élément clé du succès C2-SIC réside dans la bonne synchronisation entre les composantes. Il nécessite également une bonne maîtrise du management de l'information (processus du *Knowledge Management*) ; aussi, le bon dimensionnement des cellules *IKM (Information KM)*, avec du personnel expert du domaine des opérations, est essentiel et doit être défini dès le début de la planification.

423. Par ailleurs, les opérations s'appuient aujourd'hui sur de nouvelles formes de communication qui s'imposent désormais naturellement à travers le partage d'informations disponibles sur des portails *Web* (par ex : le POIA - Portail des Opérations Interarmées), l'usage des services « *chat* », la remontée d'évènement ou de situation interarmées ainsi que le recours désormais permanent à la *Full Motion Vidéo* et la visioconférence.

424. **Architecture SIC** (pérenne, modulaire, ouverte…) : l'efficacité d'une architecture SIC se juge à un certain nombre de critères : résilience, redondance, fiabilité, débits des échanges, résistance à la guerre électronique, soutien, interopérabilité, maîtrise du « bout en bout », niveau de cybersécurité, protection du personnel face au danger du rayonnement électromagnétique sur les personnes (DREP)… L'architecture doit reposer sur le choix judicieux des supports de télécommunication et offrir la solution la plus efficiente (efficacité pour le moindre coût) dans la logique d'économie des forces rappelée dans le CIA-01 (A)_CEF (cf. les trois principes traditionnels de l'action militaire). La performance dans la qualité de service / *Quality of Service (QoS)* doit ainsi être systématiquement recherchée et intégrée dès la phase de conception des architectures SIC, car elle conditionne l'efficacité du C2 dans la conduite des opérations.

425. À partir de la définition de l'architecture C2, des emprises à raccorder et des services à délivrer, le COMSIC IAT en déduira les architectures SIC initiales, comprenant :

a. Les architectures des systèmes de communication (SC).

b. Les architectures des systèmes d'information SI[87].

c. Le niveau de cybersécurité et l'organisation de la cyberprotection.

d. Les passerelles d'interconnexion.

[87] L'ensemble des services nécessaires aux opérations (SIO dont les SI RENS, SIL) et aux états-majors (GED, services web, internet, etc…) doivent être identifiés pour être pris en compte dans l'architecture SIC.

e. Les moyens d'appui au commandement[88] des états-majors déployés. La mise sur pied des entités chargées de l'appui au commandement requiert les participations respectives de l'armée de terre et de l'armée de l'air (pour les SIC et la protection de PC) et du CICoS (soutien vie et logistique).

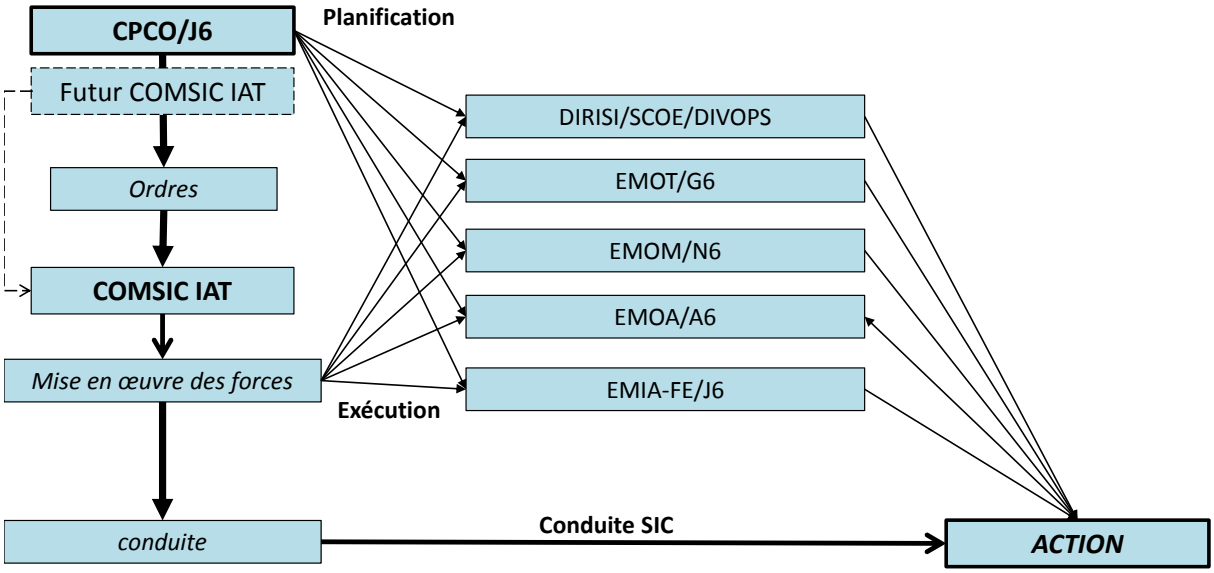

FIG. 11. – ***Processus décisionnel interarmées SIC.***

Section II − Conduite de la manœuvre SIC

426. Les principes généraux qui sous-tendent la manœuvre SIC, sont la cohérence de l'architecture entre la métropole et les théâtres et sa capacité d'adaptation aux besoins des forces et au tempo des opérations.

Phase de projection

427. **DIRISI :** Outre les réseaux satellitaires, dont elle assure la manœuvre, la DIRISI dispose de points d'appui permanent en dehors de la métropole pouvant permettre de raccorder les premiers éléments SIC mobiles projetés.

a. Le déploiement du PCIAT consiste à déployer des modules de capacité croissante : ELRT (équipe de liaison et de reconnaissance de théâtre) qui a vocation à être intégrée, toute ou partie, au sein du PCIAT.

b. PC HARPON (cadre QRF de l'ENU).

c. Des modules opératifs complémentaires (FIRI et FIA de l'ENU).

428. Sauf exception, la DIRISI/SDSSI pilote le chiffre et supervise la gestion des ACSSI au profit de l'AQ.

429. **Armée de Terre :** l'emploi des modules ENU, associé éventuellement au dispositif permanent de la DIRISI lorsqu'il existe à proximité du théâtre, permet la projection d'un échelon d'urgence composé de plusieurs éléments :

a. Équipe de reconnaissance et de liaison opérationnelle (RLE OPS).

b. Éléments d'armement d'un PC de force d'entrée de théâtre et son module d'appui au commandement fourni par la BTAC.

[88] Tel que défini dans la DIA 4, il recoupe entre autres l'énergie, hébergement, protection du PC, etc…

c. Éléments d'armement d'un PC de composante terrestre, fourni par la BIA[89] d'urgence.

d. Déploiement d'éléments de soutien logistique.

430. **Marine :** le processus pour la délivrance de SIC pour une unité de la marine nationale en opérations est le suivant :

a. Initialisation du besoin : l'expression de besoins SIC est émise par le COMSIC IA vers son contrôleur opérationnel pour validation du besoin après réception de la DIP (directive initiale de planification) ou de la DIROPCOM (directive du commandement de l'opération) si possible trois mois avant le début de la mission.

b. Validation opérationnelle : la demande en SIC de l'unité est analysée par le contrôleur opérationnel puis transmise au besoin vers l'EMO Marine ou l'EMA/CPCO selon les systèmes devant être déployés pour que la validation opérationnelle soit prononcée (validation technique acquise) : délégation au contrôleur opérationnel pour les architectures types, à l'EMO Marine pour les SIC Marine. Tout autre système reste de la responsabilité de l'EMA/CPCO qui a la possibilité de revenir sur les délégations accordées, par le biais d'un veto (procédure de silence).

c. Validation technique : la division opérations de la DIRISI analyse la faisabilité technique et valide le déploiement en désignant une DIRISI locale pour la mise en place à bord.

d. Un jour avant l'appareillage, les essais de flux et les modes dégradés sont testés, en coordination avec les centres nationaux de mise en œuvre (CNMO). Un compte-rendu est adressé au centre opérationnel de la DIRISI (COD) à l'issue.

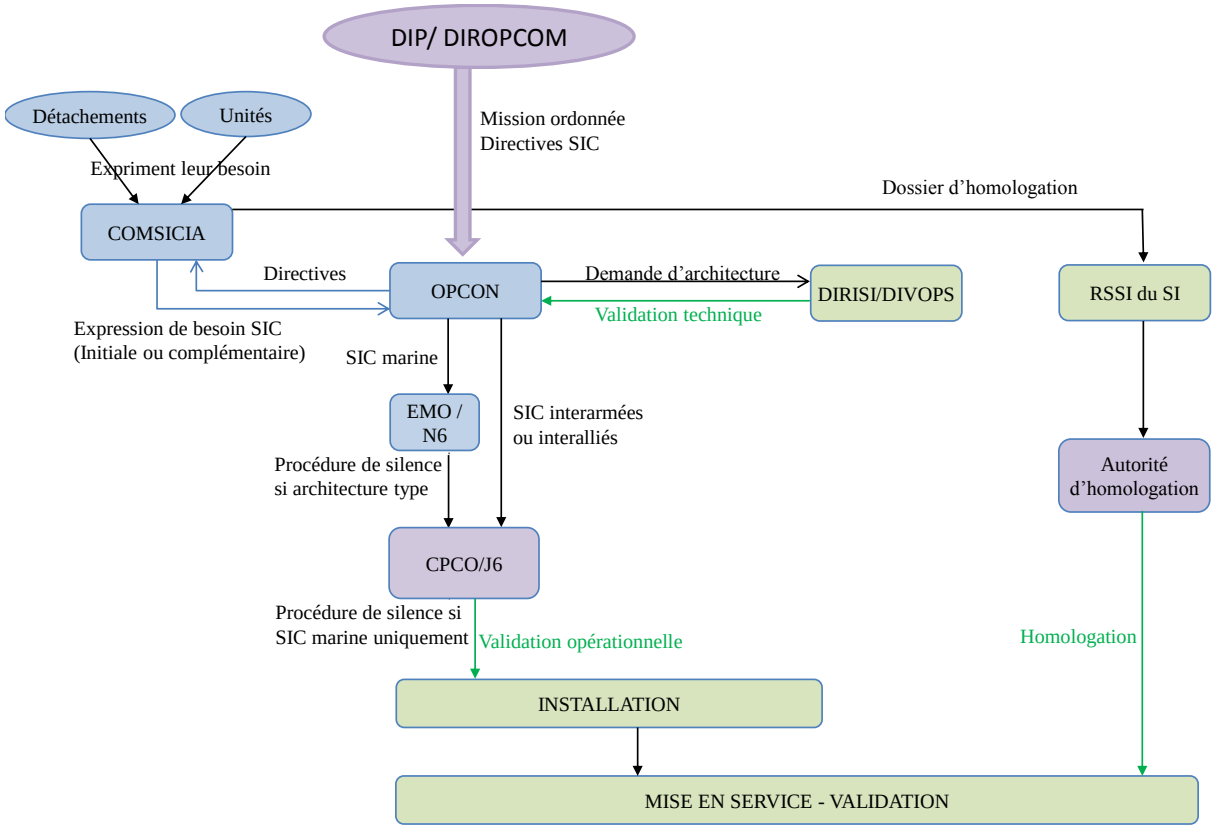

FIG. 11 bis. – ***Processus décisionnel interarmées SIC Marine.***

[89] Brigade interarmes.

~~431.~~ *PARAGRAPHE A SUPPRIMER DANS VERSION FINALE* ~~Un jour avant l'appareillage, les essais de flux et les modes dégradés sont testés, en coordination avec les centres nationaux de mise en œuvre (CNMO). Un compte rendu est adressé au centre opérationnel de la DIRISI (COD) à l'issue.~~

432. **Armée de l'air :** l'emploi des modules ENU / Rapace associés au dispositif permanent de la DIRISI, permet la projection d'un échelon d'urgence SIC adapté aux besoins d'un *JFACC*, d'une ou deux bases aériennes projetables, et permettant la reconnaissance, l'armement et la mise en œuvre des structures SIC associées.

Phase de conduite des opérations SIC

433. **Niveau stratégique :** Le travail commun des différents acteurs SIC sous la responsabilité du J6 du CPCO garantit les différents besoins en liaisons et permet d'assurer les raccordements des différents niveaux de commandement et la livraison des services demandés.

434. En phase de conduite, le J6 du CPCO s'assure de la pérennité des réseaux et de la continuité des services délivrés. Il assure le suivi SIC des théâtres. Dans le cadre de la cyberdéfense, le J6 peut coordonner une aide technique spécialisée dans la surveillance des SIC et la résolution d'incidents (avec les EMOX 6 et/ou le CALID et en liaison avec l'OG Cyber du CPCO).

435. La manœuvre SIC et SSI/LID nécessite une surveillance et une organisation précise qui reposent sur des états des lieux permanents et continus, tant en termes de systèmes de communication que d'administration des réseaux, de gestion des moyens de chiffrements, de gestion du réseau SYRACUSE, de besoins particuliers en bande passante, de fonctionnement des différents applicatifs SIAG , SIL, SIO, de gestion du spectre-électro-magnétique, de résilience des réseaux, de contraintes liées aux duplications des serveurs…

436. **Niveaux opératif et tactiques :** le COMSICIAT doit contribuer à l'engagement opérationnel de la force en garantissant l'emploi, la cohérence et la sécurité des SIC et conseillant le COMANFOR sur l'emploi des moyens SIC malgré la complexité grandissante des réseaux. A ce titre, il est responsable, sur le théâtre d'opération, de l'engagement technique et de l'adéquation des moyens aux besoins en liaisons. Pour ce faire, il doit disposer des outils lui assurant une supervision :

a. Sur les systèmes de communication (satellites, faisceaux hertziens, radio, réseaux de zone, communications satellitaires civiles, téléphones GSM, réseaux supports LDT), le bon usage de la bande passante sous spot Syracuse (en liaison avec la DIRISI), les dépenses liées à l'emploi des liaisons satellitaires civiles.

b. Sur les multiples systèmes d'information : sur *FrOpS*, Intraced, Intradef ou Internet, qu'ils soient au titre des SIL, des SIAG, des SIO notamment sur les nombreuses applications au profit de fonctions opérationnelles spécifiques comme le renseignement, le ciblage, les *Info Ops*.

c. Sur la gestion des fréquences de toutes les composantes de la force (dans le cadre d'une opération nationale) et des différents systèmes d'armes, en liaison avec les autorités civiles des nations « hôtes », compétentes dans ce domaine.

d. Sur le suivi des articles contrôlés de la SSI (ACSSI). La dimension SSI/cyberprotection doit être intégrée tant en phase de planification que de conduite avec une démarche « gestion du risque » (organisation et résilience des réseaux, architectures SIC, surveillances des réseaux et mesures préventives en réaction).

Externalisation / opérateur privé

437. Lors d'une opération, si la première phase de l'engagement peut nécessiter l'emploi exclusif de SIC militarisés en raison de leur robustesse et leur fiabilité sur le champ de bataille, il peut être fait appel par la suite, en complément ou en remplacement, à des moyens non militarisés mis en œuvre par la DIRISI ou par des opérateurs privés, tant pour répondre à des besoins

opérationnels qu'à d'autres besoins comme la condition du personnel en opération (condition du personnel en opération/ *welfare*[90]).

438. Le recours à un opérateur privé peut donc être envisagé afin de réduire l'empreinte au sol des SIC militaires déployés. Le déploiement de réseaux fixes peut être ainsi une solution fiable permettant de couvrir la zone de déploiement et de préparer le retrait puis le transfert d'autorité à un autre acteur. Dans tous les cas, il conviendra de s'assurer de la redondance, de l'intégrité, de la permanence et de la confidentialité des communications au profit du commandement. La question de l'interopérabilité avec les autres acteurs (militaires et/ou civils) devra également être prise en compte. Il conviendra cependant de bien étudier le degré de dépendance voulue vis-à-vis de l'opérateur choisi.

439. Une externalisation peut être initialisée par le COMSICIAT, avec l'appui du CPCO et/ou de la DIRISI. Les dépenses d'externalisation devront être inscrites au schéma directeur SIC du théâtre. Dans tous les cas, la surveillance et la défense des SIC engagés ne pourront être externalisées et restent sous la responsabilité des SIC.

440. L'utilisation d'INTERNET :

a. Le réseau ELINFO (élongation Internet des forces), mis en œuvre par la DIRISI, permet de raccorder les théâtres à un accès Internet métropolitain via une liaison sécurisée, c'est-à-dire maîtrisée et chiffrée par le ministère de la défense. Il complète les accès Internet fournis par des fournisseurs d'accès privés dans le cadre d'accords locaux. La passerelle n'offre qu'un support Internet ; les services internet (navigation Web, messagerie, boîtes mail, hébergement de sites web…) devront être souscrits par ailleurs.

b. Toute architecture SIC doit offrir des accès INTERNET, indispensables pour certaines fonctions logistiques (par exemple, CINDY TAURUS pour les drones Harfang) ou opérationnelles : fonctions renseignement, météo, *Info Ops* (COMOPS, OMI, CIMIC)…

c. En cas de ressource insuffisante en matière de bande passante, le recours à un fournisseur local, via la DIRISI et la DIRCOM locale, peut être effectué. Toutefois, le recours à INTERNET est potentiellement une source de vulnérabilité qu'il faudra s'attacher à surveiller et à contrôler afin d'en limiter les risques. Dans ce cadre, les procédures techniques de protection à appliquer sont les mêmes que celles implantées sur les réseaux issus de métropole.

Phase de désengagement/démontage

441. La phase de démontage des SIC doit répondre à deux exigences :

a. S'inscrire dans le cadre général de la manœuvre de désengagement « à temps » par un phasage adéquat du démontage des moyens SIC déployés, permettant ultérieurement un reconditionnement des équipements (cf. DIA 4.2.1 Désengagement).

b. Garantir au commandement la permanence de sa capacité à commander jusqu'au retrait définitif du dernier élément sur le théâtre, en particulier pour la fonction soutien.

442. Cette manœuvre des SIC doit donc être anticipée au plus tôt entre le COMSICIAT, les X6 et le J4, avec l'appui technique de la DIRISI, et peut exiger la mise en place de renforts temporaires, voire d'équipements spécifiques légers disposant d'une capacité de mobilité pour répondre aux besoins.

443. Au moment du désengagement, une attention particulière doit être accordée aux opérations de comptabilité, cession, destruction, retour du matériel en métropole. La DIRISI est le gestionnaire de biens SIC sur les théâtres d'opération.

444. **Après l'action, le J6 du CPCO** fait réaliser un retour d'expérience (dont la partie cyber) suite aux opérations. Il fait prendre les mesures directement applicables par la DIRISI ou les EMO/X6 d'armée dans le domaine des SIC et contribue directement au RETEX « froid ».

[90] L'accès à l'internet pour un usage privé dans le cadre de la CPO, ne relève cependant pas de la chaîne SIC (J6), mais de la chaîne logistique (J4/ASIA).

Relations du J6 avec J2, J3, J4, J5 et J8

445. La planification SIC est cyclique, itérative et collaborative, conduite de façon continue en étroite coordination et synchronisation avec J2 (axes images, FMV…), avec J3 et J5 (structures C2, lieu de stationnement de la force, planification de la campagne, Guerre électronique…) ainsi qu'avec J4, pour les besoins des SIC notamment en matière d'énergie, de climatisation et d'infrastructures mais également pour les besoins spécifiques des SIL qui imposent parfois des contraintes particulières, en particulier en termes de débit requis. Les aspects budgétaires et d'administration générale sont traitées avec le J8, en liaison avec le SCA, tant pour la définition du budget SIC initial nécessaire pour l'opération, que pour la prise en compte des SIAG à déployer. En phase conduite, l'élaboration des schémas directeurs SIC est réalisée en liaison avec J4, pour la mise en cohérence avec les schémas directeurs « infra », et avec J8 pour le cadre budgétaire défini.

446. La planification doit permettre d'établir à la fois les besoins SIC de l'ensemble de la force mais également les besoins J6 à honorer, pour que la manœuvre SIC puisse être planifiée et conduite : besoins en matière de connaissance de la menace et du théâtre (J2) et du plan de campagne (J5), besoins en matière de protection (J3) et de soutien du personnel SIC et des équipements (J4/ASIA).

447. Une attention particulière doit être portée sur le Chiffre avec les équipements et clés (ACSSI), dans la mesure où leur mise en place et transport obéissent à des règles contraignantes et incontournables de sécurité, engendrant notamment des délais à prendre en compte dans la planification et la conduite des opérations.

448. Le J6 peut être amené à travailler avec un *SEWOC*[91] *(Sigint & Electronic Warfare Operation Center),* lorsque ce dernier est mise en œuvre, conformément au *MC 0515/1 Concept for the SEWOC* du 27 février 2012. Le *Battle Spectrum Management (BSM*) est conduit en liaison étroite par coordination[92] entre les différents J, notamment le J2 et le J3 (cf. paragraphes 457 à 464).

Section III − Gestion du chiffre et des ACSSI[93]

Chiffre et soutien ACSSI

Le chiffre

449. Un réseau de chiffrement est constitué par l'ensemble des correspondants qui peuvent échanger entre eux des informations chiffrées par un moyen de cryptologie initialisé avec des clés de chiffrement. Tout réseau se caractérise par :

a. Une autorité d'emploi ;

b. Un ensemble de correspondants, au sens large, qu'il dessert ;

c. Un ensemble de matériels et documents ACSSI mis en œuvre ;

d. Des procédures de gestion des ACSSI ;

e. Un volume et un type de trafic ;

f. Des moyens de secours et de remplacement ;

g. Un degré de sécurité à apporter aux informations à protéger.

450. Un réseau de chiffrement doit répondre aux critères d'efficacité et de rapidité, et être adapté au format de l'information sensible à chiffrer (documents, voix, messages, vidéo, images, fichiers

---

91 Le rôle d'un SEWOC est de fournir : "*synchronization, coordination, advice and support to SIGINT and EW Operations in the Electromagnetic Environment while supporting commanders with near real time support for threat warning, intelligence analysis, assessments, target information, tactics, and countermeasures"*.

92 Le déploiement d'émetteurs radio à des fins d'*Info Ops* devra faire l'objet d'une étude technique conduite par le J6 *Frequency Manager*.

93 Article Contrôlé de la Sécurité des Systèmes d'Information.

informatiques, transmissions voix/données, etc.…). En conséquence, il peut y avoir plusieurs réseaux de chiffrement pour un même réseau de télécommunications.

451. L'organisation d'un réseau de chiffrement doit tenir compte :

a. Des caractéristiques du réseau de communications, qui permettent de choisir le type d'équipement de chiffrement (chiffreur d'artère, chiffreur IP, cryptophonie, etc.) ;

b. De l'emploi du réseau, qui définit la liste des correspondants à desservir ;

c. Du type, du format et du volume du trafic, permettant de choisir le système de chiffrement en fonction de ses caractéristiques cryptologiques ;

d. De la sensibilité des informations à traiter, qui permet de fixer le degré de sécurité du réseau.

452. Tout réseau de chiffrement[94] est donc caractérisé par :

a. Le niveau d'emploi ;

b. Le degré de sécurité ;

c. Le type de chiffrement.

453. Le centre national de mise en œuvre du chiffre (CNMO-C), appartenant à la DIRISI et implanté à Maisons-Laffitte, est chargé de la production des éléments secrets nécessaires aux ACSSI, de leur distribution ainsi que du suivi spécifique afférent, de la supervision et de l'exploitation des moyens de chiffrement télégérés ; il contribue au suivi spécifique des ACSSI.

454. Il met en œuvre le système SELTIC (Système d'ÉLaboration, de Transport et de gestion des clés). SELTIC est un système équipant les Organismes Chiffre des Armées (Terre, Mer, Air) et de certaines Directions du ministère de la défense chargés de produire, de distribuer, de gérer et de comptabiliser des éléments secrets[95] (ES).

455. Les principaux objectifs de SELTIC sont l'automatisation des moyens de production et de distribution des ES aux équipements, la comptabilité de ces ES ainsi que la fourniture à l'échelon du commandement d'une vue synthétique sur la situation des ES et sur la disponibilité des filières Chiffre. SELTIC est structuré en niveaux :

a. Un niveau Interalliées situé à l'Agence Nationale de Distribution[96], chargé de l'interfaçage avec les systèmes homologues étrangers (OTAN, UE et alliés), c'est-à-dire l'acquisition puis la distribution d'ES, ou l'envoi d'ES vers les systèmes étrangers ;

b. Un niveau Interarmées situé à la DIRISI, responsable de la gestion et de la distribution des ES pour la filière interarmées. Ce niveau est aussi responsable du suivi matériel, logiciel et des faits techniques pour l'ensemble de la communauté SELTIC raccordée à ce niveau ;

c. Un niveau national d'Armée ou de Direction, responsable de la gestion et de la distribution d'ES au sein de l'Armée ou de la Direction considérée ;

d. Un niveau local ayant à sa charge la distribution des ES vers les équipements utilisateurs.

456. Le centre national de téléchargement du chiffre (CNTC) assure la permanence de la supervision de sécurité des boitiers de chiffrement et de la cryptophonie interarmées. Il assure également la diffusion des éléments secrets (ES) électroniques interarmées et de l'OTAN. Le CNTC est implanté à Kremlin-Bicêtre.

---

94 La DIRISI/SDSSI dirige (au sens direction du Chiffre) tous les réseaux de chiffrement nationaux. Les rares exceptions, envisageable dans un cadre tactique, doivent être obligatoirement formalisées au cas par cas par l'Autorité Qualifiée (AQ) CEMA.

95 Les ES peuvent être des clés de chiffrement, des fréquences, des mots de passe, etc.

96 Implanté à Maisons-Laffitte.

457. Une force déployée doit assurer la fonction de point d'entrée/sortie de la comptabilité ACSSI sur le théâtre d'opérations. Ses attributions sur le théâtre sont les mêmes que celles d'une DIRISI régionale ou zonale. Les entités bénéficiaires assurent en fonction des spécificités du théâtre d'opérations, traduites sous la responsabilité de l'OSSI de théâtre (et non du COMSICIAT), des fonctions similaires à la comptabilité de site et/ou d'organisme.

458. **Acheminement des ACSSI :** la mise en place initiale puis le renouvellement des ACSSI et des équipements associés s'appuient sur des règles de sécurité très précises, contribuant techniquement et légalement à la sécurité des SIC. Cela peut impliquer des demandes de transport et de convoyage par le CPCO/J6 au CPCO/J4 qu'il convient de strictement respecter.

459. Les moyens et informations cryptographiques OTAN ou UE équivalents aux ACSSI sont appelés articles *COMSEC*[97]. Ils sont soumis aux mêmes principes de gestion que les ACSSI.

Section IV − Gestion des fréquences

460. Les fréquences radioélectriques sont un élément indispensable pour le fonctionnement de tout système employant des ondes radio. Leur accès, limité par la ressource qu'offre le spectre radioélectrique, est primordial pour l'utilisation optimale de l'ensemble des capacités militaires aussi bien dans le cadre des opérations, que de l'entraînement et de la préparation opérationnelle des forces. Les fréquences sont ainsi une des données d'entrée majeures pour la bonne conduite des opérations, alors qu'il s'agit d'une ressource physique finie et rare, du fait de la croissance de la demande militaire, mais également de la concurrence exponentielle des besoins civils.

461. L'augmentation de l'emploi de drones et plus généralement la conduite des opérations militaires modernes ont conduit à un accroissement du besoin en bande passante, qui doit être pris en compte dans le cadre de la gestion du spectre.

462. Le « patrimoine spectral des fréquences de la Défense » est réparti sur l'ensemble du spectre en bandes de fréquences pour des systèmes :

a. De radiocommunication fixes, mobiles ou spatiales (dont les réseaux d'infrastructure ou stratégiques) ;

b. De radiolocalisation ou de radionavigation ;

c. D'armes et de contremesures.

463. Sur le territoire national, il comprend :

a. Les bandes de fréquences attribuées au ministère de la défense par le tableau national de répartition des bandes de fréquences (TNRBF) ;

b. Les ressources exceptionnelles obtenues grâce à des accords particuliers avec d'autres affectataires.

464. Compte tenu des enjeux économiques de plus en plus importants qu'il recouvre, le spectre radioélectrique en général, celui du ministère de la défense en particulier, doit être géré avec rigueur et dans un souci permanent d'optimisation de la ressource spectrale. A ce titre, l'organisation du domaine des fréquences fait l'objet de la directive DGSIC n°18 en référence. Il appartient à la DGSIC de définir la politique d'emploi du spectre du ministère et à la DIRISI de la mettre en œuvre. Elle assure à ce titre de manière exclusive la gestion des fréquences de la Défense, à travers le Centre National de Gestion des Fréquences (CNGF). Le CNGF est l'interlocuteur de l'OTAN et des nations étrangères en sa qualité de *NARFA*[98] France.

465. Sur un théâtre, le gestionnaire de fréquences appartient à l'équipe du COMSICIAT et participe à la planification et la rédaction des ordres dans son domaine de compétence. A ce titre, il est responsable de la déconfliction des fréquences, de la déclaration des fréquences auprès du ministère de la nation-hôte ou auprès du J6 de la force pour une opération menée en coalition.

---

97 *COMmunication SECurity.*
98 *National Allied Radio Frequency Agency*.

Il assure la mise en place des outils de travail nécessaires au fonctionnement de la cellule « fréquence » (SPECTRUM XXI, bases de données…).

466. Le J6/*frequency manager* est en charge de la gestion du spectre électromagnétique du champ de bataille (*Battlespace Spectrum Management – BSM*) en coordination avec le centre de mise en œuvre des SIC interarmées (CCMO-IA SIC).

467. Supervisant l'ensemble du spectre électromagnétique utilisé, il doit avoir une connaissance précise, en liaison avec le J3 et le J2 (pour le volet SIGINT), des besoins induits par les différents systèmes d'armes ou/et fonctions opérationnelles des armées et des services, ainsi que des fréquences non utilisées par la force mais qui doivent être protégées contre les interférences. Le *Frequency manager* assume les mêmes fonctions dans le cadre d'une opération nationale.

Section V − Interopérabilité

468. La définition OTAN de l'interopérabilité est la suivante: *« The ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives ». (AAP-06 2013)*

469. La définition nationale de l'interopérabilité 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. » (DC-004_GIATO(2013)).* L'interopérabilité s'entend dans le cadre multinational, interarmées ou interministériel.

470. **Dans le cadre multinational**, l'interopérabilité SIC est recherchée afin d'échanger des informations avec les pays ou organisations avec lesquels la France constitue des coalitions.

471. La France doit disposer d'une interopérabilité technique SIC :

a. Avec l'OTAN ;

b. Avec l'UE ;

c. Dans le cadre de coalitions d'opportunité ;

d. Dans le cadre d'échanges de nation à nation (exemple : échanges bilatéraux avec les US ou UK).

472. Ces besoins d'interopérabilité se traduisent par autant de besoins de passerelles permettant l'interconnexion des réseaux entre eux. Ces passerelles sont appelées « passerelles trans-domaine ». La mise en œuvre de moyens des alliés au sein des unités françaises (états-majors, bâtiments de la marine, aéronefs…) peut également être utilisé (exemple : *CENTRIXS, SIPRNET, BICES* +, téléphonie ou Visioconférence sécurisés…).

473. L'interopérabilité technique, dans le cas de coalitions, s'appuie principalement sur les standards de l'OTAN. Elle repose actuellement sur le déploiement de passerelles applicatives issues du programme *MIP (Multilateral Interoperability Program)* autorisant l'échange de situations tactiques entre systèmes d'information opérationnels de nationalités différentes. Aujourd'hui le projet porteur des réflexions sur l'interopérabilité à l'OTAN est le concept du « *Federated Mission Network* » (*FMN*).

474. Au sein des coalitions, la France peut être « nation cadre », et, à ce titre, doit être capable de :

a. Fournir des détachements de liaison technique vers les autres nations ;

b. Mettre en œuvre un cœur de réseau de niveau « *mission secret* » au profit des partenaires de la coalition.

475. Lorsqu'elle n'est pas nation cadre, la France doit disposer des outils d'interconnexion au cœur de réseau qui est fourni. *FrOpS* apporte cette double capacité, à la fois lorsqu'il s'agit de proposer un cœur de réseau dans le cas où la France est nation cadre, ou de fournir une extension nationale interconnectable au réseau de la mission. L'intérêt supplémentaire du concept d'emploi de *FrOpS* est d'apporter un lien direct entre l'ensemble des théâtres et le CPCO.

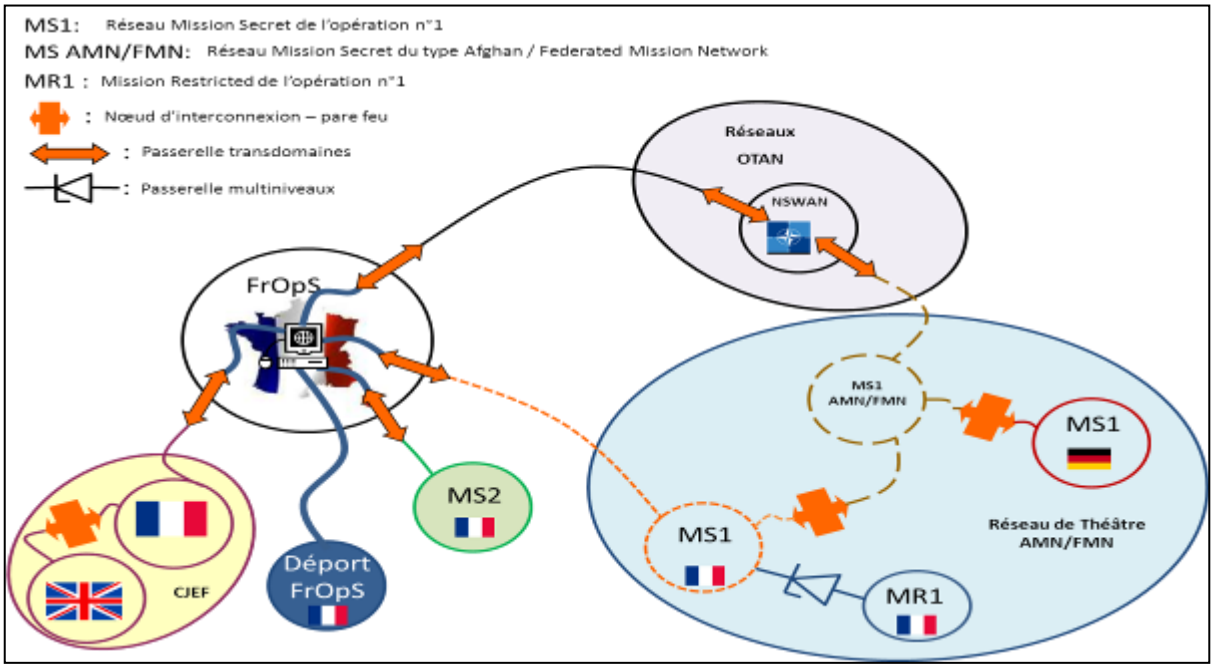

FIG. 12. – *Schéma de principe du réseau des opérations (FrOpS).*[99]

476. **Dans le cadre interarmées** : l'interopérabilité SIC est systématiquement recherchée entre les systèmes interarmées et les systèmes des armées. Une convergence dans le temps des systèmes existants vers des systèmes totalement et nativement interopérables est opérée au niveau interarmées comme au sein des armées. Le SIA répondra à cette exigence.

477. **Dans le cadre interministériel** : l'interopérabilité se concrétise par la capacité à échanger des informations entre services de l'Etat, principalement dans le cadre de « missions intérieures » (MISSINT), notamment au profit de la chaîne OTIAD[100] (organisation territoriale interarmées de défense).

478. Elle s'appuie, en particulier sur un maillage de type INPT (Infrastructure Nationale Partageable des Transmissions). L'INPT est un réseau de radiocommunications numériques, basé sur le standard Tetrapol, qui comprend :

a. Une infrastructure fixe à base de relais sur tout le territoire ;

b. Des terminaux utilisateurs avec chiffrement de bout en bout et mécanismes d'authentification ;

c. Des services d'appels individuels et multiples, de communication de groupe, de SMS, de géolocalisation, … ;

d. Une exploitation et une maintenance à la charge du ministère de l'intérieur.

479. La Défense se dote de terminaux portatifs INPT permettant d'équiper les unités engagées dans les missions intérieures.

[99] Les échanges relevant du « spécial France » se font sur un réseau différencié de classification CD-SF.
[100] *FrOpS* est également mis à la disposition de la chaîne OTIAD.

Chapitre 5
Cybersécurité & SIC

Section I – Cybersécurité

501. L'usage généralisé du numérique a modifié profondément la question de la sécurité des informations, notamment en raison de l'interpénétration des réseaux, le développement d'Internet et l'accroissement des attaques informatiques allant de la cybercriminalité à l'espionnage en passant par des actions offensives visant à nuire ou déstabiliser un État. Par nature, les infrastructures de transmissions et les réseaux numériques des armées sont des cibles potentielles et demandent donc un effort particulier de développement des capacités de cyber défense.

502. Les SIC sont au cœur des enjeux de la cybersécurité et doivent en permanence être protégés des menaces informatiques et d'éventuelles attaques, tout en garantissant la permanence, la fiabilité et la sécurité des services.

503. **Évaluation de la menace cybernétique**. Est appelé *Menace (threat)* le type d'action susceptible de nuire dans l'absolu, tandis que la *vulnérabilité (vulnerability)*, appelée aussi *faille* ou *brèche*, représente le niveau d'exposition face à la menace dans un contexte particulier. La détermination du niveau de la menace affecte non seulement les architectures des SIC envisagées, mais aussi la ressource en personnel qualifié nécessaire à la sécurisation et la défense de ces SIC. L'organisation, la détermination, la répartition, le niveau technique ainsi que la doctrine du ou des adversaires potentiels devront être mis en corrélation avec le volume de la force, la sensibilité de l'opération et son environnement, afin de déterminer les ressources à consacrer à la surveillance et la défense des SI.

504. Il s'agit par ailleurs d'identifier les vulnérabilités du dispositif SIC mis en place ainsi que le type de menace auquel il pourrait être sensible (déni de service, intrusion, vecteur d'intrusion – supports informatiques externes, connexion à l'Internet, messagerie - forum, sites web d'unités de la force pour communiquer avec les familles, réseaux sociaux…). Une attention toute particulière doit être portée aux réseaux civils utilisés concurremment et souvent très vulnérables aux attaques cyber.

505. La **Cybersécurité** est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité est obtenue par la combinaison coordonnée de la protection des SI (**cyberprotection ou SSI**) et de leur défense (**cyberdéfense**), complétée par des capacités de résistance et de rétablissement des réseaux et systèmes (**cyber-résilience**).

506. Au sein du ministère de la Défense, la cybersécurité est donc organisée selon trois piliers complémentaires et interdépendants :

a. la **protection** des systèmes d'information (ou « **cyberprotection** »), qui recouvre le champ classique de la **SSI** ;

b. la **défense** des systèmes d'information (ou « **cyberdéfense** »), qui recouvre la posture permanente de détection et de réaction aux attaques et la gestion de crise cybernétique ;

c. la **continuité** des systèmes d'information (ou « **cyber-résilience** »), qui recouvre les actions permettant d'assurer la résilience des systèmes, c'est-à-dire leur capacité à résister à une panne ou une cyberattaque et à revenir à leur état initial après l'incident.

Section II – Les piliers de la Cybersécurité

Cyberprotection ou SSI

507. La **Cyberprotection**[101] (Sécurité des systèmes d'information - SSI) est l'ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, et des services que ces systèmes offrent ou qu'ils rendent accessibles. Elle recouvre l'ensemble des moyens et des méthodes mis en place pour protéger l'information, les systèmes informatiques et les réseaux de communication par des moyens techniques (cryptographie, analyse et filtrage de flux, anti-virus, etc.), physiques ou logiciels et organisationnels (sensibilisation, formation, surveillance). Elle fait l'objet d'une politique (PSSI), régulièrement mise à jour et largement diffusée.

508. La cyberprotection permet de donner à un SI une aptitude à opérer en sécurité, aptitude qu'il convient ensuite d'entretenir par un processus de maintien en condition de sécurité tout au long de la vie du système, en dépit des évolutions techniques ou fonctionnelles et en tenant compte des risques nouveaux.

509. Les systèmes militaires doivent disposer d'une sécurisation de l'information cohérente avec les liaisons utilisées et le contexte d'emploi, en appliquant la réglementation en vigueur.

a. **Chiffre :** la sécurité des SIC passe par l'emploi de la cryptographie permettant le chiffrement des informations. À un équipement de cryptographie est associée une clé de chiffrement spécifique. La mise en place des équipements nécessaires et des clés répondent à des règles très précises, contribuant intrinsèquement à la SSI. Une violation de la réglementation, outre les risques de compromission, est punissable disciplinairement et pénalement. Pour ce domaine spécifique, et sauf exception formalisée par l'AQ, la DIRISI/SDSSI assure pour l'AQ la direction Chiffre de l'ensemble des réseaux de chiffrement (à distinguer des missions de direction technique ou celle relative à l'emploi).

b. **Gestion des ACSSI :** La sécurité des SIC repose sur la bonne gestion des ACSSI, qu'ils relèvent ou non du chiffre. Les gestionnaires de bien des équipements ACSSI doivent impérativement fournir, à la demande de la DIRISI/SDSSI, l'état inventaire et la traçabilité des ACSSI déployés.

c. **Protection contre les signaux compromettants :** la mise en place des équipements de communication, de routage et de communication, ainsi que les systèmes d'informations opérationnels doivent obéir à des règles techniques strictes limitant au maximum la diffusion de signaux compromettants susceptibles d'être interceptés par des moyens adverses. Cela implique notamment des choix judicieux en matière d'implantation géographique, avec la mise en place de zones réservées selon les critères techniques en vigueur à l'OTAN.

Cyberdéfense

510. La cyberdéfense[102] est l'ensemble des actions défensives ou offensives conduites dans le cyberespace en préparation ou dans la planification et la conduite des opérations militaires, notamment pour garantir l'efficacité de l'action des forces armées et le bon fonctionnement du ministère. Elle complète les mesures de protection des réseaux, des systèmes et de l'information (cyberprotection ou SSI) par une capacité d'opérations dans le cyberespace et une capacité de gestion de crise cybernétique.

511. Comme précisé par la doctrine de l'OTAN, les opérations dans le cyberespace[103] comportent les actions défensives (ou de lutte informatique défensive, LID), les actions d'exploitation (ou d'exploitation informatique, EI), les actions offensives (ou lutte informatique offensive, LIO). Elles sont conduites par la chaîne de commandement opérationnel de la cyberdéfense.

---

101 L'IGI 1300 constitue le document de référence à appliquer strictement.

102 La DIA 3.40 Cyber constitue le document doctrinal de référence en matière de cyberdéfense.

103 Correspondant aux *Computer Network Operations* (*CNO*), dont les définitions par l'OTAN, l'UE ou nos partenaires sont proches : actions visant à défendre, exploiter et attaquer les systèmes informatiques, les systèmes d'information, les réseaux, les logiciels et les données qu'ils contiennent, à contribuer à la supériorité de l'information tout en la déniant à l'adversaire potentiel. Ces actions regroupent l'exploitation du cyberespace (*Computer Network Exploitation CNE*), la défense de nos systèmes (*Computer Network Defence CND*) et les opérations offensives (*Computer Network Attacks CNA*).

512. **La défense des SI ou LID,** consiste à anticiper à surveiller, analyser, détecter (indice d'attaque, incident majeur, fait technique conséquent, faille logicielle, non-conformité, obsolescence,…) et réagir face à des attaques, intrusions ou perturbations qui pourraient compromettre, paralyser ou détruire nos systèmes, réseaux et données. L'EI y concourt également par le recueil du renseignement et l'exploitation des données qui peuvent faciliter la caractérisation et l'identification des attaques.

513. Souvent première source des incidents et des attaques, les comportements humains inadaptés peuvent fortement affaiblir le niveau de sécurité atteint par nos systèmes ; aussi, chaque utilisateur des SIC doit se considérer comme acteur de sa propre sécurité cybernétique à travers la mise en œuvre de pratiques simples et efficaces, appelée mesures d'hygiène cybernétique[104], contribuant à la lutte informatique défensive. Des actions de sensibilisation doivent être régulièrement conduites, ciblant les administrateurs de systèmes et l'ensemble des utilisateurs, mais aussi les échelons de commandement et de direction, responsables de la bonne hygiène de gestion et d'utilisation des systèmes. Ces bonnes pratiques doivent impérativement être étendues aux chaines d'acquisition (*supply chain*) et de maintenance.

514. Selon le théâtre d'opération, une cellule cyber de théâtre (CC de théâtre) est mise en place afin d'assurer la liaison spécialisée entre le niveau stratégique (CPCO) et le niveau opératif (théâtre). Elle coordonne au niveau du théâtre ou d'un ensemble de théâtres, en relation avec le niveau stratégique, les engagements opérationnels de cyberdéfense. Elle commande directement les unités nationales spécialisées qui lui sont rattachées. La CC de théâtre contribue aux travaux de planification, de conduite et d'évaluation.

515. **La gestion de crise cybernétique** et le **rétablissement** consistent à évaluer les conséquences opérationnelles et à rétablir les capacités altérées. Ils sont du ressort de la chaîne de commandement opérationnel de la cyberdéfense, en lien avec la chaîne de commandement des opérations pour le premier aspect, et avec la chaîne SIC pour le second. La phase de rétablissement doit permettre une analyse de l'incident pour en tirer les enseignements et ainsi corriger les vulnérabilités exploitées.

Cyber-résilience

516. La résilience se définit comme la capacité d'une organisation à faire face à des événements (incident ou agression), à leur résister et à se rétablir. Appliquée au cyberespace, elle est appelée cyber-résilience et définie comme la capacité d'un système d'information à résister à une panne ou une cyberattaque et à revenir à son état initial après l'incident.

517. La DGA prend en compte les problématiques de cyber-résilience lors de la définition des programmes d'armement dont elle assure la maîtrise d'ouvrage.

[104] Les « 10 commandements cybernétiques » diffusés au sein du ministère et des armées rappellent les règles élémentaires d'hygiène informatique (n°365 du magazine « Armées d'aujourd'hui »);
Voir également http://synoptic.intradef.gouv.fr/actualite/la-ssi-en-toute-confiance.

(PAGE VIERGE)

Annexe A
Emploi transverse des SIC

Face à l'accroissement des flux d'information et au rôle que ces derniers tiennent dans les opérations modernes, les SIC doivent faire preuve d'une réactivité et d'une adaptabilité permanentes, tout particulièrement dans le cadre de leur contribution à certaines fonctions transverses, facteurs de supériorité opérationnelle de nos armées.

SIC et maîtrise de l'information

SIC et « CMI globale »

A01. L'efficacité du C2 repose sur l'efficience de la gestion de l'information, eu égard notamment à l'importance croissante de ses flux. Au-delà des procédés et des aspects techniques définis dans le cadre de l'organisation du commandement, il s'agit désormais de mettre en place des outils et des procédures (par exemple, des Cellules de Maîtrise de l'Information (CMI)), permettant de valoriser l'information comme une aide à la décision.

A02. Les SIC soutiennent la CMI en lui fournissant l'expertise technique pour que cette dernière puisse rempli sa fonction de responsable du management de l'information.

SIC et COP

A03. La *Common Operational Picture* (COP), ou Représentation Opérationnelle Partagée (ROP), est un des processus structurants du partage de la connaissance au sein d'un état-major et s'appuie sur la mise en œuvre des opérations réseaux-centrés. La COP vise à un partage et à une synthèse interarmées, voire interalliées, de données de situation entre les différents niveaux de commandement d'une opération, de façon simple et intuitive, afin d'améliorer le processus décisionnel. En assurant des échanges fluides entre les différents intervenants, notamment en vue d'éviter les tirs fratricides, la COP permet une meilleure synthèse et de visualiser les positions Ami/Ennemi. Ce partage se matérialise sous une forme numérique associant cartographie, données, images et vidéos.

A04. Les SIC contribuent directement à alimenter la COP à travers l'optimisation des moyens de communications en charge du transfert d'informations de natures différentes et de volume en constante augmentation. L'objectif est de renforcer la capacité des systèmes d'information opérationnels à exploiter et à synthétiser les flux de données opérationnelles qui nourrissent la COP en permettant une convergence maîtrisée des flux d'information, quels que soient les systèmes d'information utilisés pour leur recueil .

A05. Les LDT participent à la COP en complément des Intranets de théâtre, relevant des SIC. La convergence des chaînes de la Numérisation de l'Espace de Bataille (NEB) et des réseaux de LDT devrait accroître à terme les flux d'informations et enrichir la COP.

A06. La COP permet, en les visualisant, de rassembler les différentes situations d'intérêt sur un même support commun, régulièrement réactualisé, permettant dès lors une meilleure fusion des informations d'ordre tactique, en particulier celles fournies à travers les LDT et une meilleure compréhension générale et partagée pour la prise de décision. En fonction du niveau (stratégique, opératif et tactique) auquel elle est disponible, la COP est utilisée comme un outil de suivi de situation (*reporting),* de commandement ou de conduite (*command & control).* Chaque niveau n'exige pas nécessairement une précision (positionnement, métadonnées, *FMV*…) ou une instantanéité (temps réel, temps réfléchi, temps différé) de l'information identiques ; ces deux critères ayant des conséquences directes sur les solutions techniques utilisées ainsi que sur les débits en bande passante utilisés pour acheminer les informations, l'expression de besoin en COP devra systématiquement être accompagnée de ses contraintes d'utilisation, pour permettre au COMSICIAT d'y répondre de façon adaptée.

SIC et ciblage (cf. DIA-3.9_Ciblage)

A07. La fonction ciblage s'inscrit en partie dans la chaîne C2 et applique un processus cyclique qui se répartit entre les différentes phases suivantes d'analyse des objectifs, de sélection des cibles, de préparation (définition des modalités/ répartition par composantes) puis d'exécution des missions de ciblage, et enfin d'évaluation des effets obtenus.

A08. Les SIC assurent alors le transfert et le fusionnement des informations pour la constitution des dossiers d'objectifs (DO), l'exécution synchronisée des missions de ciblage (tant dans les champs physiques qu'immatériels) et l'évaluation après action. Ils permettent principalement :

a. La diffusion des directives et des documents d'orientation (DIP, *CONOPS*, *OPLAN* et leurs annexes, etc…) du niveau stratégique vers les niveaux opératif et tactique pour cadrer l'analyse des objectifs de ciblage de la campagne effectuée par le personnel du ciblage ;

b. Le transfert des données provenant de tout type de capteurs terrestres, aériens, navals ou satellitaire (ATHOS), fusionnées avec l'appui de SAIM et fournies à la demande par la FIR pour :

(1) Élaborer les dossiers d'objectifs ;

(2) Diffuser périodiquement vers les composantes les mises à jour des différentes listes de cibles (cibles prioritaires, sous conditions, interdites, etc...) ;

c. La synchronisation des actions de ciblages par le niveau opératif (éventuellement stratégique), leur conduite par chaque composante et la coordination des acteurs 3D ;

d. La diffusion du *Battle Damage Assessment* et des effets obtenus, en transmettant le ROHUM, ROIM, ROEM recueillis après réalisation des actions de ciblage.

A09. En coalition, lorsque la France n'est pas Nation cadre, les SIC contribuent à l'exercice du contrôle national par le *FRA SNR (Senior National Representative)*, en permettant à la chaîne nationale de commandement, allant du CPCO jusqu'à l'échelon tactique, en passant par le Centre National de Ciblage d'échanger les informations liées au ciblage. Les SIC déployés doivent être interopérables avec le système de l'OTAN (*Joint Targeting System*) afin de permettre l'accès aux bases de données *Targeting* de l'OTAN et faciliter l'échange et l'exploitation de dossiers d'objectifs normalisés selon le formatage OTAN.

SIC et Renseignement (cf. DIA-2_RIM)

A10. Les engagements récents ont montré un accroissement constant des besoins en renseignement, avec une accélération du tempo des opérations, lié en particulier au ciblage, à la surveillance de zones étendues et à la protection des forces. La mise en œuvre de drones d'observation et le recours systématique à de l'imagerie haute définition, ont notamment démontré l'importance à accorder aux architectures SIC (axes images), permettant d'échanger et de traiter en temps réel les vidéos et l'imagerie fournis par les moyens aériens ou satellitaires. Cette nouvelle exigence a conduit à une adaptation des SIC, notamment en termes d'attribution de bande passante et de programmation de la ressource satellitaire nécessaire au transport de ce type d'information. Elle requiert une concertation entre les J2, J3, J35, J5 et J6 (stratégique et opératif) pour optimiser et planifier l'utilisation de la ressource, en fonction des priorités identifiées puis mettre en œuvre les modalités techniques après validation du CCMO SIC.

A11. Les SIC contribuent techniquement aux procédures d'échange d'information dans le cadre d'engagement de nos forces en coalition. De ce fait, le J2 doit exprimer ses besoins spécifiques auprès du J6 afin de vérifier la faisabilité technique et procédurale de ces échanges. Le niveau de confidentialité demandé doit être scrupuleusement respecté. En particulier, le besoin en débits et délais nécessite une bonne évaluation en amont par le J2 afin que le J6 puisse le prendre en compte dans la définition de son architecture SIC et durant la conduite de la manœuvre des SIC par le CCMO SIC.

A12. Les SIC sont le support du cycle de renseignement. Facilitant la mise en œuvre du processus de coordination de la recherche et de la gestion des besoins en renseignement. (*CCIRM* : *Collection Coordination and Intelligence Requirement Management*), les SIC assurent le transfert des données issues des capteurs ROHUM, ROEM, ROIM ainsi que les informations de sources ouvertes (ISO) vers les entités spécialisées des états-majors. Les SIC contribuent également aux étapes d'exploitation et de diffusion du cycle de renseignement.

SIC et GE (cf. DIA-3.6_Guerelec)

A13. La maîtrise de l'espace électromagnétique étant un des facteurs de succès d'une opération, une coordination étroite des SIC avec les acteurs GE et ROEM est nécessaire. Si la guerre électronique et le ROEM mettent en œuvre des capacités complémentaires, ils diffèrent par leur subordination dans la conduite et l'exploitation : le ROEM est du ressort du J2 et la GE du J3. La coordination avec les SIC est un enjeu pour éviter des dysfonctionnements préjudiciables à la bonne conduite des opérations, dans la mesure où la gestion du spectre électromagnétique de bataille (*Battle Spectrum Management*) impose un suivi technique unique de la part du *frequency manager officer.*

A14. La mise en place au niveau opératif d'un *SEWOC* (*SIGINT and Electronic Warfare Operations Center*) en charge de la coordination GE et ROEM doit faciliter la prise en compte du *BSM* avec le J6 (cf. § 445).

A15. Le *SEWOC* :

a. Coordonne les ressources consacrées à la GE et au ROEM dans le cadre d'une opération dans laquelle des moyens dévolus à ces deux missions sont déployés ;

b. Pilote les échanges techniques nécessaires entre le ROEM et la GE.

A16. Le CCMO SIC assumera la supervision du spectre électromagnétique en prenant en compte les besoins exprimés par le *SEWOC*.

SIC et soutien (cf. DIA-4_Soutien des opérations)

Les SIC au profit des 13 sous-fonctions du soutien

A17. Outre les Systèmes d'information opérationnels et de communication (SIOC) indispensables à la conduite des opérations, le soutien doit s'appuyer sur les SIC à travers :

a. Les systèmes d'administration et de gestion (SIAG) et les Systèmes d'information scientifiques et techniques (SIST). Les SIAG et les SIST ne sont pas inclus dans le périmètre de la DIA 6, n'étant pas du ressort de la chaîne opérationnelle.

b. Les Systèmes d'information logistiques (SIL), sous-catégorie des SIOC. Les SIL sont adaptés à chaque sous-fonction logistique et obéissent à un besoin croissant d'intégration (SILCENT[105] puis SILRIA[106], SIM@T[107], ATAMS/COMP@S, PERICLES et CHORUS pour la DIRCOM, XERUS pour la prévôté...). Certains SIL aéronautiques sont particulièrement dimensionnant pour les opérations (AMASIS, COMPAS, HARPAGON). Il faut également rechercher de plus en plus la compatibilité avec les systèmes de l'OTAN (*LOGFAS*, *OLCM*, *ADAMS*…).

A18. Les systèmes d'arme récents génèrent des paramètres informatiques spécifiques à leur logistique et à leur maintenance ; le soutien est effectué à partir de données ou de configurations connues par les forces en métropole, voire par les constructeurs, ce qui impose une connexion régulière à un techno-centre à distance. Cette modalité est une contrainte supplémentaire pour les SIC puisqu'il s'agit, notamment en opération mais également en exercices, de prévoir des flux d'informations spécifiques supplémentaires. Ainsi la plupart des systèmes logistiques et en particulier ceux liés à la mise en œuvre d'aéronefs (comme AMSIS/ATAMS et HARPAGON pour le Rafale, ou CINDY/TAURUS pour le drone Harfang) génèrent désormais des transferts de données parfois volumineux, mais essentiels pour le suivi de maintenance des appareils, dont la disponibilité peut être affectée si le Système d'Information Logistique et Technique (SILT) ne peut tenir à jour des données de maintenance.

[105] SILCENT : Système d'information logistique central.
[106] SILRIA : Système d'information logistique pour le suivi de la ressource interarmées.
[107] SIMAT : Système d'information de la maintenance de l'armée de terre.

A19. Les SIOC intègrent déjà et intégreront de plus en plus de données relatives au soutien (disponibilité des matériels, état des stocks de munitions, état des effectifs…) afin notamment de bâtir une vision opérationnelle partagée. De même, des SIAG comme *Chorus* (interministériel), ou *Rhapsodie/Orchestra* pour les RH ou les finances, sont déployés sur les théâtres d'opération ou sur les bâtiments à la mer, ce qui nécessite l'augmentation de liaisons informatiques, afin d'assurer la continuité des flux financiers et informationnels.

A20. La sous-fonction logistique Condition du Personnel en Opération (CPO) fait également appel à la mise en œuvre de SIC (internet à des fins privés, objet de la PIA 4.0.1.1) à partir de ressources militaires ou de la nation hôte. Le soutien santé doit également être pris en compte lors de l'élaboration des architectures SIC, notamment si des solutions telles que la télémédecine sont privilégiées. Il en va de même pour l'ensemble des 13 sous-fonctions du soutien, qui nécessitent toutes un recours de plus en plus fréquent aux bases de données et réseaux de métropole lorsqu'elles doivent être assurées sur les théâtres d'opération. Les architectures SIC *reachback* ou en *cloud* sont des solutions techniques permettant de prendre en compte ce type de contraintes.

Les 13 sous-fonctions du soutien au profit des SIC

A21. Le personnel mettant en œuvre les SIC en opération, souvent projeté en individuel, doit bénéficier, à l'instar du personnel des 13 sous-fonctions du soutien moral, religieux, matériel, psychologique ou social ainsi que du soutien administratif et logistique mis en œuvre pour l'ensemble du personnel de la force (cf. DIA-1.0_PERS (2013)).

A22. Le soutien technique et logistique des SIC est un aspect essentiel et mérite une attention particulière des logisticiens, dans la mesure où certains équipements sont en nombre limité et peuvent en cas d'indisponibilité technique fortement pénaliser l'exécution de la mission. Cela est particulièrement sensible notamment pour les navires, dont les ravitaillements en équipements sont limités. Le MCO doit alors être soigneusement étudié entre le théâtre, la DIRISI, les industriels et le CPCO.

A23. Les matériels majeurs SIC doivent être pris en compte dès le début de l'opération (i.e. en phase de conception de la manœuvre logistique) dans le cadre du soutien général de la force (DAL, OAL). A ce titre, une réserve opérationnelle de théâtre (ROT) est mise en place, dont la vocation est de permettre au COMSICIAT d'assurer le soutien du dispositif déployé avec une plus grande réactivité et de satisfaire les besoins urgents en raccordements.

SIC et Info Ops

A24. Les *Info Ops*, sont le processus d'état-major sur lequel s'appuie le commandement des niveaux opératif et tactiques pour mettre en œuvre la SMI (stratégie militaire d'influence) que le niveau stratégique a définie pour l'opération en cours.

A25. La structure SIC au profit du processus *Info Ops* et de ses contributeurs doit pouvoir se déployer à partir du territoire national et monter à pleine capacité opérationnelle dès la phase de préparation de l'opération.

A26. **SIC et processus *Info Ops*** : de même que les autres contributeurs, les SIC sont intégrés dans le processus de définition des effets comme dans la conduite des actions, et de leur évaluation.

a. Ainsi, si un effet est de développer au maximum la coordination avec tel acteur civil, dans telle zone, pendant telle phase, les SIC seront invités, dans le cadre du processus *Info Ops*, à proposer des solutions de liaison avec cet acteur qui permettent de réaliser l'effet dans le respect des contraintes techniques et SSI en vigueur.

b. En outre, si la planification retient l'utilisation de la déception comme mode d'action dans une phase de l'opération, les SIC pourraient être sollicités par exemple, pour élaborer une structure SIC fictive, cette structure étant totalement disjointe des réseaux SIC opérationnels pour des questions de respect des règlementations SSI.

(1) Celle-ci aura pour but de permettre à une cible/un acteur, de s'introduire sur un réseau défini et lui-même circonscrit, pour s'emparer d'une information qui sera à la base de l'intoxication de cet acteur, concourant à la réalisation de l'effet de déception.

(2) Cependant, le montage d'une telle structure temporaire ne pourra se faire que sous condition de ressources disponibles, aux ordres du responsable SIC concerné.

A27. **SIC et contributeurs APEO** : les APEO (*CIMIC, COMOPS, OMI/PSYOPS*, *KLE, ASI*)[108] ont des besoins spécifiques en termes de SIC qui seront exprimés au J6 :

a. Accès internet nombreux :

(1) Pour l'exploitation des sources ouvertes ;

(2) Pour l'animation des réseaux sociaux de la force, et l'intervention sur les réseaux sociaux publics,

b. Besoins en logiciels spécifiques, selon les règles SSI en y incluant les règles de cyber sécurité ;

c. Besoins importants en bande passante vers la métropole pour assure le *reachback* – ou « retour-métropole » (analyse et production médias, que ce soit la COMOPS ou les OMI/PSYOPS). Ce besoin sera pris en compte par le J6 dans le cadre de la planification et l'étude des besoins en bande passante sera incluse dans l'étude et le suivi permanent au même titre que les autres composantes (Renseignement, logistique…) ;

d. Besoins en fréquences des moyens radios OMI/*PSYOPS* : le J6/ *frequency manager* étudiera ces besoins et la compatibilité avec les plans de fréquences disponibles. Seul, le J6 est habilité à attribuer les fréquences sur un théâtre, à l'exclusion de toute autre entité ;

e. Besoins en liaison des DL CIMIC auprès d'entités n'appartenant pas à la force (OI, ONG), et définition de règles d'accès à certains SI dans le cadre du respect des règles de confidentialité émises par le commandement en prévoyant la séparation physique des réseaux susceptibles d'être alors utilisés.

A28. En phase de projection, il conviendra de veiller à la bonne prise en compte des besoins SIC de la COMOPS, en particulier pour répondre à la forte demande en images entre le théâtre et la métropole destinées aux médias.

A29. L'utilisation croissante d'Internet dans le cadre du processus *Info Ops* ne doit pas faire oublier d'une part les règles de sécurité déjà explicitées, mais également la responsabilité des utilisateurs. Le commandement sur le théâtre, sur avis du COMSIC IAT, doit pouvoir à tout moment, veiller à l'intégrité de ces réseaux contractualisés et peut en restreindre l'usage si la sécurité de la force est engagée.

[108] Cf. DIA 3.10

(PAGE VIERGE)

Annexe B
Demande d'incorporation des amendements

B01. Le lecteur d'un document de référence interarmées ayant relevé des erreurs, des coquilles, des fautes de français ou ayant des remarques ou des suggestions à formuler pour améliorer sa teneur, peut saisir le CICDE en les faisant parvenir (sur le modèle du tableau ci-dessous) au :

CICDE
École militaire
21, Place JOFFRE – BP 31
75700 PARIS SP 07

ou en ligne, sur les sites Intradef (http://www.portail-cicde.intradef.gouv.fr) et internet (http://www.cicde.defense.gouv.fr) du CICDE.

N°	Origine	Paragraphe (n°)	Sous-paragraphe	Ligne	Commentaire
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					

B02. Les amendements validés par le Directeur du CICDE seront répertoriés **en rouge** dans le tableau intitulé *« Récapitulatif des amendements »* figurant en page 7 de la version électronique du document.

(PAGE VIERGE)

Annexe C
Lexique

Partie I – Sigles, acronymes et abréviations

Sigles

C01. Dans un sigle, chaque lettre se prononce distinctement comme si un point la séparait de la suivante.

Acronymes

C02. Un acronyme se compose d'une ou de plusieurs syllabes pouvant se prononcer comme un mot à part entière.

Abréviations

C03. Ce lexique ne prend en compte que les abréviations conventionnelles telles que définies dans le *Lexique des règles typographiques en usage à l'imprimerie nationale (*LRTUIN), pages 5 à 11.

Charte graphique du lexique

C04. Dans ce lexique, tous les caractères composant un sigle, un acronyme ou une abréviation sont écrits en lettres capitales afin que le lecteur puisse en mémoriser la signification.

C05. Les sigles, acronymes et abréviations d'origine française sont écrits en **Arial gras, taille 9, caractères romains, couleur rouge**. Les sigles, acronymes et abréviations d'origine étrangère ou antique sont écrits en ***Arial gras, taille 9, caractères italiques, couleur bleue***.

Liste des sigles, acronymes et abréviations utilisés dans ce document

AAP	*Allied Administrative Publication*
ACSSI	Article Contrôlé de la Sécurité des Systèmes d'Information
AJP	*Allied Joint Publication*/Publication interarmées interalliée
AMASIS	*Aircraft Maintenance And Spare Information System*
ALFAN	Amiral Commandant la Force D'Action Navale
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ALI	*Air Land Interdiction*
BAP	Base Aérienne Projetable
BTAC	Brigade de Transmissions et d'Appui au Commandement
BG	*Battle Group*
BSM	*Battle Spectrum Management*
CALID	Centre d'Analyse en Lutte Informatique Défensive
CAOC	*Combined Air Operation Center*
CCMO	Centre de Coordination et de Mise en Oeuvre
CEMA	Chef d'État-Major des Armées
C2	*Command and Control*
CERT	*Computer Emergency Response Team*
CG	Centre de Gestion
CHF	Chaîne Hertzienne du Futur
CICoS	Centre interarmées de coordination du soutien
CIS	*Communication Information System (SIC)*
CMI	Cellule Maîtrise de l'information
CMO	Centre de Mise en Œuvre
CNMO	Centre National de mise en œuvre
CNSO	Centre National de Soutien Opérationnel
CO	Centre opérations
COD	Centre Opérationnel de la DIRISI

COMSEC	*Communication Security*
COMSICIAT	COMmandant des SIC InterArmées de Théâtre
COMPUSEC	*Computer Security*
COP	*Common Operational Picture*
COTS	*Commercial off-the Shelf*
CP	*Command Post*
CPCO	Centre de Planification et de Conduite des Opérations
CSFA	Commandement du Soutien des Forces Aériennes
DCISM	*Deployable CIS Module*
DIP	Directive Initiale de Planification
DIRISI	Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information
DL	Détachement de Liaison
DNS	*Domaine Name System*
DOB	*Deployable Operational Base*
EDA	Economat des Armées
EM	Etat-Major
EMA	État-Major des Armées
EMIA-FE	Etat-Major InterArmées de Forces et d'Entraînement
EMF	Etat-Major de Force
EMO	Etat-Major Opérationnel
EW	*Electronic Warfare*
FAI	Fournisseur d'accès internet
FHQ	*Forward Headquarters*
FMN	*Federated Mission Network*
FMV	*Full Motion Video*
GE	Guerre Electronique
GSM	*Global System for mobile Communications*
GT SIC Aero	Groupement tactique des SIC aéronautiques
GTRS	Groupement Transmissions
HD (station)	Haut Débit (station)
HQ	*HeadQuarters*
ICO	*Interface Control Officer*
IDP	*Information Dissemination Plan*
IEG	*Information Exchange Gateway*
IER	*Information Exchange Requirement*
IMO	*Info Management Officer*
INCON	*Information Control*
INPT	Infrastructure Nationale Partageable des Transmissions
IP	*Internet Protocol*
JFACC	*Joint Forces Air Component Commander*
JICO	*Joint Interface Control Officer*
JRE	*Joint Range Extension*
JTS	*Joint Targeting System*
KD	*Knowledge Development*
LAN	*Local Area Network / réseau local IP*
LCC	*Land Component Command*
LICOP	Liaison de Commandement Protégée
LDT	Liaison de Données Tactiques
LID	Lutte Informatique Défensive
MCC	*Maritime Component Command*
MCI	*Mission Critical Information*
MICO	*Maritime Interface Control Officer*
MIDS	*Multifunctional Information Distribution System*
NARFA	*National Allied Radio Frequency Agency*
NCC	*National Contingent Commander*
NEB	Numérisation de l'Espace de Bataille
NRF	*Nato Response Force*
OHQ	*Operations HeadQuarters*
OLID	Officier Lutte Informatique Défensive
OMIT	Organisation Mondiale Interarmées des Télécommunications
OODA	Observation – Orientation –Décision - Action
OPCOM	*Operational Command*
OPCON	*Operational Control*
OSSI	Officier de Sécurité des Systèmes d'Information
OTC	*Officer Tactical Command*
OTIAD	Organisation Territoriale Interarmées de Défense

PCA	Plan de Continuité d'Activité
PCTIA	Poste de Commandement Terre à vocation Interarmées.
PI	Point d'Interconnexion
POIA	Portail des Opérations InterArmées
PPS	Posture Permanente de Sûreté
PSSI	Politique de Sécurité des Systèmes d'Information
PMR	*Private Mobile Radio*
QoS	*Quality of Service*
SC	Système de Commandement
RAP	*Recognized Air Picture*
RDIFF	Réseau de Diffusion
REMO	Réseau de Mobiles
RGP	*Recognized Ground Picture*
RICO	*Regional Interface Control Officer*
RIFAN	Réseau d'Interconnexion de la Force d'Action Navale
RMP	*Recognized Maritime Picture*
RTRAN	Réseau de Transit
ROEM	Renseignement d'Origine Electromagnétique
SD-O	Secret Défense Opérations
SCCOA	Système de Commandement et de Conduite des Opérations Aériennes
SEWOC	*SIGINT and Electronic Warfare Operation Center*
SGTIA	Sous-Groupement Tactique Interarmes
SGTRS	Sous-Groupement Transmissions
SI	Système d'Information
SIA	Système d'Information des Armées
SIAG	Système d'Information d'administration générale
SIC	Système d'Information et de Communication
SIGINT	*Signal Intelligence*
SIL	Système d'Information Logistique
SIST	Système d'Information Scientifique et Technique
SQG	Soutien de Quartier Général
SSI	Sécurité des Systèmes d'Information
SSQG	Soutien Spécialisé de Quartier Général
SSU	Station Sol Utilisateur
TD	Transmissions de Données
TACOM	*Tactical Command*
TACON	*Tactical Control*
THD (station)	Très Haut Débit (station)
VPN	*Virtual Private Network*
VTC	Vidéo Télé Conférence
WAN	*Wide Area Network*
ZPC	Zone de Postes de Commandement

Partie II – Termes et définitions

(Sans objet).

Résumé

DIA-6_SIC-OPS(2014)

1. Intitulée « les SIC en opérations », la DIA 6 a pour objet de présenter l'ensemble du domaine SIC concourant aux opérations.

2. Les SIC s'appuient sur des systèmes de communications allant des satellites de télécommunications jusqu'aux équipements radio équipant les systèmes d'armes, en y associant des moyens fixes et des moyens mobiles.

3. Les SIC couvrent tous les besoins des forces en opérations en déployant une architecture et des systèmes permettant les échanges d'informations et de données, en en garantissant leur sécurité et en contribuant à leur diffusion.

4. Cette DIA, complétant le corpus doctrinal de l'OTAN sur les SIC, a pour ambition de :
Présenter les grands principes des SIC ;
Définir les différents niveaux de responsabilité dans la conception, la mise en œuvre et la conduite des SIC ;
Présenter l'emploi des SIC en opération.

5. Ce document s'adresse principalement à la chaîne opérationnelle interarmées afin de lui apporter les éléments de compréhension nécessaires pour la planification et la conduite des SIC dans le cadre d'une opération.

6. Il permettra en outre au personnel du domaine SIC de mieux appréhender son action au sein de la manœuvre interarmées.

Ce document est un produit réalisé par le Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE), Organisme interarmées (OIA) œuvrant au profit de l'État-major des armées (EMA). Point de contact :

CICDE,
École militaire
21, place JOFFRE
75700 PARIS SP 07

ISBN 978-2-11-138554-2