MINISTERE DE LA DEFENSE

ETAT-MAJOR DE L'ARMEE DE TERRE

COFAT

TTA 150

TITRE VIII

S.I.C.
SYSTEMES D'INFORMATION ET DE COMMUNICATION

Expert de domaine : ESAT

Edition 2008

ANNEXE A - DÉFINITIONS

A.1.1 CENTRE DE TRANSMISSIONS

Le centre de transmissions réunit sous les ordres d'un même chef un certain nombre de moyens, permettant d'assurer dans les meilleures conditions de rapidité, de rendement et de sécurité, les relations nécessaires à un ou plusieurs PC. Il fonctionne 24 heures sur 24 en vraie grandeur.

A.1.2 COMMUTATION

C'est l'ensemble des opérations nécessaires pour mettre en liaison deux abonnés.

A.1.3 COMPOSANTE STRATEGIQUE

L'appellation a deux raisons principales :

➲ le souci d'une homogénéisation avec les appellations OTAN où sont distingués effectivement les systèmes et les équipements stratégiques des systèmes et des équipements tactiques ;

➲ une réalité : les réseaux d'infrastructure constituent une ressource réellement stratégique au profit du haut commandement national ; ils sont conçus, avant tout, pour véhiculer des informations de caractère stratégique au profit du HCN.

A.1.4 CONCESSION

Dans le domaine d'un réseau, une concession est une ressource supports de transmission, qui est, soit attribuée à un réseau ou un organisme n'appartenant pas à l'armée de terre, soit reçue d'un autre réseau ou organisme n'appartenant pas à l'armée de terre.

A.1.5 IMPULSION ÉLECTRO-MAGNETIQUE (IEM)

C'est un phénomène résultant d'une explosion nucléaire. Ses effets sont surtout importants dans le cas d'une explosion exoatmosphérique (c'est-à-dire ayant eu lieu en haute altitude).Cette onde électromagnétique très brève entraîne de manière irrémédiable d'importants dégâts sur les matériels électriques, électroniques et, par voie de conséquence, informatiques. Pour envisager une bonne protection pour un système de transmissions, il faut donc protéger les fonctions vitales qui doivent être assurées pendant et/ou après l'apparition de l'IEM : c'est ce que l'on appelle durcir un équipement ou un système à l'IEM.

A.1.6 INTEROPERABILITE

Réaliser l'interopérabilité consiste à faire travailler ensemble des personnels :

- ➲ dont les missions, les mentalités et les cultures sont la plupart du temps différentes sinon divergentes ;
- ➲ qui utilisent le plus souvent des langages (écrit, parlé et informatique) non directement « compatibles » et des moyens de télécommunications disparates.

Elle est obtenue dès lors que sont remplies les conditions qui permettent aux équipements électroniques de transmissions d'assurer l'échange direct et de façon satisfaisante, d'information ou de service entre eux et/ou leurs utilisateurs.

Cinq niveaux d'interopérabilité ont été définis par l'OTAN. Ils peuvent être ainsi résumés :

- ➲ niveau 1 : interopérabilité manuelle, par le truchement des opérateurs de chacun des systèmes avec « rupture de charge » (ex. : téléphone) ;
- ➲ niveau 2 : échange de détachements de liaison (DL) équipés de terminaux d'entréesortie propres à chaque système ;
- ➲ niveau 3 : identique au niveau 2 mais chaque DL dispose en outre de moyens de traitement informatiques propres plus ou moins puissants ;
- ➲ niveau 4 : interopérabilité technique de système à système par le truchement d'une boîte d'interface automatique permettant le passage d'information présélectionnée ;
- ➲ niveau 5 : interopérabilité technique totale de système à système, mais restriction d'échanges entre bases de données.

A.1.7 RESEAU

Un réseau est un ensemble d'éléments interconnectés, c'est-à-dire de supports et d'équipements matériels reliant des terminaux les uns aux autres et acheminant des signaux vers leurs destinataires. Pour l'usager, le réseau se caractérise essentiellement par le service qu'il rend. Ainsi le Réseau Téléphonique Commuté (RTC) est le moyen d'acheminer les communications téléphoniques.

Réseau de transport : c'est un réseau réel, physiquement composé d'artères de transmissions et de commutateurs.

Réseau de desserte : par opposition à un réseau de transport, un réseau d'abonné (de desserte) est virtuel ; il offre aux abonnés divers services (téléphonie, télégraphie, télécopie...).

A.1.8 SYSTEME D'INFORMATION

C'est un ensemble structuré et cohérent de ressources (humaines, organisationnelles, techniques et financières) et de procédures, qui permet de recevoir, traiter, stocker et communiquer en temps opportun les données adéquates pour que le chef interarmes puisse prendre des décisions et conduire des actions.

A.1.9 SUPPORTS

Ils permettent l'acheminement de signaux. Différents supports sont utilisés, ils sont complémentaires. Toute communication établie entre deux usagers peut emprunter successivement plusieurs supports de différentes natures, tels que :

➲ *Ligne téléphonique :* constituée de deux fils en cuivre, isolés dans des plastiques et regroupés dans des câbles. Ces derniers peuvent être aériens ou enterrés, selon le cas.

➲ *Radio :* utilisation d'une fréquence modulée par l'information (soit en amplitude, soit en fréquence) ; fonctionnement en point à point ou en réseau. La portée est fonction de la fréquence, de la puissance de l'émetteur et de l'antenne. La qualité est fonction du temps.

➲ *Faisceau hertzien :* faisceau radio dirigé, contenant plusieurs informations, grâce à un système multiplex (à répartition en fréquence ou dans le temps). Les faisceaux hertziens fonctionnent en point à point et en duplex.

➲ *Fibre optique :* c'est un « cheveu de verre » fabriqué à partir de la silice. Il est parcouru par un rayon lumineux codé en fonction du signal à transmettre. La fibre est insensible aux différents parasites d'origine électrique ou magnétique. Ses performances permettent le transport d'un volume très important d'informations de toute nature et à débit élevé.

➲ *Satellite de télécommunications :* placé en orbite géostationnaire à 36 000 km d'altitude, il retransmet les ondes radioélectriques provenant des stations d'émission vers les stations de réception. Un satellite permet de couvrir environ un tiers de la surface du globe en s'affranchissant du terrain.

ANNEXE B - ABRÉVIATIONS

CGN Centre de Gestion National.

CGZ Centre de Gestion de Zone.

CNSST Centre National de Soutien Spécialisé des Transmissions.

COMFOR COMmandement des FORces.

COMTRANS COMmandant des TRANSmissions.

CREDO Conception, Réalisation, Étude D'Organisation.

DAT Détachement Autonome des Transmissions.

EIT Ensemble Interarmées de Transmissions.

HCN Haut Commandement National.

HF Hautes Fréquences.

IEM Impulsion ÉlectroMagnétique.

OMIT Organisation Mondiale Interarmées des Transmissions.

PATRI PATRImoine.

RNIS Réseau Numérique à Intégration de Services.

ROEM Renseignement d'Origine ÉlectroMagnétique.

SIRIUS Système Informatique des Ravitaillements Intégré et Unique au Service.

SITRANS Système d'Information des TRANSmissions.

SOCRATE Système Opérationnel Constitué des Réseaux de l'Armée pour les TÉlécommunications.

SSI Sécurité des Systèmes d’Information.

SYRACUSE SYstème de RAdio Communications Utilisant un SatellitE.

TAM Traitement Automatisé des Messages.

TEI Télécommunications Et Informatique.

SECTION I - GENERALITES SUR LA RADIOTELEPHONIE

BUT RECHERCHÉ ET DONNÉES ESSENTIELLES	Cette section vise à faire acquérir au sous-officier les connaissances générales nécessaires à l'utilisation des postes radioélectriques au combat.
RÉFÉRENCE(S)	TTA 188.
CONSEILS POUR ABORDER L'ÉTUDE	Cette étude théorique devra être complétée par un maximum d'exercices pratiques sur le terrain.

Chapitre 1 - PRINCIPES D’ETABLISSEMENT D’UNE BONNE LIAISON

1- L’EMPLACEMENT

Les principes suivants sont à respecter pour tous les postes. Ils s'appliquent à :

- ➲ L’emplacement ;
- ➲ L’antenne ;
- ➲ Les connecteurs.

L'emplacement est d'une très grande importance pour la qualité de la liaison. Compte tenu de la situation du moment, il convient de rechercher :

- ➲ Les points hauts (sommets de collines, bâtiments) ;
- ➲ Les terrains dégagés (plats ou faiblement ondulés).

Les meilleures conditions se trouvent réunies quand la liaison est prise à « vue directe » entre les correspondants. Il convient d'éviter :

- ➲ Les forêts et agglomérations ;
- ➲ Les fonds de thalwegs ;
- ➲ La proximité des lignes à hautes tensions ;
- ➲ La proximité des masses métalliques (ponts, hangars) ;
- ➲ La proximité des bâtiments importants.

En choisissant son emplacement, l’opérateur n’oubliera pas qu’il doit aussi camoufler son antenne.

2- L’ANTENNE

L'antenne doit être installée avant de mettre le poste en marche sous peine de le détériorer. Elle est maintenue verticale.

Si l'unité collective comprend deux antennes, une seule est installée en fonction de l'utilisation du moment (à terre ou à dos) mais en se souvenant que la portée est nettement réduite avec l'antenne courte.

3 - LES CONNECTEURS

Les connecteurs constituent les points délicats de tous les postes radio. Poussières, graviers et brindilles sont soigneusement retirés avant tout branchement (embase d'antenne, filetage de l'antenne, connecteur et prise de combiné).

L'humidité provoque souvent de mauvais contacts. Les connecteurs sont donc séchés avec un chiffon propre. Par temps de pluie, l'embase d'antenne est fréquemment essuyée.

Tout ce qui se visse doit être serré au maximum.

Chapitre 2 - LES RÈGLES DE SÉCURITÉ

1 - PRISE DE TERRE

Dans toutes les installations, relier à la terre les bâtis et pièces conductrices des appareils.

Relier à la terre les stations et groupes électrogènes.

Il est interdit de placer parallèlement lignes électriques et lignes téléphoniques.

2 - ANTENNES

Ne jamais toucher une antenne lorsque le poste radio est en « émission ».

Sur les moyens grande puissance (diffuseur d'alerte, radio télétype grande puissance TRCT 2), contrôler fréquemment les sécurités.

Lors d'un déplacement, les antennes de véhicules doivent être haubanées. En cas de transport par voie ferrée, elles doivent être démontées.

3 - INCENDIE

En cas d'incendie, utiliser les extincteurs appropriés.

➲ Huile, essence des groupes électrogènes → extincteur à poudre.

➲ Incendies électriques dus aux courts-circuits → extincteur à neige carbonique.

4 - IMPLANTATIONS

➲ Reconnaissance obligatoire du poste téléphonique le plus proche (privé ou public).

➲ Reconnaissance des points d'implantation de jour obligatoirement.

➲ Les antennes doivent être placées à une distance des lignes électriques au moins égale à deux fois leur hauteur.

➲ L'air ambiant des stations techniques doit être renouvelé par ventilation forcée ou par ouverture fréquente de la porte (toutes les demi-heures).

➲ Présence obligatoire des flexibles d'évacuation des gaz brûlés sur les groupes électrogènes.

➲ Bivouacs ou lieux de repos interdits à moins de 25 m des groupes électrogènes bimoteurs, qui par ailleurs ne doivent pas être placés sous le vent par rapport à la troupe.

➲ Interdiction d'utiliser les chauffages radiants dans les enceintes fermées.

sECTION II - LA PROCEDURE RADIOTELEPHONIQUE

BUT RECHERCHÉ ET DONNÉES ESSENTIELLES	La procédure radiotéléphonique a pour but de fixer la forme et la succession des différentes parties d'une conversation ou d'un message devant être acheminé par un moyen de transmission.
RÉFÉRENCE(S)	TTA 188 – TRS 121.
CONSEILS POUR ABORDER L'ÉTUDE	Effectuer le plus grand nombre d'applications pratiques dans le cadre d'exercices de réseau.

Les règles de procédure visent à :

- ➲ Conserver l'EXACTITUDE du texte ;
- ➲ Favoriser la RAPIDITÉ de la transmission ;
- ➲ Assurer la SÉCURITÉ de celle-ci.
-

L'inobservation de ces règles, toute divergence ou fantaisie sont à proscrire car :

- ➲ Elles créent la confusion ;
- ➲ Elles réduisent l’efficacité et la rapidité ;
- ➲ Elles sont causes d’indiscrétion.

Chapitre 1 - DEFINITIONS

1 - STATION RADIO

Appareil ou ensemble d'équipements radio assurant la liaison dans le cadre d'un réseau.

2 - STATION DIRECTRICE

Station qui dessert, en principe, la plus haute autorité. Elle est chargée de faire appliquer les règles de procédure.

3 - RÉSEAU

Ensemble de stations travaillant entre elles suivant les mêmes caractéristiques d'exploitation (fréquence, régime).

3 1. Réseau dirigé :

Le réseau est dit « dirigé » lorsque les stations secondaires doivent obtenir l'autorisation de la station émettrice avant de communiquer entre elles.

3 2. Réseau libre :

Le réseau est dit « libre » lorsque les stations peuvent communiquer entre elles sans autorisation préalable de la station directrice.

4 - INDICATIF

Appellation ou symbole destiné à identifier :

- ➲ une station (indicatif d'appel) ;
- ➲ une autorité (indicatif d'autorité) ;
- ➲ un réseau (indicatif collectif).

4 1. Remarque :

Actuellement, les textes en vigueur prescrivent l'emploi d'indicatifs radio tétragrammes en remplacement des systèmes précédemment utilisés : trigrammes, mots conventionnels, couleurs, etc.

4 2. Exemple :

- indicatif du 4e RI : 83 BZ ;
- indicatif de la 1re Cie du 4e RI : 4 KOF.

Il est interdit de confectionner des indicatifs dérivés à partir de ces tétragrammes. Un indicatif particulier est assigné à chacun des postes radio.

Les quatre caractères formant l'indicatif sont obligatoirement transmis lors de la première prise de contact et, par la suite, aussi souvent que cela est nécessaire. En cas de procédure simplifiée, le dernier bigramme, ou même le dernier caractère, peuvent être utilisés seuls, dans la mesure où cette manière de procéder n'est pas susceptible de provoquer des confusions.

Les indicatifs « phonie » sont transmis en épelant les lettres et chiffres qui les composent au moyen de l'alphabet phonétique réglementaire.

ALTERNAT : système de communication permettant alternativement l'émission ou la réception d'informations. Ce système utilise une seule fréquence.

DUPLEX : système de communication permettant simultanément l'émission et la réception d'informations. Ce système nécessite l'utilisation de deux fréquences.

Chapitre 2 - L'ALPHABET PHONÉTIQUE

Quand il est nécessaire d'identifier une lettre de l'alphabet, on emploie l'alphabet phonétique suivant :

LETTRE	ÉPELLATION	PRONONCIATION figurée	LETTRE	ÉPELLATION	PRONONCIATION figurée
A	ALFA	AL-FA	N	NOVEMBER	NO-VEM-BER
B	BRAVO	BRA-VO	O	OSCAR	OSS-KAR
C	CHARLIE	CHAR-LI	P	PAPA	PAH-PAH
D	DELTA	DEL-TAH	Q	QUEBEC	KE-BEK
E	ECHO	EK-O	R	ROMEO	RO-MI-O
F	FOX-TROT	FOX-TROTT	S	SIERRA	Sl-ER-RAH
G	GOLF	GOLF	T	TANGO	TANG-GO
H	HOTEL	HO-TEL	U	UNIFORM	YOU-NI-FORM
I	INDIA	INE-DIAH	V	VICTOR	VIK-TOR
J	JULIETT	DJOU-LI-ETT	W	WHISKY	OUISS-KI
K	KILO	Kl-LO	X	X-RAY	IKSS-RE
L	LIMA	Ll-MAH	Y	YANKEE	YANG-KI
M	MIKE	MAIK	Z	ZULU	ZOU-LOU

Exemple :

Transmettre le message : « Effectuer TIR ROUGE sur EXIREUIL. »

Dire : « Effectuer TIR ROUGE sur EXIREUIL – j'épelle : Echo, XRay, India, Roméo, Echo, Uniform, India, Lima, EXIREUIL. »

Si le mot n'est pas prononçable, par exemple : « Rendez-vous en XP-TZ-DC-YK. »

Dire : « Rendez-vous en – j'épelle : Ray, Papa...

1 - Prononciation des nombres

Quand les nombres sont transmis en radiotéléphonie, appliquer, pour leur prononciation, les règles suivantes :

- 0 = Zéro ;
- 1 = Un (tout seul) ;
- 2 = Deux (un et un) ;
- 3 = Troua (deux et un) ;
- 4 = Katre (deux fois deux) ;
- 5 = Cinque (trois et deux) ;
- 6 = Sisse (deux fois trois) ;
- 7 = Sète (quatre et trois) ;
- 8 = Huit (deux fois quatre) ;
- 9 = Neufe (cinq et quatre).

Exemple. Transmettre : 1965.

Dire : « 1965 – j'épelle : Un (tout seul) – Neufe (cinq et quatre) – Sisse (deux fois trois) – Cinque (trois et deux), 1965. »

2 - Virgule

La virgule doit être prononcée Virgule.

Exemple. Transmettre : 123,4.

Dire : « 123,4 – j'épelle : Un – Deux – Troua – Vir-Gu-Le –Katre.»

3 - Séparatif

Exemple. Transmettre les coordonnées suivantes : 365-487.

Dire : « 365-487 – j'épelle : Troua – Sisse – Cinque – Sé-Pa- Ra-Tif – Katre – Huite – Sète. »

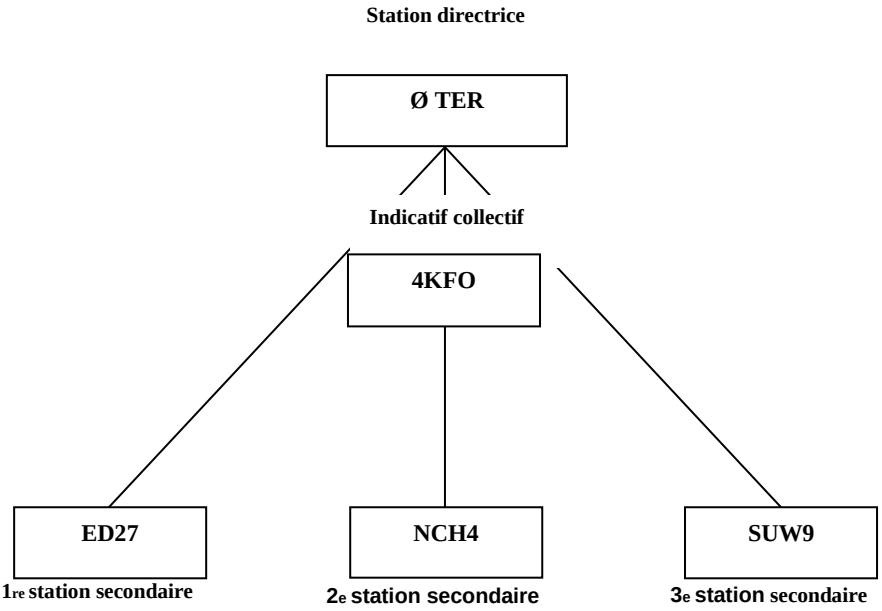
Chapitre 3 - LES RÈGLES D’EXPLOITATION

1 - TELEPHONIE

OPÉRATION à effectuer	DIRE à l'émission	ENTENDRE à la réception
Appeler un abonné.	Donnez-moi	Donnez-moi... – tel bureau ; – tel service ; – tel capitaine. Ne pas crier au téléphone: parler NORMALEMENT. Ne pas s'absenter avant d'avoir obtenu la communication demandée.
Répondre à un appel.	Ici, sergent X... de telle compagnie, sergent de semaine (ou : chef de poste, ou : fourrier, etc.).Se présenter dis-tinc-tementen indiquant : grade, nom, fonction.	Allô ! Allô ! j'écoute. ou : poste n°... j'écoute.
Nota. – En téléphonie les règles concernant la transmission de messages sont identiques à celles de la radiotéléphonie.		

2 - RADIOTÉLÉPHONIE

Schéma de réseau illustrant les exemples ci-après :



Exemples :

OPÉRATION à effectuer	DIRE à l'émission	ENTENDRE à la réception
Prise de contact. S'effectue avant d'entreprendre un trafic régulier pour s'informer de la qualité des liaisons.	4 KFO – Ici 0/TER – *Contrôle radio – Parlez* .... 4KFO – Ici 0/TER – *Reçu – Terminé.*	Ici EDZ7 – *Reçu – Parlez.* Ici NCH4 – Fort et lisible – *Parlez.* Ici SUW9 – Assez fort et clair – *Parlez.* Appréciation *Force et Lisibilité des signaux :* fort, clair, assez fort, lisible, faible, déformé, très faible, avec interférence.
Appel préliminaire. Outre la « prise de contact », il peut être nécessaire de s'assurer que le correspondant est à l'écoute.	Z7 – Ici HA – *Parlez* .... Ici H4 (transmission de la communication).	Ici Z7 – *Parlez.*
Annonce d'un message. Avant de transmettre un message à un correspondant, il vaut mieux l'annoncer au préalable.	W9 – Ici Z7 – *Prenez message – Parlez* ..... Ou : *J'ai un message* (suivi de l'urgence du message) – *Parlez*..... ... Ici Z7 – *Prenez message,* etc.	Il y a deux cas : 1. Si W9 n'est pas prêt, dire : Ici W9 – *Attendez.* 2. Si W9 est prêt à recevoir le message : Ici W9 – *Envoyez votre message – Parlez*.
Réglage du réseau. S'effectue avant d'entreprendre un trafic, pour s'assurer que toutes les stations secondaires sont réglées sur la même fréquence.	4KFO – 4KFO – Ici 0/TER – ici 0/TER – *Je vais transmettre pour réglage* – 0/TER – 0/TER – 0/TER ..... *Terminé*	Les stations secondaires ne répondent rien, mais se règlent pour un maximum de réception. La station directrice répète ainsi son propre indicatif durant 20 secondes environ, puis elle garde la manette du combiné appuyée durant 10 secondes environ. *Fin* de l'émission de réglage.
Ouverture de réseau. S'effectue après le « réglage de réseau ». La station directrice s'assure ainsi de la qualité des liaisons et du bon réglage des appareils.	4KFO – Ici 0/TER – *Contrôle radio – Parlez* ..... *Idem* « Prise de contact ».	Chaque station secondaire répond dans l'ordre qui lui a été assigné. Si l'une des stations ne répond pas, la station suivante attend environ 15 secondes avant d'émettre sa propre réponse.
Accusé de réception. S'effectue à l'issue de la transmission d'un message pour assurer un correspondant que son message a été bien reçu.	Z7 – Ici W9 – *Reçu – Parlez*	Ici Z7 – *Terminé.*
Demande de répétition.	Z7 – Ici W9 – *Répétez..* .– tout avant tel mot ;– tout après tel mot ; – le mot avant tel mot ; – le mot après tel mot, etc. *Parlez*	Ici Z7 – *Je répète...* – tout avant tel mot ; – tout après tel mot, etc. – *Parlez.*
Demande de collationnement. S'effectue à l'issue de la transmission d'un message pour s'assurer que le correspondant a bien reçu ce message.	W9 – *Collationnez – Parlez .....* ... Ici Z7 – *Correct – Terminé.*	Ici W9 – *Je collationne (elle répète intégralement la dernière transmission) – Parlez.*
Nota. – La procédure prescrite ci-dessus ne fixe que quelques règles de base. L'initiative et le bon sens permettent, en général, de régler les cas particuliers.		

Chapitre 4 - LE MESSAGE

1 - COMPOSITION

Le message est un texte rédigé par une autorité et transcrit sur des formulaires (petit ou grand format).

Le message comprend trois parties :

- ➲ l'en-tête,
- ➲ le texte,
- ➲ le final.

L'en-tête et le final comportent un certain nombre de composants. Ils facilitent l'écoulement du trafic.

Les parties, composants et éléments, ont une disposition et un ordre de succession réglementaires que doivent parfaitement connaître les opérateurs radio.

2 - DIAGRAMME SCHÉMATIQUE DU MESSAGE

PARTIES	COMPOSANTS	ÉLÉMENTS	CONTENUS
En-tête	Procédure d'en-tête	Appel ..... Invitation à prendre message	Hôtel 4 Whisky 9 ici Zoulou 7. Prenez message.
	Préambule	Urgence ..... GDH (groupe date-heure)	*Exemple :* urgent. *Exemple :* groupe date-heure : 21 (date), 07 (heure), 30 (minutes), A (fuseau).
	Adresse	*a*. Autorité légale ..... *b.* Autorités destinataires	*Exemple :* FROM = Écho Delta Zoulou 7. (Pour Action) TO = Sierra Uniform Whisky 9. (Pour information) INFO = November Charlie Hôtel 4.
Séparation			Terme de procédure placé *avant* (et après) le texte.
Texte	–	–	*Exemple :* Arrivée AS – RA – WB – Stop. Envoyer élément renfort avant la nuit.
Séparation			Terme de procédure placé *avant* (et après) le texte.
Final	Procédure finale	Instructions finales ..... Indication de fin d'émission	*Exemple :* Collationnez. Transmettez à ... *Exemple :* Parlez. Ou : Terminé.

Remarques :

Les parties suivantes sont rédigées par les autorités :

- Urgence ;
- Adresse (en clair) ;
- Groupe date-heure ;
- Texte.
-

Ces parties-là sont intangibles.

Les autres parties, dans les petites unités, sont rédigées par les opérateurs. Elles constituent le conditionnement du message.

3 - CONDITIONNEMENT DU MESSAGE

C'est l'opération qui consiste à ajouter au texte, rédigé par une autorité, les indications nécessaires à l'acheminement du message.

3 1. L’appel :

L'appel consiste à appeler la (ou les) station(s) desservant les autorités destinataires du message (destinataires pour « action » et pour « information »).

3 2. L’urgence :

L'urgence est toujours portée par l'autorité qui rédige le message. Pour le conditionnement, il s'agit seulement de recopier l'indication portée.

Les différents degrés d'urgence sont :

- ➲ FLASH ;
- ➲ IMMÉDIAT ;
- ➲ URGENT ;
- ➲ ROUTINE.

Nota. – Avec le « degré d'urgence » l'autorité mentionne également la classification du message (degré de protection). Celui-ci n'est pas transmis en radiotéléphonie.

3 3. Le groupe date-heure :

Le groupe date-heure se compose de six chiffres et d'une lettre.

Exemple : 21 (date) 07 (heures) 30 (minutes) A (lettre fuseau horaire).

Le groupe date-heure indique le jour et l'heure à laquelle le message a été approuvé par l'autorité origine.

3 4. L’adresse :

L'adresse comprend :

- l'autorité origine, c'est-à-dire celle qui a rédigé le message (FM) ;
- l'(ou les) autorité(s) destinataire(s) pour « ACTION » (TO) ;
- l'(ou les) autorité(s) destinataire(s) pour « INFO ».

Si l'adresse du message est portée en clair lors du conditionnement, l'opérateur remplacera les autorités ou les unités désignées par leur indicatif respectif.

Il est entendu que certains messages peuvent ne comporter que des destinataires « pour action » ou même uniquement des destinataires « pour information ».

Chapitre 5 - LA COMMUNICATION D’AUTORITÉ

Aux petits échelons, le trafic dans un réseau s'écoule généralement sous forme de communications verbales de chef à chef.

Exemple : un chef de section demande un tir d'appui au

PC de la compagnie. Il dira :

« Zoulou 7 ici Écho 1. Effectuer tir rouge sur Exireuil. Parlez ».

1 - COMPOSITION

La communication d'autorité peut se diviser en trois parties :

- L'appel ;
- La conversation proprement dite ;
- Le final.

1 1. L’appel :

La communication débute toujours par un appel.

Exemple : « Zoulou 7 ici Écho 1 ». Zoulou 7 est la station appelée. Écho 1 est la station appelante.

1 2. La conversation :

La conversation est la partie essentielle de la communication.

Pour une bonne compréhension mutuelle, les autorités conversant en radiotéléphonie doivent strictement observer les règles suivantes :

- Savoir quoi dire :

  préparer les éléments de la conversation.

- Comment le dire :

  articuler correctement les mots ;

  ne pas hurler devant le micro ;

  être bref et précis.

1 3. Le final :

Le final doit obligatoirement figurer à la fin de chaque émission. Lui seul permet le fonctionnement en alternat. Il se compose, suivant le cas, des termes de procédure suivants :

- PARLEZ = fin de ma transmission : je vous écoute ;
- TERMINÉ = fin de ma transmission : je n'attends et ne demande aucune réponse ;
- ATTENDEZ = je stoppe ma transmission quelques secondes.

2 - LES RÉACTIONS D’AUTORITÉ

Les autorités expéditrices ou destinataires d'un message sont habilitées à prendre certaines initiatives influant sur la transmission du message. Ces actes sont appelés « réactions d'autorité ». Tels sont, en particulier :

- ➲ l'aperçu ;
- ➲ l'annulation ;
- ➲ la vérification.

2 1. L’aperçu :

La demande d'aperçu est spécifiée par l'autorité origine à la fin du texte du message sous la forme : « faites l'aperçu ».

L'aperçu est un message réponse rédigé par l'autorité destinataire sous la forme :

« Aperçu votre message n° ... », qui signifie : j'a i bien compris votre message. Je suis en mesure d'exécuter.

2 2. L’annulation :

L'autorité origine a, seule, qualité pour annuler un message transmis. L'annulation doit obligatoirement faire l'objet d'un message rédigé à cet effet.

2 3. La vérification :

La vérification permet d'obtenir de l'autorité origine la confirmation de tout ou partie d'un message reçu.

Chapitre 6 - TERMES DE PROCÉDURE

TERMES de procédure	SIGNIFICATION	OBSERVATIONS
APERÇU	J'ai bien compris votre message. Je suis en mesure d'exécuter.	
ATTENDEZ	Je stoppe ma transmission durant quelques secondes.	
ATTENDEZ TERMINÉ	Attendez, je stoppe ma transmission pour plus de quelques secondes.	
COLLATIONNEZ	Répétez-moi cette transmission en entier exactement comme vous l'avez reçue.	
CORRECT	Ce que vous m'avez transmis est correct.	
EXCEPTÉ	Le (ou les) destinataire(s) dont la désignation suit immédiatement est (sont) excepté(s) de l'indicatif collectif.	
FROM	L'autorité origine de ce message est indiquée par la désignation qui suit immédiatement.	
ICI	Cette transmission vient de la station dont la désignation suit immédiatement.	
INFO	Le message est adressé « Pour Information » aux destinataires dont la désignation suit.	
JE COLLATIONNE.....	Ce qui suit est ma réponse à votre demande de collationnement.	
J'ÉPELLE	J'épelle phonétiquement le mot avant.	
JE RÉPÈTE	Je répète la transmission ou la partie indiquée.	
LE MOT AVANT	Le mot du message auquel je me réfère est celui qui précède.	
LE MOT APRÈS	Le mot du message auquel je me réfère est celui qui suit.	
PARLEZ	Ceci est la fin de ma transmission pour vous. Je vous écoute, parlez.	
PRENEZ MESSAGE	Prenez par écrit le message qui suit.	
REÇU	J'ai bien reçu votre dernière transmission.	Lors du *Contrôle radio* signifie « Fort et clair »
RÉPÉTEZ	Répétez... (la partie indiquée).	
SÉPARATION	Indication de séparation entre le texte et les autres parties d'un message.	Est représenté par le signe –
TERMINÉ	Ceci est la fin de ma transmission. Je n'ai plus rien à vous dire.	
TO	Le message est adressé « Pour Action » aux destinataires dont la désignation suit.	
TOUT AVANT	La partie du message à laquelle je me réfère est tout ce qui précède.	
TOUT APRÈS	La partie du message à laquelle je me réfère est tout ce qui suit.	

Chapitre 7 - LA PROCÉDURE SIMPLIFIÉE

1 - BUT

Cette méthode utilisée au niveau peloton/section et escadron/ compagnie est destinée à **simplifier l'appel et l'accusé de réception.** Elle ne supprime pas la procédure réglementaire.

2 - CONDITIONS

Elle est utilisée lorsque les liaisons VHF sont d'excellente qualité et que les utilisateurs sont parfaitement rodés à la procédure réglementaire.

Elle convient plus particulièrement aux liaisons entre chars et pelotons et implique que tous soient très attentifs.

Le réseau est obligatoirement dirigé.

3 - PRINCIPE

Par convention, l'indicatif de la station directrice (SD) n'est jamais prononcé. Les communications sont établies de la SD vers les stations secondaires (SS) ou inversement (jamais entre stations secondaires), *selon la méthode de l'indicatif unique.*

3 1. Quand une station secondaire veut appeler la SD :

Elle transmet seulement son indicatif (le dernier bigramme). La station directrice lui répond *en répétant l'indicatif de la station qui vient d'appeler.*

3 2. Lorsque la SD veut appeler une de ses SS :

Elle utilise l'indicatif de cette dernière (dernier bigramme) et la station secondaire appelée *répond en donnant son propre indicatif* (dernier bigramme).

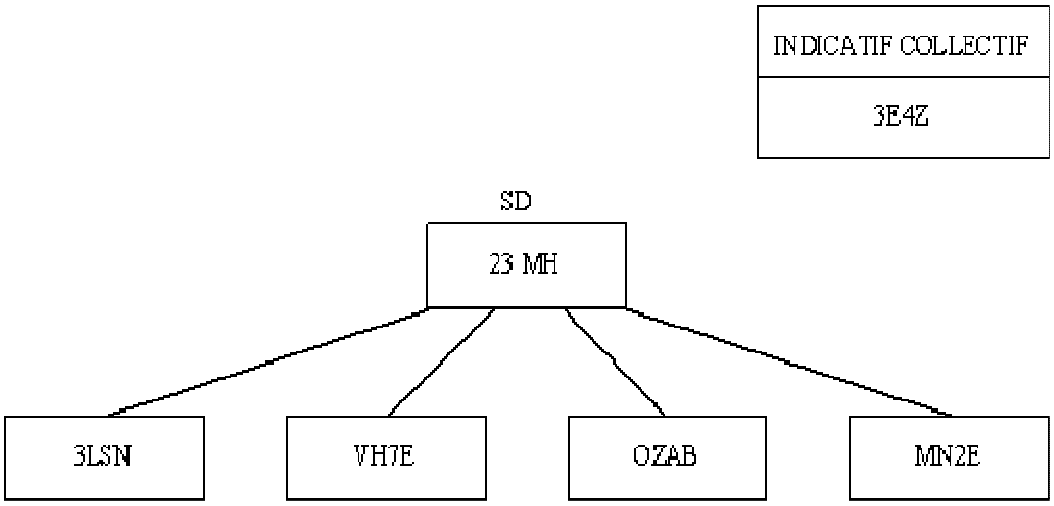
3 3. Lorsque la SD veut appeler l'ensemble de ses subordonnées :

Elle utilise l'indicatif (dernier bigramme). Les SS répondent dans l'ordre en transmettant leur propre indicatif (dernier bigramme).

L'OUVERTURE DU RÉSEAU ET LE CONTRÔLE RADIO SE FONT TOUJOURS EN PROCÉDURE RÉGLEMENTAIRE

4 - EXEMPLES

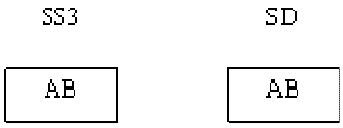
Soit le réseau :



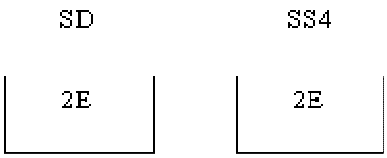
4.1 Appels :

Dès que l'ouverture du réseau et le contrôle radio ont été faits réglementairement, la méthode de l'indicatif unique peut être utilisée.

La station subordonnée n°3 appelle la SD.

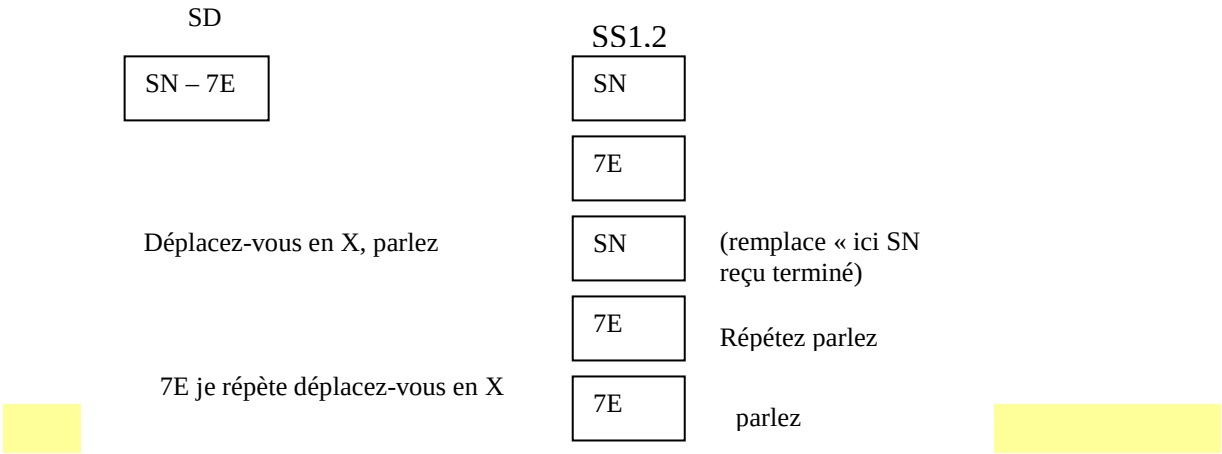


La SD appelle la station subordonnée n°4.



La SD appelle l'ensemble de ses stations secondaires (appel collectif).

4.2 Transmission d'un message pour les SS1 et SS2 :



SECTION III - LA SÉCURITÉ DES COMMUNICATIONS

BUT RECHERCHÉ ET DONNÉES ESSENTIELLES	Cette section vise à sensibiliser le sous-officier sur les dangers de l'action ennemie dans le domaine de la guerre électronique et à lui faire acquérir la conduite à tenir face à ces menaces. Elle traite, en outre, des régimes d'emploi des moyens radio et de la conduite à tenir en cas de capture par l'ennemi.
RÉFÉRENCES	TTA 188 – SIC 609 et 109.
CONSEILS POUR ABORDER L'ÉTUDE	Se reporter aux documents de référence et effectuer des exercices pratiques. Pour les personnels isolés, se mettre en rapport avec un corps de troupe disposant d'un officier transmissions.

Chapitre 1 - LA VULNÉRABILITÉ DES MATÉRIELS DE TRANSMISSIONS

Tous les systèmes de transmissions ou de traitement sont vulnérables à des degrés divers, aux différentes formes de la menace électronique.

Leur modernisation ne les met pas à l'abri, car les moyens d'attaque, utilisant la même technologie, bénéficient des mêmes progrès.

La vulnérabilité de nos systèmes provient :

- ➲ de leur emploi ;
- ➲ de leur technologie ;
- ➲ du personnel qui les met en œuvre ;
- ➲des installations elles-mêmes.

Ce chapitre va examiner, pour chaque forme de menace (écoutes – intrusion – brouillage rayonnement – pièges), les points faibles de nos communications.

1 - VULNÉRABILITÉ AUX ÉCOUTES ET À LA LOCALISATION

La vulnérabilité aux écoutes et à la localisation provient d'une sensibilité à l'interception. C'est une facilité, donnée à l'adversaire, d'analyser les informations qui circulent sur nos réseaux de transmissions.

L'étude de la vulnérabilité sera limitée aux :

- supports radioélectriques (radio, faisceau hertzien, radar) ;
- supports filaires (câble, coaxial, guide d'onde, fibre optique).

Le cas particulier des aéronefs de surveillance du champ de bataille qui peuvent être localisés par la détection de leur émetteur embarqué et celui des dispositifs IFF [1] dont l'interception et l'analyse des signaux peuvent permettre de localiser les unités qui en sont dotées sont cités pour mémoire.

1 1. Les supports radioélectriques :

Aucune émission radioélectrique, quelles qu'en soient sa nature et la zone où elle a lieu, n'est à l'abri de l'interception. Celle-ci peut être plus ou moins difficile à effectuer en fonction :

1 1 1. Des conditions d'emploi.

- ➲ Emplacement de l'émetteur et de son antenne ;
- ➲ Puissance utilisée ;
- ➲ Temps d'émission ;
- ➲ Procédure d'exploitation ;
- ➲ Périodicité des changements de fréquences.

1 1 2. De la technologie utilisée.

- ➲ Type de modulation ;
- ➲ Type d'antenne ;
- ➲ Puissance ;
- ➲ Gamme de fréquence ;
- ➲ Variation de la fréquence dans le temps (évasion de fréquence recherche de canal libre).

1 2. Les relations HF :

Les relations HF (fréquences inférieures à 30 MHz) sont établies:

- soit par onde de sol jusqu'à 100 km ;
- soit par onde ionosphérique au-delà de 150 km.

---

[1] IFF : Identification Friend or Foe

L'interception de ces relations exploitées généralement en télégraphie ou radiotéléphonie est facile à très grande distance. La précision de la localisation est généralement du dixième de la distance entre l'intercepteur et l'émetteur.

1 3. Les relations VHF/UHF :

Établies uniquement en onde de sol, les relations VHF (fréquences comprises entre 30 et 300 MHz) sont exploitées en téléphonie, télégraphie, ou même en transmissions de données. La portée des émetteurs implique généralement une écoute de proximité qui ne présente pas de difficulté technique. La localisation (précision du dixième de la distance au mieux) dépend essentiellement du relief.

Lorsqu'on « monte » en fréquence (UHF) entre 300 MHz et 3 GHz, la propagation s'effectue à vue directe ; l'interception et la localisation dépendent alors essentiellement de l'emplacement des récepteurs d'écoute. Les récepteurs embarqués à bord d'aéronefs offrent alors des possibilités supplémentaires.

1 4. Les relations FH :

Les relations faisceaux hertziens peuvent être interceptées et localisées dans des conditions analogues aux relations VHF ou UHF.

1 5. Les radars :

La localisation des radars est fonction de leur puissance. Les signatures obtenues sont mémorisées et permettent une reconnaissance automatique nécessaire à assurer l'alerte dans les délais les plus brefs.

L'identification d'un radar permet souvent de connaître l'unité ou le système d'arme auquel il appartient.

1 6. L'analyse des interceptions :

Les possibilités d’extraction des informations sont d’autant plus grandes que :

- le matériel utilisé (émetteurs, multiplexeurs, etc.) est du matériel du domaine
- civil respectant impérativement les normes internationales ;
- les informations ne font l'objet d'aucune protection individuelle (chiffrement
- de message) ou globale (chiffrement de voie ou de jonction) ;
- les supports sont spécialisés.

1 7. Les supports filaires :

Bien que généralement moins vulnérables que les précédents, les supports filaires sont également susceptibles de donner prise aux écoutes.

L'interception nécessite soit un branchement direct sur le circuit, soit une

proximité (induction).

Le maximum de vulnérabilité est présenté par :

- les lignes spécialisées (en particulier les extensions qui relient les matériels
- d'extrémité au réseau des transmissions) ;
- les réseaux locaux, notamment ceux réalisés à partir de circuits loués.

On peut considérer que le câble métallique est le plus vulnérable des supports filaires et qu'actuellement la fibre optique est la plus difficile à intercepter.

2 - VULNÉRABILITÉ À L'INTRUSION

L'intrusion nécessite une écoute préalable. La sensibilité aux écoutes conditionne donc la sensibilité à l'intrusion. Mais en outre la vulnérabilité réside dans :

- ➲ le non-respect des procédures (authentification) ;
- ➲ l'absence de surveillance de l'exploitation ;
- ➲ la grande complexité et l'absence de cloisonnement des réseaux d'informatique et de transmissions ;
- l'absence de chiffrement ;
- ➲ la mise en place de matériels et de logiciels insuffisamment élaborés ou contrôlés ;
- ➲ une mauvaise organisation de la sécurité (mots de passe en clair sur des lignes non protégées en télétraitement, télédépannage à partir du réseau commuté, etc.).

3 - VULNÉRABILITÉ AU BROUILLAGE

Le brouillage s'applique toujours aux récepteurs. Pour être efficace, il nécessite le plus souvent une analyse des caractéristiques des émissions et une certaine puissance.

Les liaisons FH étant du type duplex, il n'est théoriquement pas possible de situer les récepteurs sauf s'ils sont systématiquement au même endroit que les émetteurs (forces) ou peuvent facilement être repérés (infrastructures).

Les brouilleurs multifréquences permettent de brouiller plusieurs réseaux à fréquence fixe tout en préservant certains réseaux exploités dans le même secteur. Le brouillage est d'autant plus efficace que le débit est élevé (transmissions de données). Même s'il n'interdit pas complètement la transmission (télégraphie manuelle), le brouillage diminue le débit et oblige aux répétitions donc souvent aux fautes d'exploitation. Le brouillage des radars est réalisable.

4 - VULNÉRABILITÉ AUX RAYONNEMENTS

Les phénomènes transitoires qui accompagnent les changements rapides de l'état des circuits provoquent une variation brusque des composantes électriques et magnétiques du champ ; cela se traduit par une perturbation électromagnétique parasite qui se propage dans l'espace environnant par conduction ou rayonnement.

Tous les appareils électroniques ne présentent pas nécessairement les garanties suffisantes pour le traitement d'informations protégées. Ces dernières peuvent être compromises par l'interception des rayonnements électromagnétiques provenant du matériel. C'est le cas des équipements de bureautique, d'informatique, de transmissions qui n'ont pas été spécialement traités ou installés dans le respect des normes.

Inversement, les équipements électroniques ou magnétiques, qui ne sont pas mis à l'abri des rayonnements incidents, ne peuvent être considérés comme fiables.

5 - VULNÉRABILITÉ AUX PIÈGES

Le piégeage peut porter sur les équipements ou installations. Il peut être mis en œuvre à distance et n'est pas toujours décelable. En ce qui concerne les équipements, la vulnérabilité aux pièges peut se situer au niveau :

- ➲ de la conception ;
- ➲ de la réalisation ;
- ➲ de la mise en place ;
- ➲ de la surveillance ;
- ➲ du maintien en condition.

La vulnérabilité des installations est due essentiellement à un défaut de conception ou à un manque de surveillance en cours de construction ou d'entretien.

6 - VULNÉRABILITÉ À L'IEM

Une explosion nucléaire à très haute altitude provoque l'apparition d'une onde très brève et très énergétique sur des milliers de kilomètres carrés dont résulte l'Impulsion ElectroMagnétique (IEM).

Induite dans les circuits et composants, elle peut provoquer :

- ➲ la destruction des matériels ;
- ➲ le fonctionnement erratique des systèmes.

Chapitre 2 - LA PROTECTION

FACE À LA MENACE ÉLECTRONIQUE PRENDRE DES MESURES DE PROTECTION ÉLECTRONIQUE

1 - CONTRE LES ÉCOUTES ET LA LOCALISATION

1.1 Pour ÉVITER la DÉTECTION par la réduction de la signature électronique :

➲ Appliquer strictement les régimes précisés dans les ordres.

➲ Être bref sur tous les réseaux.

➲ Communications de moins de 25 secondes.

➲ Mouvements fréquents des PC.

➲ Utiliser : officier liaison, téléphone civil, estafette, fil.

➲ S'implanter dans les bois, collines, bâtiments... pour faire écran face à la direction de l'ennemi.

➲ Rechercher le déport des moyens rayonnants (sites radio, relais, télécommande...).

➲ Utiliser la faible puissance.

➲ Réduire la taille de l'antenne.

1.2 Pour ÉVITER L'IDENTIFICATION :

➲ Respecter les règles de procédure (TRS 121).

➲ Changer de fréquences et indicatifs selon les prescriptions de l'OCT.

➲ Proscrire les mauvaises habitudes (manipulations particulières, spécificités d'opérateurs ou d'unités).

1.3 Pour ASSURER LA SÉCURITÉ DES TRANSMISSIONS :

➲ Préparer des ordres initiaux clairs et précis.

➲ Tenir compte de l'approbation des relations.

➲ Dates, noms de localités et de personnalités, d'unités et de garnisons coordonnées (par procédés réglementaires SCDG, SLIDEX...).

2 - CONTRE LE BROUILLAGE

Pour vérifier le fonctionnement de l'appareil et l'absence d'interférences locales :

- ➲ Débrancher l'antenne :

  si le bruit persiste, vérifier les branchements et l'appareil ;

  si le bruit persiste encore le brouillage est confirmé.
- ➲ Rebrancher l'antenne.

Pour continuer à travailler sur la fréquence brouillée :

- ➲ Refaire l'accord d'antenne (BLU).
- ➲ Améliorer l'emplacement de l'émetteur.
- ➲ Augmenter la puissance.
- ➲ Rendre compte du brouillage (voir modèle en fin de chapitre 3).

Si les communications sont inexploitables :

- ➲ Changer de fréquences ou de modes d'exploitation (graphie).
- ➲ Se déplacer.
- ➲ Utiliser un autre mode de communication.

Nota. – Apprendre à reconnaître les différences entre brouillage et interférences.

3 - CONTRE L'INTRUSION

- ➲ Respecter la discipline du réseau.
- ➲ Authentifier les correspondants.
- ➲ Rendre compte de l'intrusion (voir chapitre 3).

4 - CONTRE L'IMPULSION ÉLECTROMAGNÉTIQUE

- ➲ Débrancher les matériels non indispensables.
- ➲ Fermer les ouvertures des stations en cabine.
- ➲ Mettre sous abri métallique les matériels réservés.

Chapitre 3 - GUIDE D’EMPLOI DES MOYENS RAYONNANTS

1 - RÉGIMES D’EMPLOI

Les régimes d'emploi sont une prérogative du commandement et sont précisés dans l'ordre d'opération.

Un échelon donné ne peut imposer un régime d'emploi moins contraignant que celui imposé par l'échelon supérieur.

Des régimes différents peuvent être simultanément imposés en fonction des matériels (radio HF, radio VHF, faisceaux hertziens, radars), des puissances utilisées, des unités (missions, postures...), de la phase d'engagement.

(Voir tableau ci-dessous paragraphe suivant).

2 - FONCTIONNEMENT DES RÉSEAUX RADIO

Un GDF (groupement de forces) doit faire fonctionner environ 500 réseaux avec seulement 250 fréquences qui sont identiques à celles des autres GDF français.

21. Contraintes :

Cette ressource limitée impose des répétitions de fréquences.

22. Règles à appliquer :

Précisées dans le chapitre précédent, elles peuvent être résumées ainsi :

- ➲ Réduire chaque fois que possible le nombre de réseaux au sein de l'unité.
- ➲ N'utiliser que les fréquences attribuées avec la puissance prescrite.
- ➲ En cas d'interférence, rendre compte.
- ➲ En cas de brouillage, appliquer les règles ci-dessus.
- ➲ En cas de gêne importante et en l'absence de fréquence de dégagement :

  - ne pas travailler sur une « fréquence silencieuse » non attribuée ;
  - utiliser la puissance maximum seulement en cas d'urgence ;
  - essayer l'intégration radio-fil vers les correspondants dotés de RITA.

Si le réseau est gêné par des interférences amies, changer si possible de fréquence.

Les changements de fréquences en cours d'action font l'objet d'ordres particuliers.

23. Définitions :

FRÉQUENCES PRÉSERVÉES DU BROUILLAGE AMI : Fréquences INTERDITES (ou TABOUES) : fréquences qui ne doivent jamais être brouillées parce qu'elles sont vitales pour les activités amies.

RÉGIMES D'EMPLOI

RÉGIMES	MOYENS	HF (MA BLU)	VHF (MF)	RITA	RADARS
Silence	Niveau 1	Silence absolu. Application mesures de protection : - anti IEM ;- électronique.Utilisation moyens non rayonnants.	*Idem* HF.	*Idem* HF. Réseau non déployé.	Matériels à l'arrêt et camouflés.
	Niveau 2	*Idem* niveau 1 sauf : - pour postes très faible puissance ; - pour tous les moyens en cas de force majeure (attaque aérienne, NBC, rencontre avec l'ennemi) ; - sur	*Idem* HF. Pas d'IRF. Émetteur d'alerte autorisé en cas d'urgence.	*Idem* HF. Système minimum déployé mais non activé. Pas d'intégration radio. Pas de PRA-IN.	Matériels sous tension. Aucune émission autorisée sauf ordre particulier.

		décision CDT. Tous les MOYENS SONT en VEILLE.			
Discrétion	Niveau 1	Pas d'émission sauf si la gravité de la situation l'exige (puissance limitée à 10 W).	Uniquement réseaux vitaux sans antenne, grand gain et puissance limitée à 1,5 W. Pas d'intégration radio. Non-utilisation des sites et relais. Limite durée émissions.	Réseaux minimums ouverts (CN et jonctions). Pas d'intégration radio (CRR à l'arrêt). Pas de relais. Raccordement en gamme 2 seulement. Sites radio de GDF non raccordés.	Fonctionnement en faible puissance. Changements de position fréquents (< 2 h). Limitation durée émissions. Pas de balayage (coups de phare). Émission alternée des stations.
	Niveau 2	Émission autorisée uniquement sur ordre ou en cas de force majeure (puissance limitée à 100 W).	Intégration radio autorisée. Sites et relais possibles. Utilisation émetteurs 1 KW (alerte, art.) selon ordres particuliers.	Réseaux limités, pénétrante autorisée (sans emploi des relais organiques). Utilisation PRA-IN (CRR à l'arrêt) seulement. Raccordement site radio GDF possible.	*Idem* niveau 1.
Liberté	Niveau unique	Régime normal. Application mesures de protection décrites. Respect de la procédure. Respect des règles d'utilisation. Risque majeur par rapport à la GE ennemie.	*Idem* HF. Ouverture tous réseaux utiles.	*Idem* HF. Réseau normal déployé. Intégration radio entièrement en service.	Fonctionnement normal. Mesures de protection à appliquer.

FACE À LA MENACE ÉLECTRONIQUE RESPECTER LES RÉGIMES D'EMPLOI IMPOSÉS

Fréquences GARDÉES : fréquences employées par l'ennemi et qui servent de source de renseignement pour les forces amies.

Fréquences PROTÉGÉES : fréquences indispensables attribuées pour les opérations des forces amies et qui ne doivent subir qu'un minimum de brouillage.

3 - ORDRES ET COMPTES RENDUS

À adresser par l'échelon concerné aux unités subordonnées pour tout changement de fréquence imposé par une gêne, ou un changement de zone d'activité.

3 1. Ordre de changement de fréquence :

OBJET : CHANGE FREQ.

- A Lots ou fréquences supprimés.
- B Lots ou fréquences attribués.
- C GDH du changement.
- D Limites zones de validité nouvelles fréquences.
- E Indicatifs à utiliser.

3 2. Compte rendu de brouillage ou d'intrusion ou d'interférence :

À adresser, dès que possible, par un moyen protégé à l'échelon immédiatement supérieur.

OBJET : CR BRUIT.

- A Unité concernée - position (coord. UTM).
- B Réseaux et fréquences gênés.
- C Type de gêne (brouillage, ou intrusion, ou interférence).
- D GDH début - durée.
- E Éléments d'identification :
  en cas de brouillage : caractéristiques et efficacité ;
  en cas d'intrusion : caractéristiques ;
  en cas d'interférence :
  puissance et antennes utilisées,
  indicatifs, noms... entendus.
- F Mesures prises.

Chapitre 4 - CONDUITE À TENIR EN CAS DE CAPTURE PAR L’ENNEMI

L'ennemi peut utiliser un poste radio pris aux amis pour s'introduire dans les réseaux, donner des ordres destinés à jeter la confusion ou obtenir des renseignements. Si sa capture est devenue inéluctable, l'opérateur a le devoir de détruire son poste et de ne laisser subsister aucun indice qui permettrait à l'ennemi de reconstituer le réseau ami (exemple : quartz des TR-PP 11).

Émetteurs-récepteurs, accessoires, documents techniques sont écrasés ou brûlés. Les câblages sont coupés. Les morceaux sont ensuite dispersés, jetés à l'eau ou enterrés.

Sur les émetteurs-récepteurs de 4e génération et sur certains boîtiers de chiffrement (CNT), il existe une touche RAZ (remise à zéro ou effacement d'urgence) qui efface les clés de chiffrement utilisées dans les réseaux. Tout opérateur a le devoir d'appuyer sur cette touche en cas de capture.

SECTION IV - LA COMPOSANTE STRATÉGIQUE DES TRANSMISSIONS

BUT RECHERCHÉ ET DONNÉES ESSENTIELLES	Cette section vise essentiellement à fournir aux sous-officiers une information sur la Composante Stratégique des Transmissions de l'Armée de Terre : les télécommunications et les systèmes d'information.
RÉFÉRENCE(S)	TTA 133.
CONSEILS POUR ABORDER L'ÉTUDE	Cette étude théorique pourra être complétée par l'étude du mémento sur les SIC figurant dans les documents à connaître pour la préparation à l'EA2/FS du BSTAT

La fonction opérationnelle SIC est chargée d'établir les liaisons nécessaires au commandement et d'en assurer le fonctionnement. Pour remplir cette mission, l'arme des Transmissions met en œuvre un système de transmissions unique, à **trois composantes interconnectables** :

- une composante tactique au profit des forces (cf section V) ;
- une composante des SIC opératifs au profit du commandement (cf section VI) ;
- une composante stratégique qui dessert l'ensemble des garnisons (métropole, outre-mer, forces pré positionnées).

Le resserrement du format de l'armée de terre, la mise en place de nouvelles structures de commandement et l'émergence de la fonction Télécommunications et Systèmes d'Informations (TSI) ont contribué à l'évolution des missions générales des Systèmes d'Informations et de Communications (SIC) de la composante stratégique.

Les missions de la chaîne TEI de l'armée de terre sont :

- Assurer ou participer à **l'interconnexion** aux réseaux nationaux militaires et civils, aux réseaux alliés ainsi qu'au raccordement des forces projetées dans un cadre national ou multinational ;
- Fournir en tout temps, en métropole et selon le cas en outre-mer et à l'étranger, au profit des organismes de l'armée de terre, de la Défense ou d'autres ministères, un **service fiable**, **sécurisé**, et de **qualité,** dans le domaine des télécommunications et de l'informatique ;
- Participer à la **conception,** réaliser ou participer à la **réalisation**, **mettre en oeuvre** et **maintenir** les systèmes d'information et de communication qui lui sont confiés.

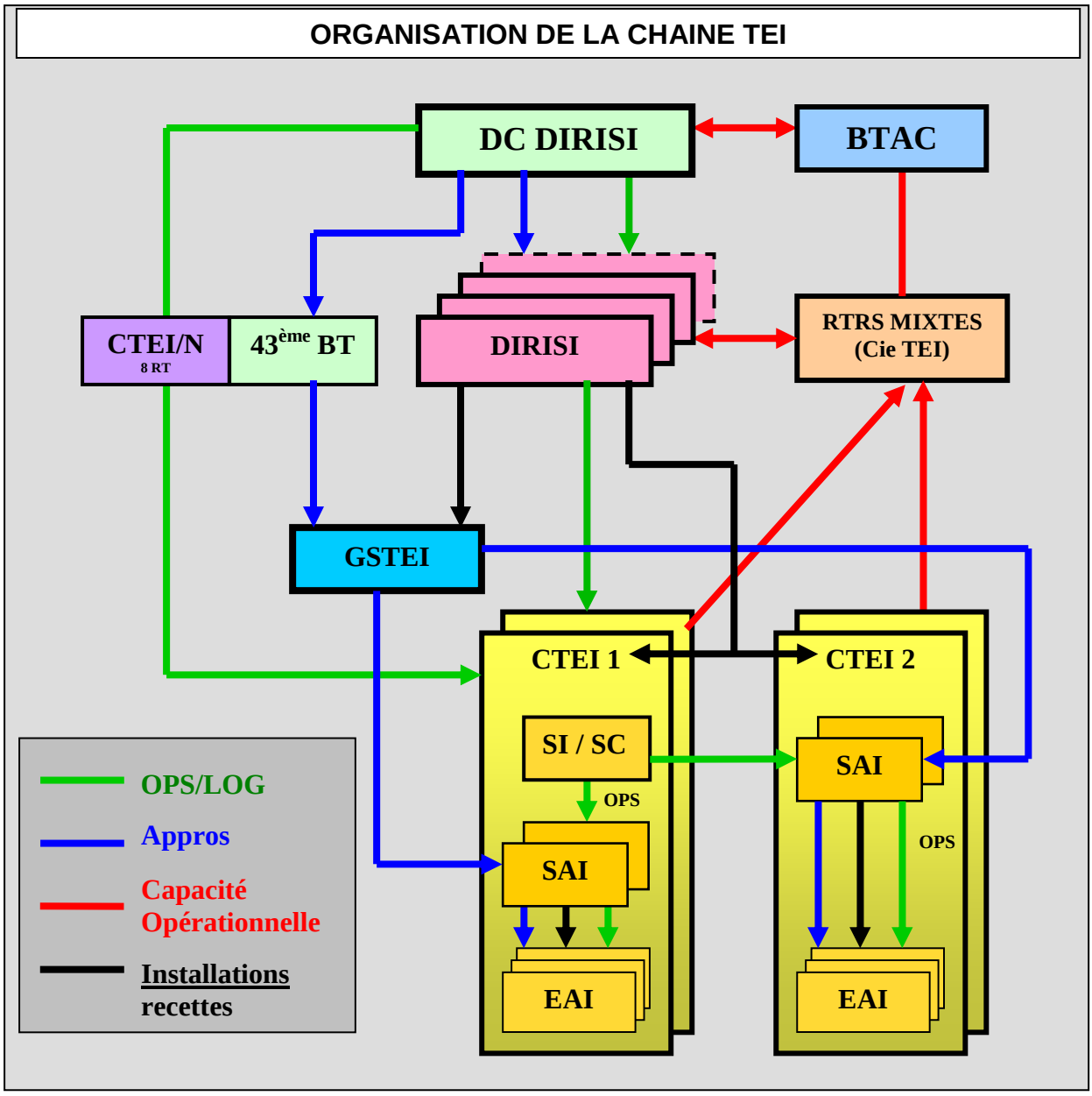
CHAPITRE 1 – L'ORGANISATION GENERALE DE LA COMPOSANTE STRATEGIQUE

La Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information (DIRISI), rattachée à l'EMA[2] a vocation à assurer la direction et le soutien des réseaux d'infrastructure des armées, des services communs ainsi que des systèmes d'information d'intérêt commun au profit de l'ensemble du ministère. De création récente, elle monte progressivement en puissance.

Pour l'Armée de Terre, cette direction et ce soutien sont assurés par la chaîne TEI de l'ex DCTEI[3] .

Pour réaliser les missions dont elle a la responsabilité, elle s'appuie sur des entités ayant des fonctions de commandement organique fonctionnel et sur des entités ayant des fonctions de commandement organique territorial.

[2] EMA : Etat Major des Armées.
[3] DCTEI : Direction Centrale des TElécommunications et de l'Informatique.



L'exercice du commandement organique fonctionnel, dessiné ci-dessus, s'applique :

➲ en premier lieu aux domaines de l'emploi des moyens et à la conduite des opérations. La politique est assurée par la Direction Centrale DIRISI (DC DIRISI) et la conduite par les DIRISI locales (des régions Terre).

➲ en deuxième lieu, il s'applique au niveau de la mise en œuvre des moyens, notamment au travers des fonctions accueil - gestion – soutien, exercées au niveau régional par les Centres Techniques des Télécommunications Et de l'Informatique (CTEI1) et les Groupements de Soutien des Télécommunications et de l'Informatique (GSTEI), et au niveau

zonal ou local par les CTEI 2 et les Sections et Eléments d'Appui d'Infrastructure (SAI et EAI).

L'exercice du commandement organique territorial s'applique à la préparation de la chaîne ; il est notamment responsable de :

- l'organisation, l'instruction, l'entraînement et la sécurité des entités TEI ;
- la définition et l'expression des besoins (hors domaine TEI) ;
- la gestion et l'administration du personnel ainsi que l'application de la réglementation relative aux conditions de vie.

Les organismes exerçant ce commandement sont :

- la brigade de transmissions et d'appui au commandement;
- les régions terre (RT) dans leurs domaines respectifs de compétences ou d'attributions.

Il s'exerce sur :

- les régiments "mixtes" (comprenant des unités de la composante tactique et des unités de la composante stratégique des SIC) ;
- le 8ème RT (régiment exclusivement composé de compagnies de la composante stratégique) ;
- le 43eBataillon de transmissions ;
- le Groupement de Soutien de Bicêtre (GSB).

1 - principe de surete DES SIC STRATEGIQUES

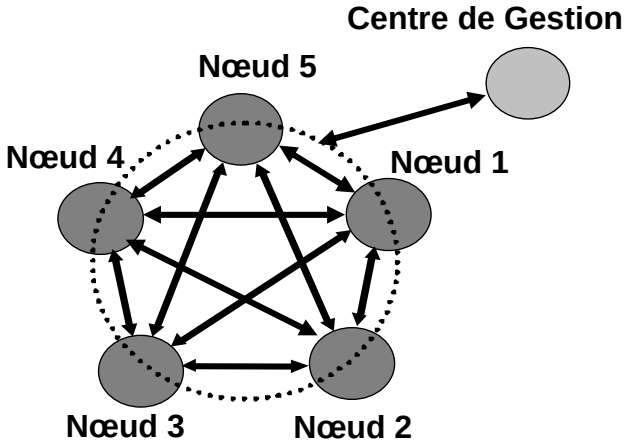
La permanence des liaisons, indispensable à l'accomplissement des missions, est réalisée par :

- ➲ le maillage des réseaux et la diversification des moyens (redondance) ;
- ➲ l'interconnexion et l'interopérabilité de ces réseaux avec d'autres réseaux (civils et militaires).

1 .1 Maillage des réseaux et diversification.

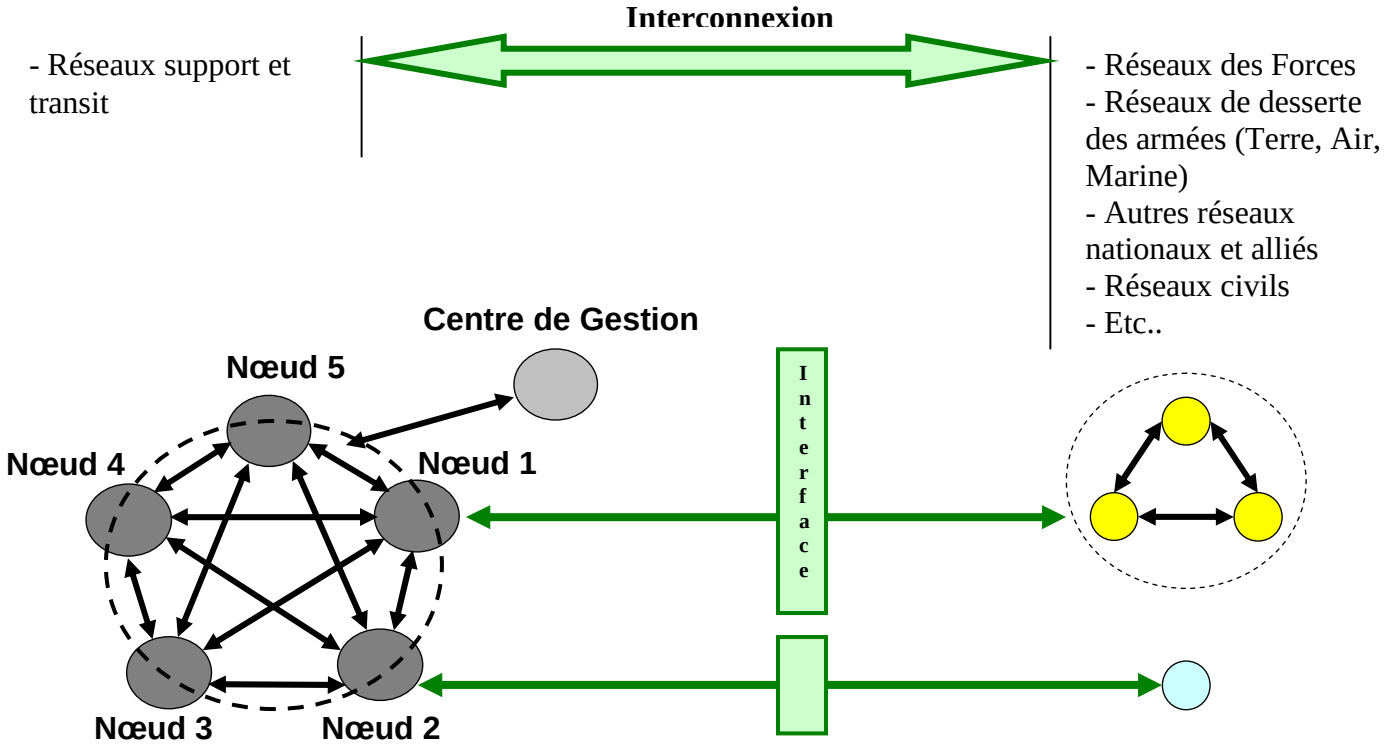
Par opposition au système hiérarchique, le maillage est obtenu par la structure propre des réseaux de support (hertzien ou fibre optique), permettant des routages diversifiés. La complexité du maillage nécessite généralement une gestion centralisée du système.

La diversification des moyens est assurée par la juxtaposition de systèmes différents, complémentaires, mettant notamment en œuvre des relations utilisant les réseaux des opérateurs civils.



1 .2 Interconnexion et interopérabilité.

La composante stratégique des SIC de l'armée de terre n'est pas la seule de ce type dans la Défense Nationale. La spécificité des missions de la composante "forces", la particularité des systèmes de télécommunications des autres ministères, des pays voisins et de l'OTAN, ne permettent pas une interopérabilité parfaite entre ces réseaux, d'où un nombre important d'interconnexions.



- ➲ **Vers la composante des forces.**

  Un certain nombre de sites sont équipés pour accueillir les raccordements d'unités de forces. Le réseau tactique de zone, basé sur le système RITA 2G[4], présente des interfaces normalisées lui permettant de se raccorder directement sur le réseau de transit SOCRATE[5].

  Par ailleurs, des sites d'accueil satellitaire permettent le raccordement des forces projetées aux différents réseaux de métropole.

  Les stations MATILDE[6] permettent le raccordement des stations HF NG des forces sur le réseau télégraphique.

- ➲ **Vers les autres armées.**

  L'interconnexion téléphonique est réalisée via le réseau de transit interarmées SOCRATE, au travers de la mise en œuvre du Plan de Numérotage InterArmées (PNIA).

  Dans le domaine de la télégraphie, les trois armées sont interconnectées par l'intermédiaire de passerelles entre les Centres de Relais Automatique (CRA).

  Pour la transmission de données, le réseau fédérateur des armées est le réseau IP SOCRATE.

- ➲ **Vers les alliés et l'OTAN.**

---

[4] RITA : Réseau Intégré de Transmissions Automatique.
[5] SOCRATE : Système Opérationnel Constitué de Réseaux des Armées pour les TElécommunications.
[6] MATILDE : Modernisation et Amélioration des Transmissions Interarmées Longue DistancE

Des passerelles télégraphiques et téléphoniques sont également activées vers l'Allemagne, l'Espagne, la Belgique, l'Italie et vers l'OTAN.

- ➲ **Vers les autres ministères.**

  Dans le cadre de la téléphonie à usage général, l'interopérabilité est réalisée via les réseaux des opérateurs civils, notamment pour le réseau fermé d'autorités RIMBAUD[7].

  En matière de télégraphie, une passerelle est activée au Secrétariat Général pour la Défense Nationale (SGDN).

  De plus, les réseaux de l'armée de terre utilisent les réseaux d'opérateurs civils.

[7] RIMBAUD : Réseau InterMinistériel de Base Uniformément Durci.

2 - LES RESEAUX FONCTIONNELS DES SIC STRATEGIQUES

2. 1 Généralités.

Les réseaux de télécommunications des armées ont évolué vers un ensemble moderne et cohérent de systèmes de télécommunications commutés à intégration de services (voies, données, images) de type RNIS[8].

Une répartition fonctionnelle a été effectuée entre les besoins de "transit", communs à tous, et les besoins de "desserte", plus spécifiques à chaque armée.

L'ensemble des réseaux des armées s'appuie sur deux types de réseaux principaux :

➲le réseau de transit interarmées SOCRATE, chargé de fédérer et de moderniser les fonctions nationales de transit ;

➲les réseaux de desserte rénovés des armées, à savoir :

- MTGT[9] pour l'armée de terre ;
- MTBA[10] pour l'armée de l'air ;
- RVDM[11] pour la marine.

Un plan de numérotation interarmées a été mis en place pour faciliter l'interfonctionnement entre les réseaux de desserte.

2. 2 Les réseaux de transit.

- 2.2.a. Le réseau de transit interarmées SOCRATE et ses raccordements.

Réseau métropolitain interarmées et unifié des télécommunications d'infrastructure, SOCRATE (Système Opérationnel Constitué des Réseaux des Armées en pour les TElécommunications) assure la satisfaction des besoins opérationnels des armées et de la gendarmerie, en temps de paix, crise ou engagement.

Le réseau de transit interarmées SOCRATE est constitué de la fédération des anciens réseaux hertziens des armées (RITTER[12] pour l'armée de terre, RA 70[13] pour l'armée de l'air, réseau "sémaphore" de la marine), complétée de fibres optiques à haut débit louées à des opérateurs publics.

Les supports de télécommunications sont entièrement numériques. Ces artères, fortement maillées, sont sécurisées au niveau confidentiel défense (chiffreurs d'artères). La majorité des nœuds de communication, ainsi que les sites de desserte les plus importants, sont protégés contre les effets des Impulsions ElectroMagnétiques issues d'une explosion Nucléaire à Haute Altitude (IEMN/HA).

Les nœuds de communication sont équipés de commutateurs de technologie ATM[14]. Cette technologie autorise une meilleure sûreté de fonctionnement par reconfiguration automatique du réseau en cas de dégradation d'artères

---

[8] RNIS : réseau Numérique à Intégration de Services.
[9] MTGT : Moyens Transmissions des Garnisons Terre.
[10] MTBA : Moyens Transmissions des Bases Aériennes.
[11] RVDM : Réseau Voix Données de la Marine.
[12] RITTER: Réseau Intégré des Transmissions de l'armée de terre.
[13] RA70:Réseau Air 1970. Réseau support de l'armée de l'air.
[14] ATM: Asynchronous Transfert Mode (mode de transfert asynchrone).

ou d'équipements de commutation. Ces reconfigurations s'effectuent en totale transparence pour les usagers.

SOCRATE offre deux grandes fonctions nationales de transit :
➲ un transit ATM au profit de la téléphonie multiservices (MTGT pour l'armée de terre) ;

➲ un transit IP au profit des réseaux fédérateurs IP des armées (REFEDAT pour l'armée de terre).

La direction du réseau SOCRATE est assurée au sein de la DIRISI[15], organisme interarmées.
➲ Le système de gestion du réseau permet une supervision en temps réel des équipements et de réaliser des opérations de télémaintenance. Il est organisé autour d'un centre national de gestion (CNG) et de centres zonaux de gestion (CZG), Organismes à Vocation Interarmées (OVIA), armés 24 heures sur 24. Le CNG est un OIA intégré à la DIRISI.

➲ Le soutien sur sites est assuré par des Centres d'Intervention de Secteur (CIS), soumis à un régime d'astreinte. Les personnels des CIS sont sous responsabilité organique de leur armée d'appartenance et pour emploi sous la responsabilité fonctionnelle de la DIRISI.

2.2.b. Les réseaux des opérateurs civils.

En complément des circuits offerts par les réseaux militaires et afin de raccorder l'ensemble des implantations, les armées louent des liaisons aux opérateurs civils.

Ces liaisons peuvent se classer en trois types :
➲ Les Liaisons de Défense (L.D.) : elles relient directement, par câbles ou fibres optiques, deux établissements de la défense, sans transiter par un répartiteur général d'un opérateur public. Principalement utilisées pour assurer la desserte téléphonique des emprises non pourvues de commutateurs téléphoniques, ces liaisons sont progressivement reprises dans le programme MTGT ;

➲ Les Lignes Supplémentaires Extérieures (L.S.E.): elles permettent de déporter un équipement de télécommunications à une distance maximale de 500 mètres. Ces liaisons, en voie de disparition, relient le plus souvent un abonné isolé à son commutateur téléphonique de rattachement ;

➲ Les Liaisons Louées (L.L.): elles constituent des supports utilisés en prolongement des réseaux militaires, pour la desserte des abonnés isolés et des garnisons non desservies par moyens militaires (y compris certaines liaisons internationales). Elles peuvent se classer en deux grandes catégories :

➲ Les liaisons permanentes qui ont vocation à relier deux entités de façon fixe pendant une période longue (en général plus d'une année),

[15] DIRISI: Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la défense

➲ Les liaisons temporaires réalisées dans le cadre d'exercices ou d'opérations particulières (plan ORSEC, opérations extérieures,…).

Les liaisons proposées par les opérateurs de télécommunications couvrent un large éventail de produits, de la liaison analogique (2 ou 4 fils) aux liaisons haut débit à 155 Mbit/s en passant par tous les débits utilisés par l'armée de terre. Ces liaisons peuvent être supervisées par l'opérateur et dans le cas des liaisons haut ou moyen débit, elles peuvent être reconfigurées de façon dynamique en cas d'incident sur le réseau.

La gestion du parc de liaisons louées de l'armée de terre est assurée de façon centralisée par la DIRISI.

2. 3 Les réseaux fonctionnels de l'armée de terre.

- 2.3.a. MTGT

La modernisation des réseaux de desserte de l'armée de terre s'effectue dans le cadre d'un programme d'armement dénommé modernisation des Moyens de Transmissions des Garnisons de l'armée de terre (MTGT).

Les MTGT constituent les réseaux de desserte propres à l'armée de terre. Ils ont pour vocation de faire évoluer le réseau téléphonique de l'armée de terre vers un réseau multiservices " voix - données – images " de type RNIS, en totale interopérabilité avec les services offerts par le réseau de transit des armées SOCRATE et par les réseaux publics. Le réseau MTGT constitue donc le prolongement du système SOCRATE jusqu'à l'abonné.

Il permet le transfert d'informations :

➲ entre usagers d'une même garnison "terre" ;

➲ entre usagers de garnisons différentes ;

➲ entre usagers d'une garnison "terre" et des abonnés raccordés à un réseau externe relié sur SOCRATE (réseaux des autres armées, réseaux tactiques, alliés, etc.) ;

➲ entre usagers d'une garnison "terre" et usagers (militaires ou civils) du réseau public.

Il comprend :

➲ un Centre National de Gestion (CNG) implanté au sein du CTEI N, au Mont-Valérien, chargé d'assurer la supervision 24 heures sur 24 de l'ensemble des MTGT et la configuration des données qui leur sont communes ;

➲ des Centres Zonaux de Gestion (CZG), assurant la gestion et la supervision des équipements situés dans leur zone de responsabilité pendant les heures ouvrables ;

➲ des Sections d'Assistance et d'Intervention (SAI), intégrées au sein des CTEI 1 et CTEI 2, répartis sur le territoire national.

- 2.3.b. Le Réseau FEDérateur IP de l'Armée de terre.
- *Le REFEDAT est destiné à interconnecter les réseaux locaux de l'armée de terre. Il assure le transport des informations numériques, sous la forme de datagrammes, au travers du protocole de routage IP*[16].

➲ Architecture :

Le REFEDAT se décompose en deux grands sous-ensembles :

- un réseau de transit composé de 16 nœuds régionaux couvrant l'ensemble de la France. Ces nœuds sont reliés entre eux par des liens redondants à haut débit. Leur architecture nodale garantit le bon acheminement des datagrammes vers leur destination. Afin d'augmenter la capacité de transit de REFEDAT, ces 16 nœuds sont raccordés au réseau IP-SOCRATE , qui assure alors le transit du réseau REFEDAT ;

- un réseau de desserte désigné sous le terme de REFEDAT II, qui assure le raccordement capillaire, au cœur de réseau, des organismes.

➲ Utilisateurs :

Les utilisateurs du REFEDAT sont :

- les organismes de l'armée de terre ;

- le réseau « sensible France » pour les liaisons des SIL[17] avec leur base centrale en métropole ;

- les organismes hors Armée de terre souhaitant bénéficier cependant de ses services à partir d'une convention passée avec l'E.M.A.T.

➲ Services offerts :

- accès à une application métier fonctionnant sous protocole IP ;

- accès aux services Intraterre;

- accès aux services Intradef via le segment d'interface Terre ;

- accès au réseau ADER (ADministration En Réseau).

➲ Administration et gestion du REFEDAT :

L'administration du REFEDAT est assurée par la DIRISI qui collecte les demandes des grandes directions et des états-majors, organise et administre les raccordements ainsi que les plans d'adressage et de nommage. Elle définit les procédures de travail avec les organismes des échelons directement subordonnés et rédige les directives d'emploi.

La **gestion** du REFEDAT est une mission confiée au CTEIN. Situé au Mont valérien, il assure la permanence du réseau, le suivi de la qualité de service ainsi que la gestion des incidents dépassant le cadre local.

- 2.3.c. Le réseau télégraphique de l'armée de terre :

[16] IP : Internet Protocol.
[17] SIL : Système d'information logistique (SILCENT,SIMAT,….)

- ➲ Organisation du réseau :

  Le réseau télégraphique offre à ses abonnés, en tout lieu et en tout temps, la garantie d'acheminement de bout en bout, la remise et la protection de l'information en fonction du niveau de confidentialité.

  Il repose sur des centres de commutation raccordant les systèmes automatisés de desserte des abonnés articulés autour du système de Traitement Automatique de Messages (TAM), implantés au sein des CTEI1, CTEI 2, et du CTEI MINDEF.

  Le réseau télégraphique est par ailleurs interconnecté avec :

  - les réseaux de l'armée de l'air, de la marine et certains ministères ;

  - le système de télécommunications de l'OTAN (via le réseau de la marine) ;

  - des moyens de circonstance mis en place au profit des forces projetées dans le cadre d'opérations extérieures ou de projections intérieures (MATILDE, CARTHAGE[18], MELCHIOR[19]...) ;

  - les pays frontaliers grâce à des passerelles télégraphiques bilatérales.

  Le transport des informations est assuré au format ACP 127, par des liaisons spécialisées à la norme V24 à 9600 bauds.

  ➲ Commandement du réseau :

  Opérationnel 24 heures sur 24, le réseau télégraphique de l'armée de terre est administré par la DIRISI.

  Conçu pour avoir un taux de disponibilité extrêmement élevé, il est supervisé en permanence au niveau national (CTEIN/CNG) et au niveau régional (CTEI 1).

  ➲ Sécurité du réseau :

  La sécurité du réseau contre les actes de malveillance qui viseraient soit à :

  - dégrader son fonctionnement ;

  - s'introduire dans les systèmes (TAM en particulier) ;

  est assuré par un par un Equipement de Trans-chiffrement Numérique Automatique (ETNA).

- 2.3.d. La messagerie universelle sécurisée (MUSE) :
- La messagerie universelle sécurisée est un système informatique utilisé pour :
  ➲ la transmission de messages formels entre les différentes organisations du ministère de la défense (armées et organismes) ;

[18] CARTHAGE: Communications Automatisées Radioélectriques Tactiques HF en Ambiance de Guerre Electronique.
[19] Moyens d'ELongation pour les Communications Hf Interarmées et Otan en Réseau.

➲ les échanges d'informations entre les personnes (interpersonnel) ;

➲ les échanges de données entre applications.

Il se substituera progressivement au réseau télégraphique de type ACP 127 au cours de la période 2005 - 2008 et est inter opérable avec les autres systèmes de messageries et avec les alliés. Il a vocation à être utilisé en temps de paix, de crise ou de guerre. Il permet par ailleurs de traiter, en ligne[20], les messages de niveau "confidentiel défense / confidentiel OTAN".

[20] Position connectée au réseau, par opposition à "hors ligne", soit hors de tout raccordement à un quelconque réseau (poste isolé).

3 - LES SERVICES DES SIC DE LA COMPOSANTE STRATEGIQUE

3. 1 La téléphonie.

Le réseau téléphonique MTGT offre des services comparables à ceux du réseau public NUMERIS, tels que "renvoi d'appel", "identification de l'appelant" et "transfert d'appel".

Il est complété par des services spécifiquement militaires, tant au niveau de la sécurité du réseau que de l'acheminement des informations, tels que le "cloisonnement d'utilisateur", "le groupe fermé d'usager" et "la priorité", ce dernier n'étant attribué qu'à certains usagers.

Par ailleurs, les services péri-téléphoniques suivants sont offerts :

- la messagerie vocale ;
- l'annuaire intégré permettant notamment l'affichage du nom et la numérotation par le nom sur les postes numériques.

3. 2 La messagerie.

La desserte de la messagerie formelle au profit des organismes de l'armée de terre est assurée par le réseau télégraphique de type ACP 127. Ce réseau gère 4200 adresses et achemine, en clair ou crypté, de l'ordre de 6 millions de messages par an.

- ***Généralités sur les moyens de desserte mis en œuvre.***

Depuis l'automatisation des centres de transmissions tributaires, les usagers sont dotés de systèmes informatiques leur permettant de se connecter au réseau de desserte, soit par l'intermédiaire du réseau téléphonique commuté (RTC), soit directement à partir de leur réseau local. Ils peuvent également, dans des circonstances exceptionnelles, utiliser des équipements télégraphiques nécessitant des liens physiques pour se raccorder au système "TAM".

- ***Le logiciel Transwin .***

Le logiciel TRANSWIN (TRANSmissions sous WINdows), installé sur un poste de travail de type bureautique et connecté à un serveur TRANSTEX, offre la possibilité d'émettre et de recevoir des messages affectés d'un degré de protection inférieur ou égal à "diffusion restreinte". Cet équipement de desserte peut en fonction du besoin, être associé à un autre moyen de type TRANSWIN CD pour le traitement hors circuit des messages classifiés de niveau limité à "confidentiel défense" et de niveau "secret défense" avec le TM32.

4 – INTERNET/ INTRANET - VISIOCONFERENCE

4.1 Internet

Internet est une interconnexion de réseaux offrant l'accès à une variété d'informations et de services allant du document à la vidéo. Ce réseau multimédia très ouvert permet l'échange du courrier au moyen d'une adresse électronique ou la fourniture de services et utilitaires. Il fonctionne en utilisant un protocole commun, qui permet l'acheminement de proche en proche de messages découpés en paquets indépendants (Internet Protocol). L'accès au réseau est ouvert à tout utilisateur ayant obtenu une adresse auprès d'un fournisseur d'accès à Internet (FAI ou provider) suivant les procédures en vigueur. La connexion au réseau Internet est soumise à des principes de sécurité qui imposent que les stations soient dédiées et physiquement isolées des réseaux militaires. De plus, l'utilisation de données provenant de l'Internet à transférer dans un autre réseau, nécessite le passage préalable par un sas (station blanche) qui assure au minimum le contrôle antiviral.

- 4.1.a Les services.

Il faut distinguer cinq catégories de services :

1. le courrier électronique, service le plus utilisé, permettant d'envoyer et de recevoir du courrier électronique ou mail ;
2. le forum (ou news) permettant d'échanger idées et opinions sur un sujet particulier ;
3. la recherche d'informations sur le Web permettant de "feuilleter" un grand nombre d'informations à partir d'un ordinateur et de trouver des éléments d'informations détaillés, sur des domaines variés ;
4. le téléchargement (ou FTP) permettant d'acquérir ou de mettre à disposition de nouveaux outils ou fichiers par transfert électronique ;
5. le télé service simplifiant toute démarche entre deux personnes morales ou physiques en dématérialisant les documents papiers qui y sont attachés.

- 4.1.b Modalités de raccordement.

Pour se raccorder à l'Internet, l'usager doit être doté des équipements suivants :

- ➲ un ordinateur disposant d'un modem relié à une ligne permettant de connecter l'ensemble au fournisseur d'accès ; actuellement il est mis en oeuvre des accès ADSL partagés entre plusieurs stations via un réseau physique dédié ;
- ➲ un logiciel d'accès à Internet ou navigateur ;
- ➲ un fournisseur d'accès à Internet (ou FAI). Il peut être gratuit ou non et proposer des services en ligne. Le paramétrage du navigateur permet de configurer le poste dédié à l'accès à l'Internet. Il tient compte des caractéristiques de l'abonnement souscrit auprès du FAI retenu.
- ➲ la politique de l'armée de terre concernant les raccordements au réseau Internet est définie dans la note n°81/DEF/EMAT/BMS I/R1 du 20 janvier 1998 ;

- la note n°717/DEF/EMAT/BPSI/A2 du 13 avril 2000 délègue, au directeur central des télécommunications et de l'informatique, la gestion des autorisations d'accès et des adresses et la note n° 796/DEF/EMAT/BPSI/A2 du 27 avril 2000 en précise les modalités ;
- politique Internet de l'armée de terre N° 501679/DEF/EMAT/BSIC du 02 décembre 2002.
- Règles de nommage des adresses Internet N° 501470/DEF/EMAT/BSIC/AD du 24 octobre 2002 ;
- sécurisation des sites Internet en "gouv.fr" N° 500186/DEF/EMAT/BSIC/SSIC du 07 février 2003 ;
- contrôle des sites Internet de l'armée de terre N° 500550/DEF/EMAT/BSIC AD du 04 avril 2003 ;
- directive pour la création d'un site Internet N° 500661/DEF/EMAT/BSIC/AD du 25 avril 2003 ;
- politique Internet V 2.3 N° 501066/DEF/EMAT/BSIC AD du 16 juillet 2003.

4. 2 Intranet

Un intranet est l'utilisation des techniques de l'Internet au service de l'informatique interne d'une entreprise ou d'un organisme.

- 4.2.a. Les services.

  Les services mis en œuvre par l'intranet de l'armée de terre (INTRATERRE) sont l'annuaire, la messagerie, le WEB, les forums et le transfert de fichiers. L'Intraterre s'interface avec les intranets du ministère de la défense et les intranet des autres ministères raccordés entre eux via des segments d'interface afin de former le réseau ADER.

- 4 .2.b. Organisation.

  Un intranet peut reposer sur plusieurs modèles d'organisation :

  - modèle centralisé : ce sont des serveurs centralisés, administrés par une entité particulière, et un processus formalisé pour développer et installer de nouveaux serveurs ;
  - modèle décentralisé : une liberté totale est laissée à chaque organisme pour mettre en œuvre les serveurs et y intégrer les informations de son choix ;
  - modèle "mixte" : une combinaison des deux modèles précédents.
  - L'intranet de l'armée de terre s'appuie sur un modèle "mixte":
  - pour les services offerts, seuls les services communs à l'ensemble de l'armée de terre sont décentralisés : annuaire global, listes de diffusion nationales, groupes de discussion à portée nationale, moteur de recherche. Un site web portail donne accès aux sites des différents organismes ;
  - en ce qui concerne l'organisation technique, des règles sont fixées pour le nommage (noms de domaines, adresses de messagerie, noms de

machines), ainsi que pour la coordination entre les services locaux et centraux (accès au réseau fédérateur, réplication entre serveurs).

Les grandes règles organisationnelles et techniques de l'intranet de l'armée de terre sont décrites dans la note intitulée "politique intranet de l'armée de terre" et diffusée par l'EMAT sous le numéro 817/DEF/EMAT/BPSI/A2 du 05 mai 1999.

4. 3 La visioconférence.

La politique d'emploi de la visioconférence repose sur la note n°913 /DEF/EMAT/BSIC/SC-S/23 du 28 juin 2002.

La visioconférence, mise en oeuvre par l'armée de terre, est composée d'ensembles fixes pour faciliter le commandement organique global et mobiles pour faciliter le commandement opérationnel circonstanciel des grandes unités projetées.

La visioconférence est un service associant l'image et le son. De plus, elle offre la possibilité d'échange de fichiers ou de documents dans une communication entre plusieurs sites. Pour établir une communication en visioconférence au delà de deux sites, il est nécessaire d'utiliser un équipement supplémentaire appelé pont de visioconférence, en anglais Multipoint Control Unit (MCU).

Le pont de visioconférence permet à des participants situés à des endroits géographiquement différents et utilisant divers réseaux de télécommunications (tel que le RNIS public, le RNIS privé : SOCRATE/MTGT, les réseaux IP) de participer à une visioconférence multi sites.

D'autre part, afin de pouvoir communiquer avec quiconque quel que soit le système, pour assurer l'inter fonctionnement, il est indispensable d'implanter des passerelles au sein des divers réseaux de communications.

Le débit nominal d'un terminal de visioconférence est de 384 kbps sur un réseau RNIS et équivalent en IP. Toutefois, en fonction de la ressource disponible sur les réseaux supports et transports, ce débit peut-être de 256, voire 128 kbps s'il est jugé suffisant en terme de qualité d'image.

La sécurisation des informations échangées entre les différents ponts multipoints et sites du système est réalisée par des boîtiers de chiffrement d'artères, agréés pour traiter des informations jusqu'au niveau "confidentiel défense" et "confidentiel OTAN".

Les systèmes déployés et mis en service dans leur globalité entre septembre 1999 et mars 2000 ont permis de réaliser un réseau fixe lourd en meubles pour salles (système en version infrastructure) et un réseau mobile lourd en conteneurs (système en version projetable). Les équipements de ces deux réseaux sont en cours de rénovation.

5 – L’INFORMATIQUE

5 1. La bureautique.

La bureautique comprend l'ensemble des techniques de l'informatique et de la télématique appliquées aux travaux de bureau notamment en matière de traitement de texte, de communication de la parole, de l'écrit et de l'image.

1998 marque le début des achats par la chaîne TEI de micro-ordinateurs et des périphériques associés au profit de l'ensemble des organismes de l’armée de terre. Depuis le 23 mars 2001, le ministère de la défense s'est doté de capacités propres d'achat de matériels informatiques en notifiant le marché convention GAIA (Groupement des Achats Informatiques des Armées). La Chaîne TEI réalise ses opérations d'achats conformément à ce marché.

Le renouvellement de ces équipements est prévu dans le schéma directeur de l'informatique. L'EMAT précise les durées de vie des équipements qui sont actuellement de 5 ans pour les postes de travail et de 3 ans pour une imprimante.

La prise en charge du soutien de la bureautique de l’armée de terre par la chaîne TEI concerne les matériels non consommables achetés par la chaîne à compter de 1998, et s'exerce à l'issue de la garantie constructeur (3 ans pour les micro ordinateurs).

5 2. L’infoservice.

Un infoservice est un système d'information ayant pour but la consultation sélective de bases de données par des utilisateurs autorisés. Il s'agit d'un outil d'aide à la décision.

La machine supportant ces bases de données, sur lequel les différents organismes autorisés par l'EMAT/BSIC, peuvent installer un, voire plusieurs infoservices, est appelée "infocentre"national. Dans le cadre de la fonction TSI, la chaîne TEI a pour mission d'assurer l'exploitation des infoservices hébergés sur cette machine.

La mise en place d'un infoservice nécessite divers développements. Les structures d'accueil, les programmes de translittération et de chargement, les requêtes et les univers sont à la charge des BOSI et BDI des organismes. Un contrat de service est établi entre les organismes demandeurs et la DCTEI. Ce contrat définit les besoins en ressources et en exploitation pour les infoservices.

Lorsque l’infoservice est développé, l’équipe du CTEI N procède à l'intégration qui permet de tester techniquement et fonctionnellement l'infoservice en environnement de production.

6 – LA GESTION DU SPECTRE ELECTROMAGNETIQUE

Les cadres interarmées et interalliés des opérations ont mis en avant l'exigence d'interopérabilité pour les échanges d'informations et l'adoption de modes de fonctionnement communs pour l'ensemble des nations participantes. L'organisation du commandement et des procédures appliquées par l'OTAN lors des différentes opérations récentes s'impose de plus en plus comme « standard » dans l'ensemble des opérations multinationales et nationales menées aujourd'hui. Cette organisation repose sur une centralisation de la responsabilité de la gestion du spectre électromagnétique pour l'ensemble du théâtre d'opération.

6 1. Les acteurs.

Aujourd'hui, au sein du secteur des radiocommunications de l'Union Internationale des Télécommunications (dépendant de l'ONU), le Règlement des Radiocommunications (RR) est mis à jour tous les deux ou trois ans lors des Conférences Mondiales des Radiocommunications (CMR). Ce document a valeur de traité international.

Grâce aux comités civils et militaires, il a pu être établi un accord sur les fréquences (NJFA : NATO Joint Frequency Agreement) qui s'impose à la communauté militaire mais aussi aux administrations des pays concernés. Toutefois, lors d'un déploiement sur un théâtre d'opérations extérieures, la nation hôte et les nations invitées sont des acteurs à part entière avec des rôles bien identifiés.

6 2. Les nations.

L'allocation de spectre au niveau international est décrite dans le règlement des radiocommunications de l'UIT. Au sein de chacune des trois régions de l'UIT, chaque nation exerce son droit souverain à l'utilisation du spectre.

Reconnu par la constitution de l'UIT, le droit souverain de réglementer ses télécommunications revient à chaque état. En France, le cadre est fixé par la loi de 1996 et une Agence Nationale des Fréquences (ANFR) a été créée en janvier 1997 pour la gestion du spectre.

L'ANFR répartit et attribue les bandes de fréquences aux différents affectataires en conformité avec les prescriptions du Règlement des Radiocommunications et propose au premier ministre le Tableau National de Répartition des Bandes de Fréquences (TNRBF).

6 3. Le ministère de la Défense.

La Défense est un des 12 affectataires nationaux. Le ministre de la Défense fixe des priorités dans sa politique des SIC et la décline au travers d'un plan stratégique dont certains enjeux stratégiques font référence au patrimoine immatériel de la Défense, dont les fréquences.

Niveau Interarmées

La Direction générale des SIC (DGSIC) [21]

La DGSIC pilote et contrôle l'utilisation du spectre des fréquences de la Défense.

Dans le cadre de ses attributions, le directeur général élabore la politique générale en matière d'utilisation du spectre des fréquences de la Défense, tant au niveau national qu'international, et veille à la coordination des besoins en fréquences des utilisateurs du ministère.

La sous-direction communications électroniques et fréquences (SDCEF) de la DGSIC [22]

Appuyée par la DIRISI, la SDCEF est le correspondant privilégié des organismes extérieurs nationaux et internationaux, elle représente le ministère de la Défense au Conseil d'administration de l'ANFR, dans les négociations avec les autres affectataires, les réunions OTAN, ainsi que les conférences mondiales (CMR) et régionales (CRR) organisées par l'UIT.

Bureau fréquence de la DIRISI

La DIRISI dispose d'un bureau fréquences qui a repris l'appellation de "National Allied Radio Frequency Authority France" (NARFA FRANCE).

La DIRISI dans le cadre du «soutien fréquences» a pour principales missions :

- la préparation, la coordination et l'**assignation** des fréquences réservées et attribuées au profit des différentes armées, directions et services conformément aux directives de la DGSIC ;
- la préparation des données pour les cellules fréquences des états-majors de théâtre en cas de déploiement ;
- la cohérence des données pour faciliter les échanges entre l'UIT, l'ANFR, l'OTAN et le ministère de la Défense ;
- la tenue de la base interarmées des assignations de fréquences (BIAF).

Niveau Armée de terre

La politique et la gestion des fréquences radioélectriques dévolues à l'armée de Terre reposent principalement sur :

La cellule fréquences à l'EMAT

La cellule fréquences de l'EMAT est chargée de définir la politique de gestion du domaine des fréquences radioélectriques de l'armée de Terre et contribue à la défense des intérêts de l'armée de Terre au sein du Ministère et vis-à-vis du monde civil.

la cellule fréquences du CFAT

Compte tenu des spécificités des équipements de l'armée de Terre, le CFAT assure, par délégation de la DIRISI, la gestion des fréquences tactiques temporaires nécessaires à la préparation opérationnelle et à l'engagement des forces sur le territoire métropolitain

[21] La DGSIC est directement placée sous l'autorité du ministre de la Défense, un Officier Général Fréquences conseille le directeur.

[22] Les missions de la **SDCEF** reprennent celles dévolues jusqu'à présent au Bureau Militaire National des Fréquences **(BMNF)**.

Chapitre 2 – LA SECURITE DES SIC DE LA COMPOSANTE STRATEGIQUE

1 - La protection du secret

1.1 Généralités

Dans le contexte global et permanent de la guerre de l'information, la sécurité des systèmes d'information et de communication caractérise l'état de protection, face aux risques identifiés, qui résulte de l'ensemble des mesures générales et particulières prises pour assurer la **disponibilité**, **l'intégrité** et **la confidentialité** du système et de l'information traitée.

- **La disponibilité** est l'aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performances.

- **L'intégrité** du système et de l'information garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime. Lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est à dire la garantie de son origine et de sa destination.

- **La confidentialité** est le caractère réservé d'une information dont l'accès est limité aux seules personnes habilitées et ayant le besoin d'en connaître pour les besoins du service.

L'organisation déployée et les règles de protection du secret et des informations concernant la Défense nationale et la sûreté de l'État font l'objet de l'instruction générale interministérielle 1300/SGDN/SSD/DR du 25août 2003 et en interne armée de terre de la Voie Fonctionnelle SSI (VF SSI diffusée sous le n° 1631/DEF/EMAT/BSIC/SSIC/71/DR du 16 octobre 2001) et de la Politique de Sécurité Interne de l' armée de terre (PSI AT diffusée sous le n° 500272/DEF/EMAT/BSIC/SSIC/DR du 08 mars 2007).

1.2 Besoins de sécurité

Dès le stade de la conception d'un système d'information et de communication, la déclinaison des objectifs de sécurité correspondant à l'emploi du système résulte d'une analyse de vulnérabilités corrélée aux menaces pertinentes vis-à-vis de la fonction opérationnelle et du contexte d'emploi du système considéré.

La chaîne TEI, comme les administrations et services déconcentrés de l'État, est tenue de mettre en œuvre toutes les mesures organisationnelles et techniques visant à assurer la protection des informations qu'utilise l'armée de terre. Les mesures techniques traitent les 3 domaines de la SSIC[23]:

- ➲ La sécurité informatique ;
- ➲ le chiffre et la sécurité des communications ;
- ➲ les protections contre les signaux parasites compromettants.

C'est une obligation légale, dès lors qu'il s'agit d'informations classifiées de défense (TSD, SD, CD[24] [1]) et réglementaire pour les informations sensibles n'ayant pas une confidentialité de défense.

---

[23] SSIC : sécurité des systèmes d'information et de communication.
[24] TSD, SD, CD: très secret défense, secret défense, confidentiel défense.

L’armée de terre utilise des systèmes d'information et de communication automatisés. Ces systèmes sont souvent reliés entre eux par des systèmes de transmission permettant l'accès au partage d'un grand nombre d'informations. De fait, l'ouverture recherchée pour l'amélioration des échanges augmente la vulnérabilité des organismes.

La menace pesant sur les systèmes est complexe et étroitement liée à l'évolution des technologies et aux comportements des utilisateurs. Pour s'en préserver, il faut être capable de déterminer ce qui doit être protégé, contre qui et à quel coût. Seule une analyse méthodique de risques, objective et structurée, peut permettre :

1 d'identifier les vulnérabilités potentielles et les modes d'attaques associés ;

2 de définir les parades nécessaires et leurs coûts d'acquisition, de mise en œuvre et de maintien en condition opérationnelle.

1.3 Maîtrise du risque

Associée à la notion de risques, la SSIC a pour objet la dissuasion, la prévention, la détection et la réparation des atteintes susceptibles d'entraîner des conséquences inacceptables pour les missions de l’armée de terre.

L'augmentation combinée des menaces et des vulnérabilités des systèmes conduit à la croissance du risque. La maîtrise du risque consiste à fixer des objectifs de sécurité au travers d’une FEROS[25] Ces objectifs se déclineront en règle de sécurité pour le système considéré au sein d’une PES[26]. L’armée de terre s’est dotée de la démarche d’assurance sécurité ORION[27] pour aider les RSSI[28] de projet dans ce travail.

Les mesures spécifiques de protection dans les domaines du chiffre, des transmissions, de l'informatique et des installations techniques font l'objet de la démarche de sécurisation SELATER et du SIC109.

1.4 Chaîne fonctionnelle

On trouve respectivement du niveau de l’EMAT, en passant par la RT ou tête de chaîne et jusqu’au niveau organisme un officier responsable de la sécurité des SIC : l’OSSIC

[25] FEROS : fiche d’expression rationnelle des objectifs de sécurité ;
[26] PES : procédures d’exploitation de la sécurité.
[27] ORION : démarche d’assurance sécurité pour la conduite des projets SIC
[28] RSSI : responsable sécurité du système d’information dans un projet.

2 – SECURITE INFORMATIQUE

Les systèmes informatiques permettent d'obtenir rapidement et subrepticement de grandes quantités d'informations sensibles. Cette vulnérabilité est accrue par l'emploi d'ordinateurs individuels autonomes, en réseau ou faisant fonction de terminaux intelligents pour un ordinateur central ou un serveur.

La sécurité informatique a pour but de limiter les risques identifiés en prenant des mesures techniques et non techniques (organisationnelles ou environnementales) correspondant aux objectifs de sécurité fixés.

La conception des moyens de protection, leur gestion, leur maintenance ainsi que l'exploitation des fonctions de sécurité ne peuvent être confiées qu'à des personnes justifiant le besoin d'en connaître et formées à cet effet sur le plan technique et réglementaire.

2.1 Contrôle d'accès.

Le contrôle d'accès physique aux locaux constitue la première mesure de sécurité. Les différentes zones où sont traitées et stockées des informations, sont protégées en fonction de la sensibilité de ces dernières. Pendant l'absence du personnel, les locaux où se trouvent les postes de travail doivent être fermés à clé. Les locaux de plus grande vulnérabilité doivent être contrôlés par un système anti-intrusion et éventuellement équipés d'un système d'alarme.

Le contrôle d'accès des personnels aux matériels constitue la seconde mesure de sécurité importante. L'accès aux ressources informatiques n'est accordé qu'aux personnes ayant le besoin d'en connaître. Chaque utilisateur, responsable du poste de travail mis à sa disposition, veille à respecter les consignes de sécurité ; il signe une attestation de reconnaissance de responsabilité. L'accès aux systèmes d'information se fait grâce à l'attribution d'un profil, qui confère à l'utilisateur des droits qui lui sont propres. Le contrôle d'accès logique utilise le plus souvent un mécanisme à base de mot de passe (phase d'authentification).

2.2 Protection des systèmes.

Assurer la sécurité physique des systèmes d'information et de communication consiste à appliquer des mesures environnementales visant à prévenir et limiter les risques d'incendie, de variations électriques, de fumées ou de variations de température, etc.

Les mesures de sauvegarde permettent d'assurer une protection des données. Cette responsabilité incombe à l'utilisateur et à l'administrateur. Ce dernier doit veiller à stocker les sauvegardes dans des lieux distincts des zones d'exploitation.

Tous les postes de travail et les serveurs interconnectés doivent être protégés par l'antivirus de l'armée de terre. Ce logiciel est destiné à éviter la duplication et l'activation de code malveillant susceptible de perturber le fonctionnement du système d'information et de communication. La mise à jour régulière de sa base de signatures de virus connus permet de diminuer la probabilité d'agressions virales. La configuration des équipements informatiques permet souvent d'effectuer des paramétrages assurant un niveau de sécurité supérieur à la configuration " par défaut ". Des guides de paramétrage facilitent cette démarche. Ils sont disponibles sur le site SSI de l'armée de terre.

2.3 Protection de l'information transportée.

La protection de l’information transportée est assurée d’une part par l’architecture déployée et notamment par le cloisonnement, et d’autre part au travers de la mise en œuvre d’équipements de sécurité réseau afin de protéger le transport.

La protection du transport de l'information repose sur l'utilisation de moyens de chiffrement. Ces moyens sont obligatoirement agréés lorsqu'ils traitent de l'information sensible classifiée de défense, ou cautionnés lorsqu'ils traitent de l'information sensible non classifiée de défense (DR, CONF. PERSONNEL, CONF. MEDICAL, CONF. ENTREPRISE, …).

3 - LE CHIFFRE.

- **3.1 Domaine d'action.**

Le chiffre est l'ensemble des moyens de cryptologie, matériels, documents et logiciels dénommés **ACSSI** pour Articles Contrôlés SSI, permettant de transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou de réaliser l'opération inverse.

Le chiffre augmente le niveau de confiance que l'on peut accorder à un système d'information et de communication. Il assure la protection de l'information à transmettre, quelles que soient la nature et la qualité de la chaîne de liaison utilisée. Cette protection est principalement un service de confidentialité, mais également d'intégrité au titre de l'authentification de l'émetteur et de la garantie du contenu.

La qualité du service fournie par le chiffre repose sur:

- la qualification et l'habilitation des personnels ;
- l'herméticité des systèmes de chiffrement ;
- la conformité des locaux aux normes de sécurité matérielle et de zonage (pour les rayonnements) ;
- la maîtrise des conditions d'élaboration, de diffusion, de conservation et d'utilisation des ACSSI (voie technique du chiffre) ;
- la stricte application des règles d'emploi des systèmes et des règles de conservation et de diffusion des informations traitées ;
- le contrôle rigoureux de ces mesures.

- **3.2 Confidentialité et intégrité.**

Le chiffrement permet la protection des informations pour les rendre inintelligibles et non modifiables à toute personne n'ayant pas le besoin d'en connaître ou le besoin d'en modifier. Il est obligatoirement assuré par des équipements agréés, lorsqu'il s'agit d'informations sensibles classifiées de défense.

La clé est le paramètre secret fondamental qui intervient dans le processus de chiffrement et de déchiffrement de l'information. C'est sur elle que repose, en grande partie, la sécurité offerte par le chiffre.

Les réseaux de chiffrement sont constitués par l'ensemble des correspondants organisés entre eux pour échanger des informations chiffrées.

On peut les distinguer par leurs fonctionnalités :

➲ le réseau téléphonique qui permet, grâce à ces équipements de cryptophonie, la confidentialité des conversations téléphoniques et la protection des télécopies ;

➲ le réseau télégraphique qui permet d'offrir un service de confidentialité allant jusqu'au niveau " secret défense ", en desservant une large majorité d'organismes en métropole et outre-mer ;

➲ les réseaux à intégration de services et à commutation de paquets qui disposent de chiffreurs d'artères et d'extrémité protégeant la transmission des données

- **3.3 Authentification et signature.**

La Messagerie Universelle SEcurisée (MUSE) est un système d'information, qui offre un service de messagerie permettant de traiter des informations classifiées de défense. Outre la confidentialité, ce système permet d'utiliser un mécanisme de signature électronique. Cette transformation cryptographique authentifie le signataire de façon formelle, préserve l'intégrité des données signées et ajoute une fonction de non répudiation.

Le déploiement d'une infrastructure de gestion de clés complète ce service.

- **3.4 Gestion des ACSSI.**

La gestion des articles contrôlés de la SSI s'effectue à travers deux chaînes distinctes (TEI et Matériel), dont les procédures sont décrites dans l'ordre de base des ACSSI de l’armée de terre (OBATAC).

L'instruction interministérielle 910/DISSI/SCSSI/DR du 19 décembre 1994 impose une gestion spécifique aux ACSSI. Cette gestion, centralisée, permet en particulier de connaître en permanence la position des ACSSI. Leur suivi est assuré au travers de la voie fonctionnelle SSI et de la voie technique du chiffre. Les ACSSI sont comptabilisés individuellement.

La directive 911/DISSI/SCSSI/DR du 20 juin 1995 précise que la comptabilité des ACSSI classifiés de défense doit être conforme à l'IGI 1300, mais elle est séparée de celle des autres documents et matériels classifiés. Les règles de traitement des ACSSI sont néanmoins différentes de celles des documents classifiés de défense " normaux ", en ce sens que leur sensibilité particulière est bien affirmée par cette directive.

L'ensemble de ces prescriptions implique donc un système de gestion indépendant, qui réclame des mesures de protection dues à la compilation des informations sensibles.

4 – PROTECTION CONTRE LES DES SIGNAUX PARASITES COMPROMETTANTS

4.1 La menace TEMPEST

Les systèmes d'information et de communication fonctionnent à partir de matériels électriques, qui génèrent des perturbations électromagnétiques durant leur fonctionnement. Certaines de ces perturbations sont corrélées avec des informations traitées et qualifiées dans ce cas de " signaux parasites compromettants " (SPC). Leur interception et leur exploitation, en vue de rétablir l'information traitée, constituent la menace TEMPEST (Total Electronic and Mechanical Protection against Emission of Spurious Transmissions).

Les perturbations tendent à se propager vers l'espace extérieur suivant deux manières :

- ➲ par rayonnement en espace libre ;
- ➲ par conduction sur les conducteurs reliant le matériel ou sur les matériels voisins.

Il est possible d'exploiter des SPC à des distances variant de quelques dizaines de mètres pour les parasites rayonnés, à plusieurs centaines de mètres pour les parasites conduits. La distance à laquelle les SPC sont exploitables peut être augmentée notamment par la présence de fréquences porteuses fortuites, qui peuvent être modulées par les SPC et les transporter ainsi à des distances insoupçonnées.

Les précautions à prendre pour l'installation des équipements font l'objet de l'Instruction Interministérielle 300/SGDN/TTS/DR du 20 juin 1997 et du volume 5 du TRS 109[29]. Il s'agit en particulier :

- ➲ d'utiliser des matériels spécialement conçus pour limiter les émissions de SPC ;
- ➲ d'empêcher la capture de ces signaux parasites en créant des zones de sécurité permettant la surveillance ;
- ➲ d'empêcher ou de limiter au maximum la propagation des parasites, en filtrant les conducteurs de ligne et d'alimentation (électrique, téléphone, eau, climatisation, évacuation, …), en isolant électriquement les équipements.

La protection contre les SPC est obligatoire pour le traitement des informations sensibles classifiées de défense (IM 900) et recommandée pour le traitement d'informations sensibles non classifiées de défense (recommandation 901).

4.2 Zonage.

Le zonage TEMPEST sert à limiter les coûts imposés par la protection contre les SPC. Ce zonage s'effectue en tenant compte de la menace TEMPEST et en utilisant le bon équipement à la bonne place. La directive de zonage TEMPEST est la note n°495/SGDN/TTS/SSI/DR du 19 septembre 1997.

[29] TRS 109: Règlement de sécurité des communications (document de base de la SSI).

Le zonage comporte deux volets: le zonage des locaux et le zonage des matériels.

➲ Le zonage des locaux consiste à classer ces derniers en quatre zones 0, 1, 2 ou 3 selon l'affaiblissement qu'ils présentent par rapport à la limite de la zone de sécurité. Le zonage des locaux ne prend en compte que les SPC pouvant être émis en rayonnement.

➲ Le zonage des matériels consiste à classer ces derniers en quatre catégories A, B, C ou D selon leur degré de protection face à la menace TEMPEST.

4. 3 Cages de Faraday.

Les cages de Faraday, du nom de l'inventeur Michael Faraday, sont des dispositifs à parois conductrices, qui permettent d'isoler électriquement les corps placés à l'intérieur. Elles utilisent aussi la propriété du " blindage " qui provoque un affaiblissement de l'énergie électromagnétique " rayonnée ".

Afin de réduire l'énergie " conduite " des perturbations électromagnétiques, les liaisons avec l'extérieur sont assurées par des conducteurs électriques associés à des filtres conformément à la directive d'installation n° 485/SGDN/DCSSI/DR du 01 septembre 2000, à l'exception du conducteur de liaison de terre.

Il existe deux utilisations possibles d'une cage de Faraday :

- ➲ protéger un matériel installé à l'intérieur des perturbations électromagnétiques générées à l'extérieur, dans le cas de mesures de " CEM " (Compatibilité ElectroMagnétique) ou de protection contre l'" IEMN " (Impulsion ElectroMagnétique Nucléaire) ;
- ➲ réduire à l'extérieur de la cage, de manière significative, les perturbations électromagnétiques générées par un matériel installé à l'intérieur, dans le cas de l'ACEM (Anti-Compromission ElectroMagnétique) ou également appelé TEMPEST.

En terme d'exploitation, ces cages reçoivent des équipements permettant l'élaboration, le traitement, la modification et l'émission-réception d'éléments classifiés de défense en s'affranchissant des contraintes de zonage évoquées dans la directive n° 495. Leur rôle d'écran vis-à-vis de l'" IEMN " permet de garantir une fonction de disponibilité élevée.

CHAPITRE 3 - LES RESEAUX DE TELECOMMUNICATIONS LONGUE DISTANCE

1 – LES TRANSMISSIONS LONGUE DISTANCE ET OUTRE MER

1.1 Les transmissions par satellites

Elles ont un caractère interarmées très marqué et permettent d'assurer les liaisons (téléphonie, télégraphie, transmission de données, télécopie) entre le haut commandement national et les éléments des forces armées projetés ou prépositionnés, déployés dans les zones de couverture du satellite.

1. 2 Les transmissions par radio HF

La rénovation des stations HF fixes et du raccordement aux réseaux d'infrastructure des forces déployées, qu'elles soient terrestres ou maritimes, est réalisée dans le cadre du programme MATILDE (Modernisation et Amélioration des Transmissions Interarmées Longue DistancE).

Les moyens de transmissions sont répartis sur différents types de sites :

➲ Outre-mer, MATILDE est déployé sur : les DIRISI outre mer, les sites isolés (sites fixes de l'Armée de Terre).

➲ En métropole, MATILDE est déployé sur : les sites accueil métro HF, stations métropolitaines de l'OMAR[1] , les stations d'accueil CARTHAGE[2], les sites accueil métropolitains SATCOM, les sites Régions Terre pour les utilisateurs de l'Armée de Terre.

Les forces projetées dotées de CARTHAGE et situées à moins de 1000 km des sites distants peuvent accéder aux services de MATILDE. Ces forces sont appelées *CARTHAGE OM* .

Enfin, les navires en portée HF d'un site distant et ayant une composante Marine peuvent accéder aux services de MATILDE. Ces navires sont appelés *OMAR OM* .

1. 3 Les transmissions d'outre-mer :

Chaque commandement d'outre-mer (la plupart du temps interarmées) dispose d'un système de télécommunications moderne pour assurer les raccordements vers la métropole, les liaisons locales et le raccordement d'unités déployées.

1.3.a. L'OMIT.

L'Organisation Mondiale Interarmées des Transmissions assure, par un réseau à couverture mondiale et par interfaces adaptées, les liaisons entre le HCN et les commandements d'outre-mer, ainsi que les liaisons de ces

commandements entre eux. Il permet également de raccorder au HCN des éléments engagés outre-mer.

C'est au sein des Éléments Interarmées de Transmissions (EIT) que sont mis en œuvre les moyens de transmissions de l'OMIT, radio HF ou station SYRACUSE.

1.3.b. Les liaisons internes.

Elles relient le Commandement Supérieur (COMSUP) considéré et les formations placées directement sous ces ordres. Elles sont réalisées à l'aide de moyens radioélectriques.

1.3.c. Les DAT.

Aux ordres de l'Etat-major des Armées (EMA), les **détachements autonomes de transmissions** participent aux missions de recherche du renseignement d'origine électromagnétique.

1.3.d. Les MTGT (Moyens de Transmissions Garnisons Terre).

Dans sa configuration actuelle, le réseau MTGT consiste essentiellement en une réorganisation du réseau sur une nouvelle architecture. La nouvelle génération d'autocommutateurs ALCATEL 4400 constituera le noyau dur des futurs moyens de transmissions. Ils offriront :

- ➲ le confort du numérique ;
- ➲ l'intégration de voix, données et multimédia ;
- ➲ la simplification des procédures grâce au plan de numérotation interarmées (PNIA) ;
- ➲ la fiabilité ;
- ➲ l'indépendance vis-à-vis des opérateurs publics ;
- ➲ une ouverture vers les réseaux tactiques et stratégiques interarmées via SYRACUSE.

---

[1] Organisation Maritime des transmissions haute fréquence

[2] Communications Automatisées Radioélectriques Tactiques HF en Ambiance de Guerre Electronique

CHAPITRE 4 - LES SYSTÈMES D'INFORMATION

1 - GÉNÉRALITÉS

Le terme "système d'information" désigne, un ensemble structuré et cohérent de ressources (humaines, organisationnelles, techniques et financières) et de procédures permettant de recevoir, traiter, stocker et communiquer en temps opportun les données informatiques utilisées par un organisme afin qu'il remplisse ses missions.

On distingue deux types principaux de systèmes d'information :

➲ **application** : logiciel conçu et développé pour remplir une fonction spécifique d'un organisme, selon des règles de gestion qui lui sont propres. Il automatise tout ou partie des tâches entrant dans les attributions de ses utilisateurs. Une application est liée soit à :

- un métier (RH, logistique, etc.) ;
- des services transverses de base (annuaire, nom de domaine, etc.) ;
- des services communs (messagerie, travail collaboratif, etc.).

➲ **progiciel** : logiciel ou ensemble de logiciels réalisant une fonction générale, développé par un éditeur, utilisé ensuite par un organisme de manière native ou moyennant un paramétrage permettant de l'adapter à un contexte fonctionnel spécifique, en particulier :

- tableur ;
- traitement de texte ;
- présentation assistée par ordinateur.

Un système d'information comprend des équipements informatiques qui lui sont propres et s'appuie généralement sur des ressources informatiques et de télécommunications partagées avec d'autres systèmes (réseau local, de desserte ou de transport).

Parmi les ressources informatiques, certains logiciels, généralement objets de normes ou de standards, revêtent une importance particulière :

➲ **logiciel d'exploitation** (logiciel de base) : logiciel indépendant de toute application, régissant l'exécution des programmes et pouvant remplir des fonctions telles que l'affectation des ressources, l'ordonnancement, la gestion des entrées et sorties et des données ;

➲ **logiciel de soutien** : logiciel ou programme qui aide au développement, à la maintenance ou à l'utilisation d'autres logiciels ou qui fournit des fonctions générales, indépendantes des applications, en particulier :

- compilateur ;
- système de gestion de base de données ;
- infrastructure de gestion de clefs ;
- annuaire.

Un serveur est une unité fonctionnelle qui fournit des services partagés à des stations de travail ou à d'autres unités fonctionnelles sur un réseau de données.

Les serveurs constituent par ailleurs des ressources informatiques importantes.

Les serveurs hébergent les types de services suivants :

➲ Services d’usage général

• services de base (DNS, WINS, gestionnaires de comptes, pare-feux, PROXY, etc.) ;

• services de bureautique (partage de fichiers, gestionnaires d’imprimantes, etc.) ;

• services communs : Web, messagerie, travail collaboratif, annuaire, FTP, listes de diffusion, système de diffusion de correctifs (systèmes d’exploitation, antivirus, etc.),

• service de sécurité

➲ Services spécifiques

• services métiers en développement ;

• portails services métiers en production ;

• services communs intégrés métiers (portails Web applicatifs, portails d’intégration, individualisés, etc.).

Chaque chaîne reste propriétaire de son système d'information (SI) et en assure la maîtrise d'ouvrage.

Dans son périmètre technique la chaîne TEI fédère :

➲**Les services de communication** pour assurer le transfert de la voix, des images et des écrits (téléphonie, visioconférence, messageries, télégraphie et serveurs d’application associés).

➲**Les chaînes de liaisons** pour les logiciels de base, les réseaux locaux (câblage et éléments actifs), le transport des données (IP, x25, …), les supports (FH, fibres optiques, câbles) et les systèmes de communication

➲**Les réseaux de desserte**

➲**La sécurité des systèmes d'information** (SSI), de manière à préserver la disponibilité, l'intégrité et la confidentialité de ces systèmes.

2 - LE SYSTEME D'INFORMATION DE L'ARMEE DE TERRE (SIAT)

Le système d'information de l'armée de Terre (SIAT) comprend :

- ➲ les systèmes d'information d'administration et de gestion (SIAG),
- ➲ les systèmes d'information logistique (SIL),
- ➲ les systèmes de simulation de l'informatique de l'armée de Terre dédiés à la formation et à l'entraînement.

La politique générale de l'armée de Terre et les objectifs particuliers sur les différents systèmes sont décrits dans les volets stratégiques et opérationnels du schéma directeur du SIAT (SDSIAT).

L'organisation du SIAT comprend pour l'essentiel des échelons de gouvernance, de conduite et de réalisation.

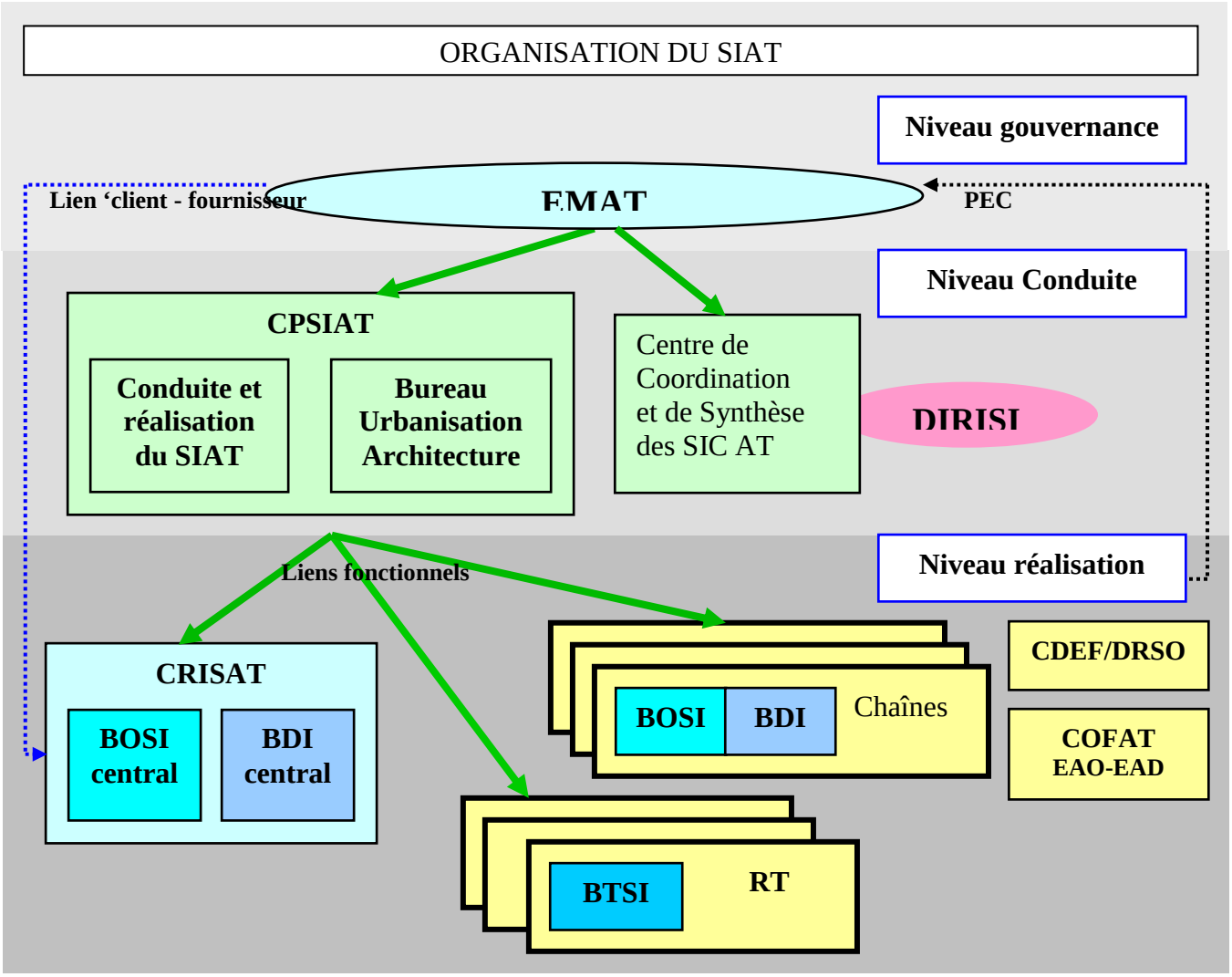
- ➲ Échelon de gouvernance : organisation possédant la capacité de définir la stratégie d'action et de fixer les objectifs relatifs au domaine des SI.

- ➲ Échelon de conduite : organisation possédant la capacité de coordonner et de contrôler les actions nécessaires à la réalisation des objectifs fixés par le niveau de gouvernance et de proposer des actions de son niveau.
  - Centre de Pilotage des Systèmes d'Information de l'Armée de Terre (**CPSIAT**)[30], constitué de deux bureaux : "Conduite SIAT" et "Bureau Urbanisation et Architecture".
  - Centre de Coordination et de Synthèse des SIC fixes de l'Armée de Terre (**CCSAT**), assure l'interface entre l'AdT et la Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information (**DIRISI**).

- ➲ Échelon de réalisation : organisation ayant la capacité de concevoir, de développer, d'installer et de maintenir le SIAT.
  - -Centre de Réalisation Informatique des Systèmes de l'Armée de Terre (**CRISAT**)[31], constitué d'un **BOSI** et d'un **BDI,** chargé de la réalisation des systèmes de l'EMAT et des organismes de l'AdT ne disposant pas d'entités de réalisation.
  - -Bureau Développement Informatique (**BDI**), attaché à un organisme de niveau central, en charge de la réalisation, de la maintenance des applications et de l'architecture technique des applications
  - -Bureau Organisation et Systèmes d'Information (**BOSI**), attaché à un organisme au niveau central ou local, réalisant l'assistance à maîtrise d'ouvrage. Il a aussi en charge la conception fonctionnelle

[30] CPSIAT : ses missions étaient assurées jusqu'en 2007 par CERSIAT/BAE
[31] CRISAT : ses missions étaient assurées jusqu'en 2007 par CERSIAT/BDI

du système d'information et le pilotage de son exploitation et de sa maintenance.
-Bureau Télécommunication et Systèmes d'Information (**BTSI**), entité des états-majors de RT chargée du suivi voire de coordonner le déploiement, participer au soutien fonctionnel des utilisateurs des systèmes d'information et des moyens bureautiques implantés dans sa zone de responsabilité.



3 - PRINCIPALES APPLICATIONS

- Il existe plusieurs dizaines d’applications au sein de l’arlée de terre, on en citera que quelques unes :
-
- **SAF2** (Système d'Aide aux Formations) : ce système apporte une aide à la gestion au profit des formations de l'armée de terre.
- **SIMAT** (Système d'information du MATériel) : ce système permettra de gérer l'ensemble des matériels de l'armée de terre.
- **SIRH** (Système d’information des ressources humaines).
- **SITRAG** (Système d'lnformation du génie).
- **CREDO** (Système de gestion et d'élaboration des documents d'organisation).
- **SIRIUS** (Système de gestion des matériels HCCA de la DCCAT).
- **PATRI** (Système de gestion et de programmation des travaux d'infrastructure du génie).

SECTION V - LA COMPOSANTE TACTIQUE DES TRANSMISSIONS

BUT RECHERCHÉ ET DONNÉES ESSENTIELLES	Cette section vise essentiellement à fournir une information sur le sy
RÉFÉRENCES	SIC 200 – SIC 603

Pour obtenir le meilleur rendement des moyens et adapter au mieux l'ensemble du système à la situation tactique, la manœuvre au niveau transmissions est centralisée entre les mains du commandant des transmissions du groupement de forces concerné (COMSIC).

La combinaison des systèmes d'information et de communications tactiques donne au chef interarmes la capacité de commandement.

3 éléments seront abordés de manière successive, le RITA 2G, les réseaux radios, les systèmes d'information de niveau tactique.

Chapitre 1 – ORGANISATION GENERALE DE LA COMPOSANTE TACTIQUE

Créés principalement pour une utilisation tactique, Les SIC tactiques intègrent généralement, en fonction des systèmes, des moyens de raccordement, des moyens de commutation, des réseaux locaux informatiques, des matériels d'extrémité. Ils sont utilisés, soit pour constituer une première ossature de télécommunication entre les PC projetés et la métropole, soit pour fournir des moyens de télécommunication légers dans le cadre d'opérations plus restreintes.

Les SIC tactiques appartiennent à la chaîne des forces. Le **CFAT** [32] est tête de chaîne pour le commandement des forces de manoeuvre. Plusieurs entités sont en charge des SIC sur le plan de la conception et de la mise en oeuvre.

La division SIC de l'état-major du CFAT est chargée de la conception des réseaux et systèmes d'information et de communications, de la sécurité des SIC, de la gestion du spectre. Elle planifie, en associant les **EMF**[33] concernés l'ensemble des moyens SIC nécessaires aux différents engagements en liaison avec l'EMIA/TSI et l'EMA/CPCO et le CFLT/divsic.

La division SIC du CFLT [34] est chargée de la conception et de la sécurité des systèmes d'information logistiques. Elle s'assure, en liaison avec le CFAT, de la cohérence de l'ensemble de la fourniture des supports de communications et de la mise en place des moyens nécessaires à la chaîne logistique.

La division SIC de l'EMF est chargée, en liaison étroite avec le CFAT, de la conception et de la planification des réseaux et systèmes d'information et de communications, ainsi que de la sécurité des SIC du niveau de force qu'elle doit mettre sur pied (DIV OTAN ou PCIAT).

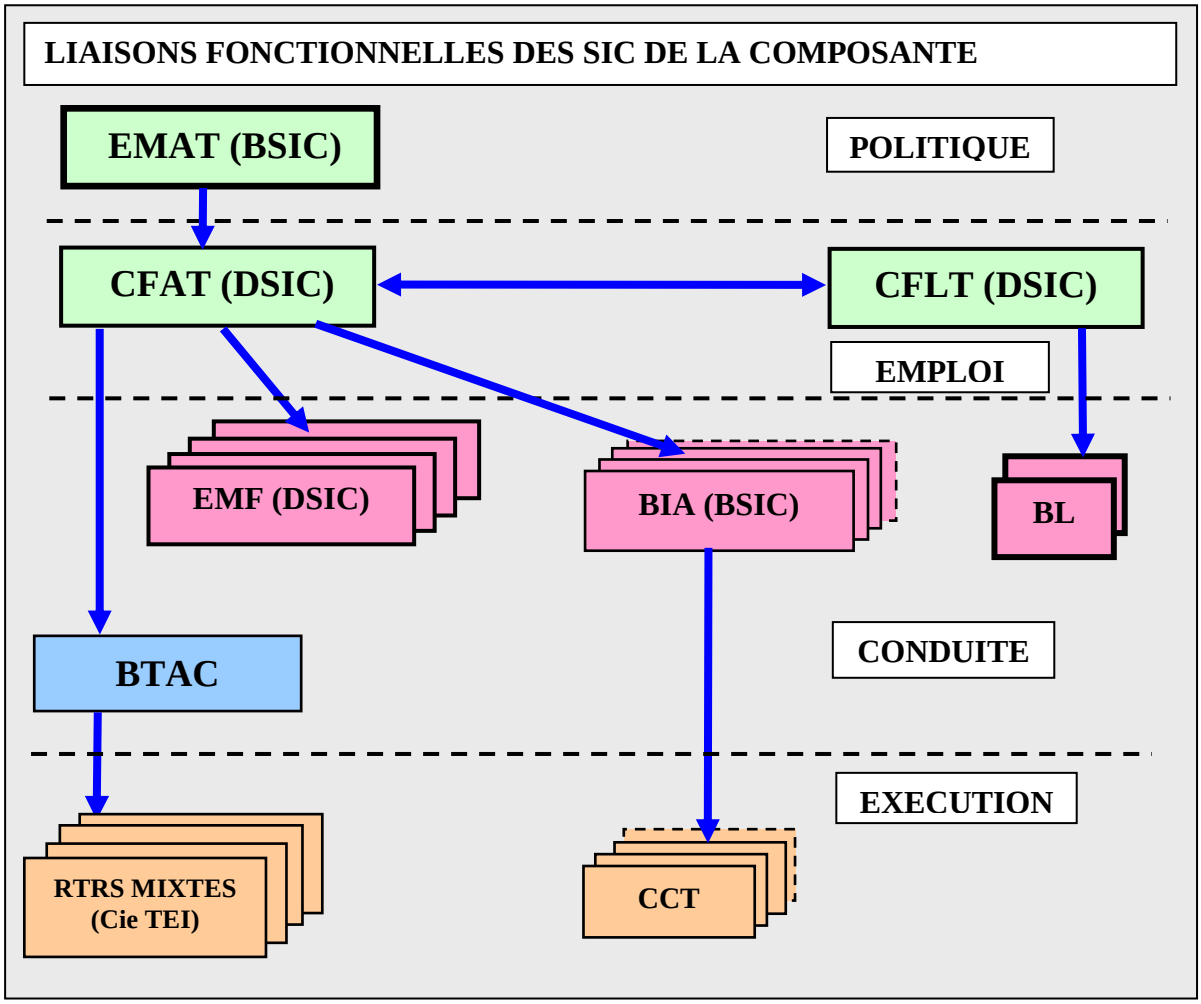
Le bureau SIC de la BIA[35] est chargé de la préparation opérationnelle de ses moyens SIC dédiés (CCT[36]) et des sections transmissions de ses unités. Si nécessaire, ce bureau contribue à la planification opérationnelle, tant au niveau de la BIA qu'avec les échelons supérieurs.

Le bureau SIC de la BL[37] est chargé de la préparation des moyens SIC dédiés aux systèmes d'information logistiques opérationnels.

La Brigade de transmissions et d'appui au commandement (BTAC) est chargée de la mise en oeuvre des systèmes de transmissions pour les niveaux 1 et 2, ainsi que pour le niveau 3, lequel dispose cependant de sa CCT.

---

[32] CFAT: Commandement de la Force d'Action Terrestre.
[33] EMF: Etat Major des Forces.
[34] CFLT: Commandement de la Force Logistique Terrestre.
[35] BIA: Brigade Inter Armes.
[36] CCT: Compagnie de Commandement et de Transmissions.
[37] BL: Brigade Logistique.


LIAISONS FONCTIONNELLES DES SIC DE LA COMPOSANTE
EMAT (BSIC)
POLITIQUE
CFAT (DSIC)
CFLT (DSIC)
EMPLOI
EMF (DSIC)
BIA (BSIC)
BL
BTAC
CONDUITE
EXECUTION
RTRS MIXTES
(Cie TEI)
CCT

CHAPITRE 2 - LE RESEAU INTEGRE DE TRANSMISSIONS AUTOMATIQUE (RITA) 2G

1 - PRESENTATION GENERALE

RITA 2G - réseau intégré de transmissions automatique, est issu de la valorisation de RITA 1G.

Il constitue l'épine dorsale du **réseau tactique** de zone car il est composé de :

➲ moyens de commutation assurant le transit et le raccordement des communications des abonnées,

➲ supports de transmissions raccordant les commutateurs entre eux.

RITA 2G assure l'intégration des réseaux tactiques français et alliés, civils et militaires ainsi que l' interopérabilité des différents supports et applications.

L'évolution liée à l'aspect lacunaire des espaces d'engagements amène à déployer les postes de commandement (PC) de tous niveaux dans des zones contrôlées plus ou moins vastes.

Ainsi se créent différentes **zones de PC** (ZPC) plus ou moins éloignées les unes des autres, constituant des **bulles** reliées par le réseau RITA.

Ce système déploie sur le terrain un **maillage évoluant au rythme de la manœuvre interarmes**.

Le maillage est constitué de nodes implantés sur des points hauts ; tous sont reliés entre eux par des jonctions hertziennes appelées jonctions de maillage.

La plupart des PC sont raccordés aux nodes de maillage par des liaisons appelées jonctions de raccordement.

Les abonnés mobiles (GTIA, compagnies…) se raccordent à ce réseau par la radio de combat via un node de déport, pion tactique permettant une liaison permanente avec les PC.

Le réseau RITA est constitué de stations de commutation déployées et raccordées à l'aide du centre de commandement du réseau :

11. Le Centre de Commandement du Réseau (CECORE)

Le **CECORE** permet :

➲ la supervision automatique du réseau : jonctions réalisées, prévues et étudiées ;

- ➲ les calculs pour l'établissement de ces jonctions à partir du terrain numérisé ;

- ➲ l'établissement d'un plan de fréquences qui tient compte de l'environnement ;

- ➲ la tenue à jour du potentiel des moyens du réseau ;

- ➲ la génération et la diffusion des clés de chiffrement.

12. Les stations de commutation sont de trois types :

- ➲ stations **CMAI** : Centres Multiservices d'Accès et d'Interface dédiés au raccordement des dessertes d'abonnés filaires ainsi qu'au raccordement des autres réseaux,

- ➲ stations **CART** : Centres d'Accès Radio et de Transit assurant le raccordement automatique des abonnés radio mobiles et contribuant au maillage de zone,

- ➲ stations **CTRT** : Centres de Télé exploitation Radio et de Transit pour le raccordement radio des Réseaux de Combat (RdC) ou Combat Net Radio (CNR).

CHAPITRE 3 - LES RESEAUX RADIO

Utilisés pour le commandement « à la voix » des unités tactiques, les réseaux radios se sont développés pour fournir un moyen secours efficace du réseau tactique de zone abordée précédemment.

3 réseaux seront abordés :

- le réseau VHF (Very High Frequency)
- le réseau UHF (Ultra High Frequency)
- le réseau HF (High Frequency)

1 - Réseaux VHF

Le système radio PR4G assure au sein des grandes unités tactiques les liaisons internes des GTIA, celles des systèmes d’armes et le transit des transmissions de données correspondantes. Il a la capacité de s’intégrer sur le réseau tactique de zone RITA 2G.

2 - Réseaux UHF

Le système SATURN a été lancé en 1991 pour équiper certaines plates-formes de l’ALAT dans le cadre de la coordination 3ème dimension. Il ne permet pas une intégration automatique au réseau tactique de zone RITA 2G.

Le système MIDS-Terre limité aux systèmes de défense sol-air et aux systèmes embarqués à bord des aéronefs. L'emploi de ce système est confié à l'artillerie.

3 - Réseaux HF

Les réseaux HF sont employés, de manière générale, au sein de la composante terrestre pour les communications téléphoniques et la transmission de données à grande distance, en secours du réseau tactique de zone. Au niveau d'un LCC, deux réseaux radio sont mis en œuvre (système de commandement et logistique) en secours ou en complément du réseau tactique de zone. Il s'agit d'un réseau transmission de données et d'un réseau recueil HF. Un troisième réseau radio est mis en œuvre au profit du système de commandement : le réseau téléphonie de commandement.

La HF de nouvelle génération CARTHAGE offre aujourd'hui le support radio HF interne des forces terrestres. L'intégration HF automatique via le réseau de zone RITA 2G est techniquement prévue par colocalisation d'une station CARTHAGE sur le site d'intégration.

CHAPITRE 4 - LES SYSTEMES D'INFORMATION DE NIVEAU TACTIQUE

Les systèmes d'information relevant de l'informatique générale ou opérationnelle sont amenés à prendre une place de plus en plus importante en temps de paix, de crise ou de guerre.

Dans le cadre tactique, ces systèmes ont vocation à procurer une aide au commandement (SICF, SIR) ou à la mise en œuvre des systèmes d'armes.

À cet effet, ils offrent aux utilisateurs des outils informatiques évolués qui facilitent la tâche des utilisateurs en terme :

- d'évaluation de situation ;
- de coordination des moyens ;
- de composition automatique de messages ;
- de gestion de données complexes (logistique, renseignement...).

D'une exploitation de plus en plus simplifiée, proche des techniques relevant des logiciels de bureautique, les systèmes d'information sont au cœur d'une armée de haute technologie.

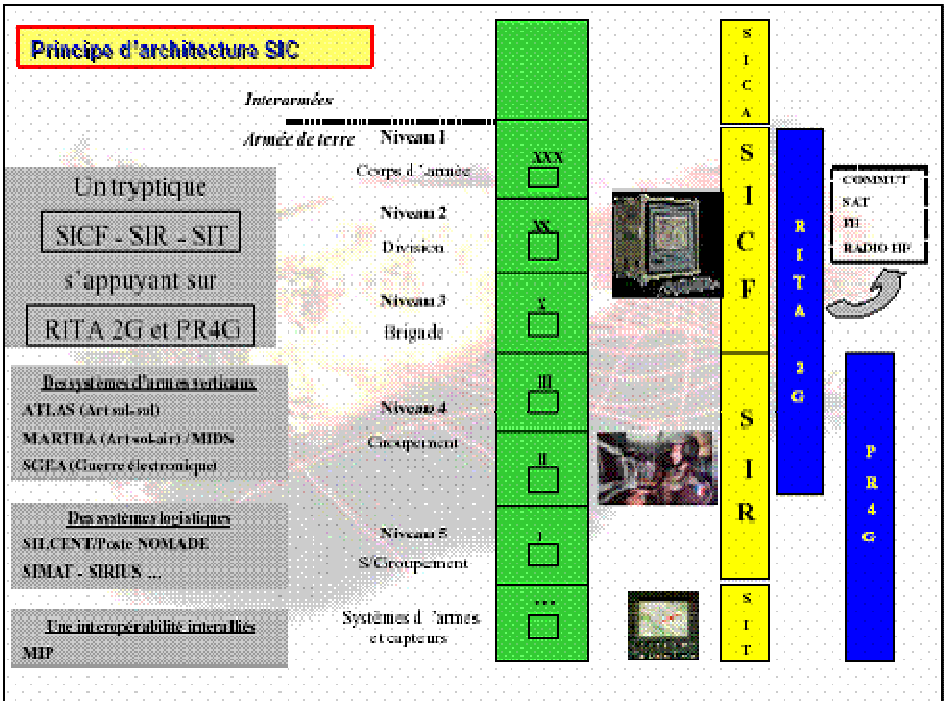
Ils garantissent une prise de décision rapide et optimisée.

Les échanges de données inter PC générés par le système d'information et de commandement des forces terrestres (**SICF**) s'effectuent par le biais du réseau tactique de zone.

Les applications supportées par les systèmes d'information terminaux (**SIT**) et régimentaires (**SIR**) transitent sur les réseaux tactiques du niveau brigade et en dessous ainsi que sur les réseaux commandement des régiments impliqués dans le déploiement de la logistique de théâtre.

Les systèmes d'information logistiques (**SIL**) au nombre desquels figurent SIMAT, SILCENT, SIRIUS, … et généraux (gestion, administration) transitent de même via ces différents réseaux.

Le schéma ci-dessous permet de mieux visualiser tous ces systèmes :



A compter de 2006, les "petits PC" et diverses entités tels que groupements tactiques interarmes et d'appui, détachements de liaison et de zones (logistiques) fonctionnelles, assureront au SIR et aux SIL un accès direct au réseau tactique de zone.

La combinaison des systèmes d'information et de communications tactiques donne au chef interarmes la capacité de commandement.

SECTION VI - LA COMPOSANTE OPERATIVE DES TRANSMISSIONS

BUT RECHERCHÉ ET DONNÉES ESSENTIELLES	Cette section vise essentiellement à fournir une information sur le système
RÉFÉRENCES	

Liens entre la métropole et les théâtres d'opération, les systèmes d'information et de communications du niveau opératif permettent à l'état-major des armées d'assurer le commandement opérationnel des forces en opération. Situés sur le territoire métropolitain et en projection sur les théâtres, l**es SIC opératifs** appartiennent à la Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information de la Défense (DIRISI) et sont mis en œuvre par le 41e Régiment de transmissions et le 8e Régiment de transmissions.

Le 41e RT est un régiment ayant statut d'Organisme à vocation Inter Armées/Terre (OVIAT) qui reçoit ses missions du SGDN et l'EMA (Etat-Major des Armées). Il met en œuvre des équipements de transmissions spécifiques qui utilisent essentiellement des satellites militaires dans le cadre du SYstème de RAdioCommunication Utilisant un SatellitE (SYRACUSE).

Chapitre 1 – LE SYSTEME SYRACUSE

1 - DESCRIPTION DU SYSTEME

1.1. Caractéristiques du réseau

Composante majeure du réseau de transit interarmées, réalisant l'interface entre les réseaux fixes et les réseaux des forces projetées par l'intermédiaire d'autres systèmes (réseau ARISTOTE, SOCRATE…), le système SYRACUSE (SYR) constitue un réseau de télécommunications durci face à une attaque d'origine électromagnétique.

Ce système est composé de deux sous-ensembles devant être utilisés conjointement (séparément de manière exceptionnelle) :

- le support satellitaire (composé d'un segment sol et d'un segment spatial) ;

- le système de commutation ARISTOTE (en tant que systèmes d'élongation et de desserte).

Plusieurs équipements contribuent à sa sécurité :

- l'antenne active du segment spatial ;

- les modems XXI, du segment sol, garantiront à l'horizon 2008 le maintien de services (débits réduits) en cas d'agression électromagnétique vers le satellite, jusqu'au niveau division. En deçà (niveau brigade et bataillon), cette capacité ne sera pas disponible pour des raisons techniques et de choix de conception ;

- les équipements de chiffrement d'artère qui équiperont les stations sol.

Le système SYRACUSE III s'appuie sur deux satellites (SYR3A et SYR3B) d'une durée de vie estimée de 15 ans, placés en orbite géostationnaire respectivement à 47°E et 05°W.

Ce dispositif demeure complété jusqu'en 2010 par les capacités des deux derniers satellites de la génération TELECOM II.

1.2. Fonctionnement et direction du réseau

Le chef d'état-major des Armées assure le commandement du réseau.

Par délégation, la division " Emploi " (EMA/EMPL /6) de l'EMA pilote le programme SYRACUSE, définit les règles d'emploi, coordonne les relations avec les alliés et arbitre les demandes de service si elles sont supérieures aux capacités disponibles.

Relevant du CEMA, la DIRISI assure la direction du réseau, la supervision, l'exploitation, le soutien de SYRACUSE. Chaque armée déploie ses propres stations autonomes.

Le Centre de Planification et de Conduite Syracuse Aristote (CPCSA) de la DIRISI est responsable de l'exploitation du réseau SYRACUSE.

Il administre et exploite ce réseau en permanence (H24) à deux niveaux :

- un niveau de direction, pour l'organisation générale de l'exploitation, de la planification et du maintien en condition opérationnelle du réseau métropolitain.

- un niveau de conduite temps réel, pour la supervision et la conduite des ressources du réseau (modems, bandes de fréquences, puissance sol et bord, configuration charge utile et équipements du réseau de télécommunications).

Il dispose d'un centre nominal situé à Maisons-Laffitte, avec une dévolution à la station métropolitaine de Favières.

2 - DESCRIPTION DU SERVICE OFFERT

2.1. Périmètre du service

Le périmètre du service est interarmées pour tous les clients opérationnels de chaque armée impliquée dans une OPEX, une MISINT ou un exercice.

Les différentes interfaces d'entrée de la DIRISI pour toute demande de ressource satellitaire ou dysfonctionnement d'une liaison déjà établie sont les suivantes :

- préparation d'un déploiement opérationnel et d'un exercice : Bureau Opérations ;
- dysfonctionnement d'une liaison : Centre Opérationnel de la DIRISI.

2.2. Caractéristiques du service

Le système assure la mise à disposition de supports de communication entre :

- les abonnés métropolitains des réseaux d'infrastructure et ceux de forces déployées (raccordement métropolitain);

- les abonnés d'un même théâtre (raccordement intra théâtre).

Chapitre 2 – LE SYSTEME ARISTOTE

ARchitecture Indépendante des Supports de Transmission Optimisant le Transit d'Elongation

1 - DESCRIPTION DU RESEAU

1.1. Caractéristiques du réseau

Le système ARISTOTE est un réseau de transit « longue élongation », basé sur le modèle du réseau de transit métropolitain SOCRATE.

C'est le réseau de commutation entre les réseaux outre-mer et projetés (OMIT, réseaux tactiques des Armées, unités opérationnelles) et les réseaux fixes.

Constitué d'un « coeur de transit » métropolitain, organisé autour de **trois Noeuds Métropolitains de Transit (NMT) colocalisés avec les stations métropolitaine SYRACUSE** et reliés entre eux par des artères de commutation issues du réseau SOCRATE, il assure le raccordement de noeuds tactiques (terrestres et naval) déployés. Il est à ce titre l'interface unique d'entrée du système SYRACUSE.

Son architecture fédère et optimise l'utilisation des ressources de transmissions satellitaires ou de liaisons transcontinentales, entre :

- la métropole et les théâtres d'opérations

- en intra / inter théâtres.

1.2. Fonctionnement et direction du réseau

Le chef d'état-major des Armées assure le commandement du réseau.

Par délégation, la division " Emploi " (EMA/EMPL /6) de l'EMA pilote le système SYRACUSE **(qui inclut le réseau ARISTOTE)** et en définit les règles d'emploi.

Relevant du CEMA, la DIRISI assure la direction du réseau, la supervision, l'exploitation, le soutien du réseau ARISTOTE.

La gestion du réseau ARISTOTE est organisée autour d'un Centre de Gestion Nominal (CGN), implanté à Maisons Laffitte, constitué des entités suivantes :

- CCR-N : Centre de Commandement du Réseau Nominal,

- CGR-N : Centre de Gestion du Réseau Nominal,

- Serveur de messagerie MS-Exchange,

redondé par un Centre de Gestion Secours (CGN-S) de structure physique identique et situé sur le site de la station métropolitaine de Favières, secondé selon besoin par un Centre de Gestion de Théâtre (CGR-T).

2 - DESCRIPTION DU SERVICE OFFERT

2.1. Périmètre du service

Le périmètre du service est interarmées.

Le système permet le « bout en bout » entre les abonnés de théâtre et les abonnés métropolitains, en utilisant les supports de communications longue distance disponibles (liens satellites civils et militaires, longues lignes internationales (LLI), fibres optiques et chaînes hertziennes).

En assurant l'interconnexion avec tous les réseaux civils et militaires existants, il permet aux abonnés de ces différents réseaux de communiquer, sans restriction technique. Cependant, des mesures de cloisonnement, relevant de l'application des directives SSIC nationales et/ou de l'OTAN, seront systématiquement appliquées.

Ce réseau assure l'extension des réseaux informatiques locaux en profitant des technologies disponibles s'appuyant sur le protocole Internet (IP).

2.2. Caractéristiques du service

Le rôle d'ARISTOTE comprend en quatre fonctions :

- ➲ la mise en œuvre des communications entre les usagers du système (métropole et théâtres) ;
- ➲ le traitement des communications commutées et routées (établissement, maintien, libération) de manière automatique ;

- ➲ la réalisation de l'ensemble des bouts en bouts fonctionnels identifiés entre le théâtre et la métropole en utilisant des ressources de transmissions satellites disponibles dans les Armées (SYRACUSE, VSAT, INMARSAT) ;
- ➲ l'optimisation de l'utilisation de la ressource de transmission allouée aux liaisons entre les noeuds ARISTOTE :
  - compression des communications phonie claire, chiffrée et FAX,
  - gestion de la congestion du lien satellite (priorité et préemption),
  - annulation d'écho compatible des délais de transmission de supports satellite.

CHAPITRE 3 - SERVICES SATELLITAIRES NON MILITAIRES

L'utilisation de services satellitaires non militaires au profit d'unités à déployer, peut être envisagée en cas d'impossibilité de raccordement aux infrastructures satellitaires militaires (SYRACUSE) du fait :

- de la non couverture de la zone d'intervention ;

- du besoin d'équipements spécifiques liés à la mission ne nécessitant pas la mise en place d'infrastructures lourdes et permanentes (mobilité – discrétion – souplesse d'emploi….) ;

- d'une décision de commandement.

Cette fourniture de services de télécommunications est régie par les conventions ASTEL S (Acquisition de Services de TELécommunications par Satellites commerciaux) et INMARSAT.

Pour pouvoir utiliser ces services, il est obligatoire que le demandeur ait passé un marché dans le cadre de cette convention.

Le périmètre du service est interarmées.

Les capacités de communication offertes par ces services couvrent, en fonction du type de lots, la téléphonie claire et cryptée, le positionnement GPS, la transmission données et fax (9600bps), l'envoi de SMS, la messagerie vocale...