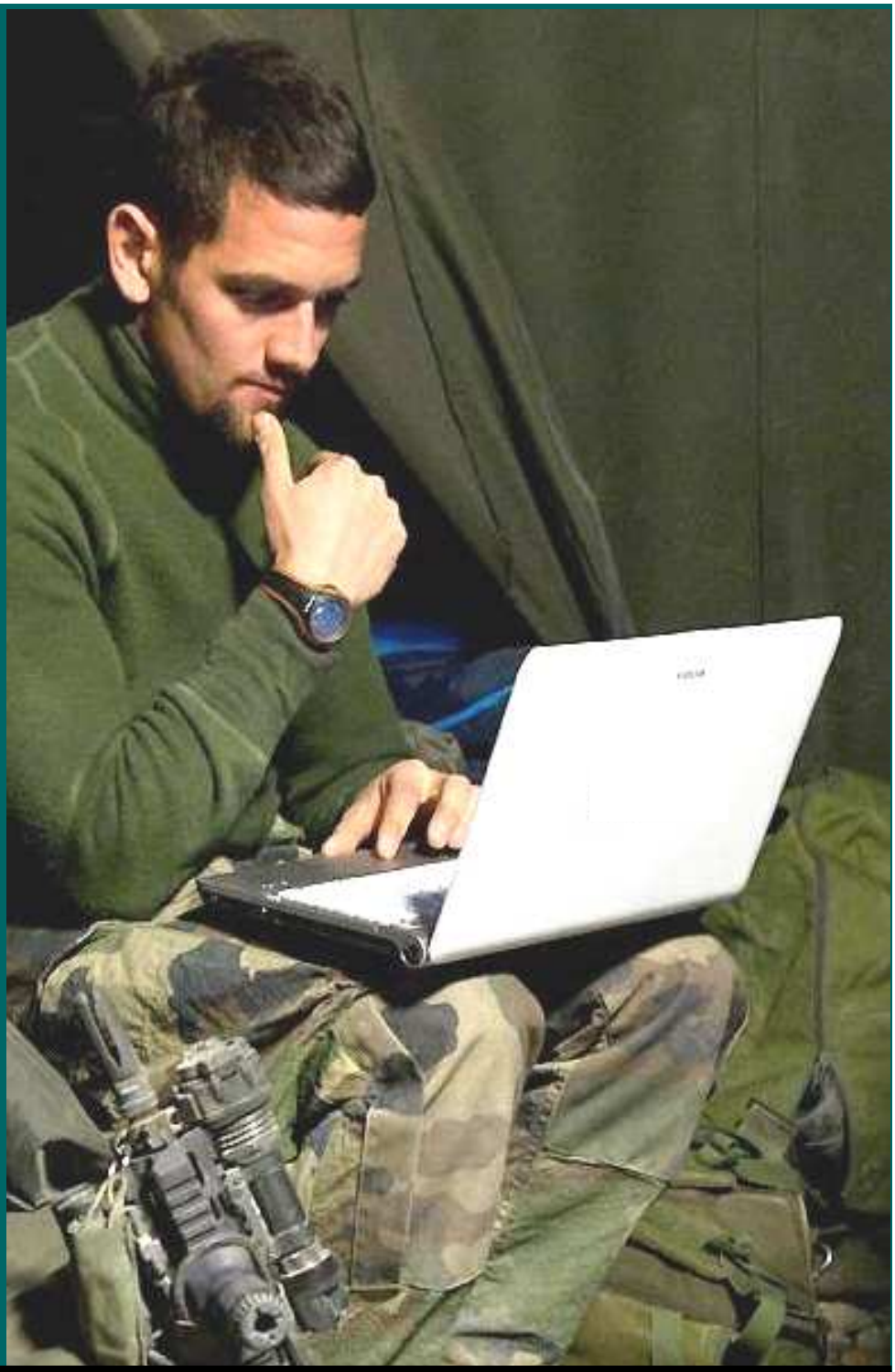
État-major
des armées

Division
soutien



Utilisation d'Internet à des fins privées dans le cadre de la condition du personnel en opération

Publication interarmées PIA-4.0.1.1_UIFP-CPO(2011)

N° D-11-009052/DEF/EMA/SC-SOUT/SLI/SDO/NP
du 18 novembre 2011

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE
ET DES
ANCIENS COMBATTANTS

Intitulée *Utilisation d'Internet à des fins privées dans le cadre de la Condition du personnel en opération,* la Publication interarmées (PIA) 4.0.1.1_UIFP-CPO(2011) respecte la charte graphique définie dans la PIA-7.2.4_RDIA(2010), n° 161/DEF/CICDE/NP en date du 18 juin 2010. Ladite charte graphique est elle-même conforme aux prescriptions de l'*Allied Admi-nistrative Publication (AAP) 47(A*[1]*)* intitulée *"Allied Joint Doctrine Development".* Elle applique également les conseils du *Lexique des règles typographiques en usage à l'Imprimerie nationale (LRTUIN, ISBN*[2] *978-2-7433-0482-9)* dont l'essentiel est disponible sur le site Internet www.imprimerienationale.fr ainsi que les prescriptions de l'Académie française. La première de couverture de ce document a été créée par le Centre interarmées de concepts, de doctrines et d'expérimentations (CICDE)[3]. Attention : la seule version de référence de ce document est la copie électronique mise en ligne sur les sites Intradef et Internet du CICDE (http://www.cicde.defense.gouv.fr) dans la rubrique *Corpus conceptuel et doctrinal interarmées !*

[1] La lettre A signifie que le document original a subi une révision complète depuis sa première promulgation.
[2] *International Standard Book Number* / Numéro international normalisé du livre.
[3] Photo ministère de la Défense (MINDEF).

PIA-4.0.1.1_UIFP-CPO(2011)

UTILISATION D'INTERNET À DES FINS PRIVÉES DANS LE CADRE DE LA CONDITION DU PERSONNEL EN OPÉRATION (UIFP-CPO)

N° D-11-009052/DEF/EMA/SC-SOUT/SLI/SDO/NP
du 18 novembre 2011

(PAGE VIERGE)

Lettre de promulgation

Le général de corps aérien Éric ROUZAUD
Sous-chef d'état-major Soutien
(SCEM/SOUT)

Paris, le 18 novembre 2011
N° D-11-009052/DEF/EMA/SC-SOUT/SLI/SDO/NP

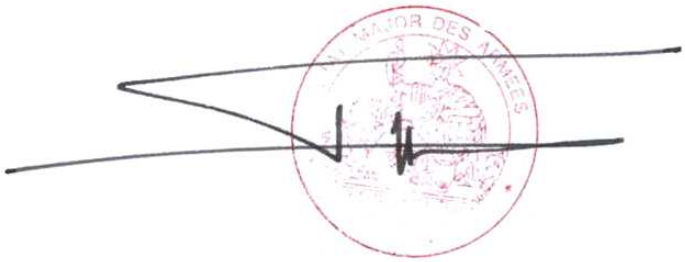
1. Intitulée *Utilisation d'Internet à des fins privées dans le cadre de la Condition du personnel en opération*, la Publication interarmées (PIA) 4.0.1.1_UIFP-CPO(2011) a pour but de définir précisément le cadre de mise en œuvre de l'internet de loisir en opération et d'en énoncer les principes d'emploi et les spécificités.

2. Il est nécessaire que toute autorité responsable du soutien logistique d'un théâtre ainsi que le personnel concerné par le domaine CPO s'imprègne de l'esprit et de la lettre de ce document et participe activement à la compréhension des objectifs recherchés par cette nouvelle définition d'emploi.

3. Ainsi, le rôle du commandement opérationnel est renforcé quant à la garantie du respect et de la compréhension des règles d'utilisation par le personnel projeté.

4. Cette publication constitue l'application des instructions et textes de références ainsi que les mesures de sécurité techniques et organisationnelles susceptibles de minimiser les risques.

5. Son objectif premier est d'officialiser ce que l'EMA a décidé, pour que le personnel sur les théâtres en connaisse les raisons.



(PAGE VIERGE)

Récapitulatif des amendements

1. Ce tableau constitue le recueil de tous les amendements proposés par les lecteurs, quels que soient leur origine et leur rang, transmis à la division SOUTien de l'État-major des armées (EMA) en s'inspirant du tableau proposé en annexe B (voir page 33).

2. Les amendements validés par la division SOUTien de l'EMA sont inscrits **en rouge** dans le tableau ci-dessous dans leur ordre chronologique de prise en compte.

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

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

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

N°	Amendement	Origine	Date de validité
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			

(PAGE VIERGE)

Références

a. Voir annexe A, page 31.

Préface

1. L'État-major des armées (EMA) attache une importance significative à la Condition du personnel en opération (CPO), dont l'un des objectifs clés est notamment la préservation du moral du combattant. À ce titre, le déploiement de l'internet[4] de loisir fait désormais partie intégrante des prestations CPO offertes aux troupes déployées sur un théâtre d'opérations.

2. Les enseignements récents ont fait clairement apparaître la nécessité d'actualiser le cadre de mise en œuvre de cette prestation en opération. Notamment avec les évolutions technologiques et son utilisation devenue partie intégrante du quotidien de chacun pour communiquer et s'informer, la mise à disposition d'un internet de loisir ne pouvait rester inchangée au regard de l'évolution comportementale et technologique de notre société.

3. Cependant, la protection des militaires et de leurs familles et la sécurité opérationnelle doivent être en permanence assurées au titre de la primauté de la mission, qui est le principe premier de la politique de CPO.

4. Dès lors, la nécessité d'assurer un soutien de l'homme de qualité comme l'impératif de garantir la confidentialité des informations relatives à la mission militent pour la stricte application d'une directive relative à l'utilisation d'un internet de loisir dans le cadre de la CPO.

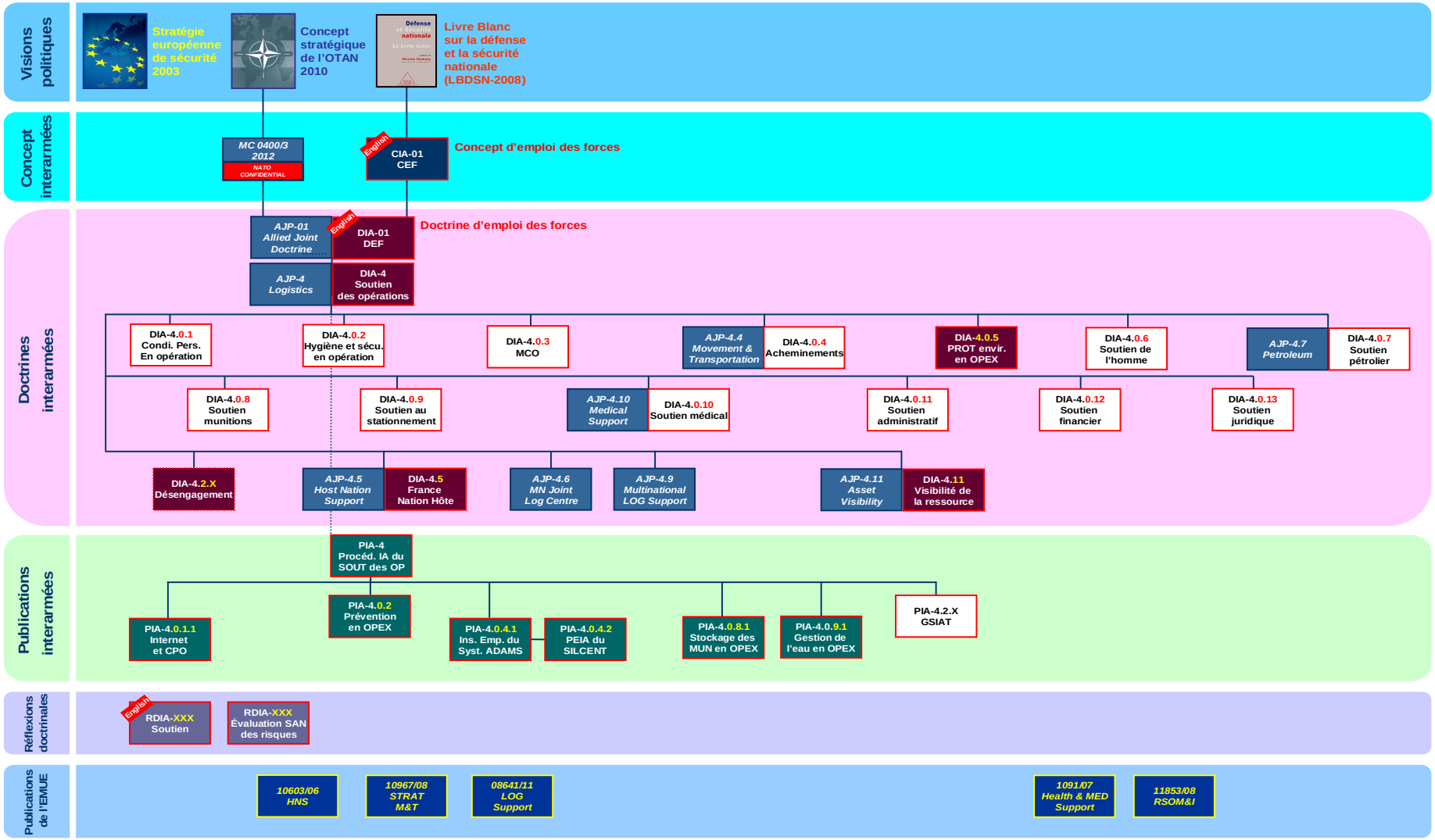
5. Cette PIA replace l'Internet de loisir dans la perspective de l'engagement de nos forces armées. Elle permet de définir l'utilisation de l'Internet de loisir en opération ainsi que le niveau de prestation acceptable au regard des objectifs de l'EMA en matière de CPO.

6. Elle décrit les modalités de mise en œuvre de la prestation, et tout particulièrement les responsabilités de l'utilisateur et du commandement.

[4] Le terme d'origine américaine ***"Internet"*** a été dérivé du concept d'*internetting* (en français : *« interconnecter des réseaux »*) dont la première utilisation documentée remonte à octobre 1972 par Robert E. Kahn au cours de la première *International Conference on Computer Communications* (ICCC) à Washington. Les origines exactes du terme *Internet* restent à déterminer. Toutefois, c'est le 1er janvier 1983 que le nom *"Internet"*, déjà en usage pour désigner l'ensemble d'*ARPANET* et plusieurs réseaux informatiques, est devenu officiel. En anglais, on utilise un article défini et une majuscule, ce qui donne *the Internet*. Cet usage vient du fait que *"Internet"* est de loin le réseau le plus étendu, le plus grand *"internet"* du monde, et donc, en tant qu'objet unique, désigné par un nom propre. Un *internet* (un nom commun avec *« i »* minuscule) est un terme d'origine anglaise utilisé pour désigner un réseau constitué de l'interconnexion de plusieurs réseaux informatiques au moyen de routeurs. Une publication au Journal officiel de la République française indique qu'il faut utiliser le mot *« internet »* comme un nom commun, c'est-à-dire sans majuscule[2]. L'Académie française recommande de dire *« l'internet »*. Il existe une controverse sur le sujet entre les partisans des expressions *« l'Internet »*, *« Internet »* et *« l'internet »*. Les publications interarmées utilisent la deuxième et la troisième formule.

(PAGE VIERGE)

Domaine 4 *Soutien*



(PAGE VIERGE)

Sommaire

Chapitre 1
Problématique

101. Les quatre dernières années d'utilisation de l'internet de loisir sur les théâtres d'opérations, ont mis en exergue les points suivants :

a. l'émergence de risques réels au regard des exigences opérationnelles :

(1) collectifs : captation d'informations opérationnelles engageant la sécurité de la force et/ou la réussite de la mission ;

(2) individuels : isolement, addiction, etc. ;

b. une forte frustration du personnel projeté quant à la prestation proposée au regard des prestations accessibles en France ou proposées par les fournisseurs locaux sur les théâtres ainsi que par certains contingents étrangers.

102. **À l'heure où Internet occupe de plus en plus de place dans notre vie quotidienne et propose de plus en plus de services, il convient de préciser que son utilisation à des fins privées dans le cadre de la Condition du personnel en opération (CPO) ne peut être semblable à ce qui peut être pratiqué chez soi en France.**

103. **Dès lors, la nécessité d'assurer un soutien de l'homme de qualité comme l'impératif de garantir la confidentialité des informations relatives à la mission militent pour la définition d'une politique concernant l'utilisation de l'internet de loisir dans le cadre de la condition du personnel en opération.**

104. **Dans ce contexte, la primauté accordée à la prise en compte des contraintes opérationnelles (confidentialité des informations liées aux opérations, protection des soldats, etc.), par rapport à la satisfaction totale des besoins exprimés par les utilisateurs de l'Internet de loisir, représente l'axe principal autour duquel s'articule la politique relative à l'utilisation de l'internet de loisir.**

(PAGE VIERGE)

Chapitre 2
Les principes

201. Les règles à mettre en œuvre pour l'utilisation de l'internet de loisir en opération découlent en droite ligne des principes de primauté de la mission, de juste suffisance, d'universalité et d'adaptation définis dans le cadre de la politique interarmées de la CPO.

Section I – Protection de nos forces

202. La réussite des opérations militaires dans un environnement opérationnel, technologique et médiatique complexe exige que le personnel militaire respecte des règles strictes d'utilisation de l'internet de loisir en opération et que le commandement soit sensibilisé aux risques encourus par l'utilisation de cette technologie. La responsabilisation des utilisateurs est une condition indispensable à la sécurité de nos forces face au risque avéré de capture d'information sensible *via « la toile ».*

203. L'usage de postes privés mobiles (ordinateur, téléphone, etc.), très largement répandu sur un théâtre d'opérations, doit être pris en compte dans le cadre de la sécurisation globale et faire l'objet de directives précises du COMSICIAT[5]. Ces matériels constituent un vecteur de fuites d'informations, avec des connexions à l'Internet parfois non maîtrisées. L'interdiction de l'usage de tels matériels peut être décidée par le commandement au regard du niveau d'insécurité informatique et des risques opérationnels engendrés[6].

Points d'application

204. Le personnel et le commandement doivent être particulièrement sensibilisés aux risques et responsabilités qui s'appliquent à la protection et la sécurité de l'information ainsi qu'à la lutte contre la délinquance.

Protection et sécurisation de l'information

205. Utilisés sans règles d'emploi sur un théâtre d'opérations, l'Internet de loisir comme le téléphone peuvent devenir une arme tournée contre nos forces[7]. L'utilisation de moyens autres que ceux mis en place par la chaîne de commandement (fournisseurs locaux d'accès à Internet, etc.) ou le non-respect des règles édictées par celle-ci accentuent la vulnérabilité des détachements projetés dans un contexte où les acteurs locaux (mouvances armées, acteurs étatiques et privés) sont techniquement capables d'intercepter les informations échangées si le dispositif technique mis en place n'est pas assez protégé.

206. Des événements récents sur les théâtres ont confirmé l'exploitation de cette vulnérabilité. **À ce titre, toute information (photos ou écrits) relative à des dispositifs de la force, à des départs en mission, à des identités, etc. doit être formellement proscrite dans le cadre de l'utilisation de l'internet de loisir en opération.**

207. Dans ce cadre, l'objectif premier du principe de sécurisation relatif à l'utilisation de l'internet de loisir en opération consiste à assurer la protection des échanges privés des militaires français en OPEX[8] face aux capacités d'écoute du camp adverse. Plus concrètement, il s'agit de faire face au risque de diffusion volontaire ou involontaire d'informations considérées comme sensibles sur des sites d'échanges et dans des courriers électroniques.

---

[5] COMmandant des Systèmes d'Information et de Communication InterArmées de Théâtre.

[6] Article L4121-2 du code de la défense : *« Indépendamment des dispositions du Code pénal relatives à la violation du secret de la défense nationale et du secret professionnel, les militaires doivent faire preuve de discrétion pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions. En dehors des cas expressément prévus par la loi, les militaires ne peuvent être déliés de cette obligation que par décision expresse de l'autorité dont ils dépendent. L'usage de moyens de communication et d'information, quels qu'ils soient, peut être restreint ou interdit pour assurer la protection des militaires en opération, l'exécution de leur mission ou la sécurité des activités militaires. »*

[7] Cf. *MC 045.*

[8] OPération EXtérieure.

Lutte contre la délinquance

208. L'utilisation d'Internet est un vecteur nouveau et croissant :

a. d'infractions non spécifiques à ce *média* ;

b. d'infractions relevant du cadre spécifique de la délinquance électronique[9].

209. La délinquance informatique correspond à une conduite proscrite par la législation et/ou la jurisprudence et qui nécessite l'utilisation des technologies numériques dans la commission du délit. Les types de délits liés à l'informatique sont nombreux : attaque des serveurs et des sites *Web*, diffusion de virus informatiques, propagande haineuse, etc.

210. Dès lors, la lutte contre la délinquance informatique dans le cadre de l'utilisation de l'internet de loisir en opération s'appuiera sur une information du commandement et des utilisateurs sur les menaces et les vulnérabilités liées à la criminalité informatique ainsi que sur la mise en œuvre des dispositions prévues par la législation en la matière.

Rôle du commandement

211. Au niveau stratégique, le commandement a la responsabilité de définir, pour chaque opération, les modalités organisationnelles et contractuelles de l'internet de loisir au travers des prismes décrits dans les paragraphes qui suivent.

La sécurisation des systèmes

212. La mise en œuvre d'une prestation Internet de loisir en opération, quel que soit son procédé, nécessite le respect du niveau de sécurité souhaité par le commandement et défini dans le cahier des charges de l'appel d'offres. La définition du niveau de sécurité de cette prestation doit couvrir les aspects suivants : organisation, sécurité physique et informatique, sensibilisation, gestion des supports, gestion des configurations, sécurité des communications, etc.

213. Concernant la sécurité des communications, le recours à un réseau câblé plutôt que *WIFI*[10] ainsi qu'à une architecture de type *VPN*[11] est un procédé à privilégier pour diminuer le risque d'écoute passive du réseau. En outre, si le réseau de desserte Internet emprunte un cheminement non maîtrisé (comme celui des fournisseurs locaux d'accès à Internet), il est nécessaire de fédérer les accès personnels par un ou plusieurs points d'accès maîtrisés qui utiliseront chacun un *VPN* jusqu'en France où les échanges seront ainsi mêlés au flux banalisé des échanges sur le territoire national[12].

La maîtrise de l'information

214. Cet axe implique le respect des règles élémentaires suivantes :

a. n'avoir qu'un seul fournisseur d'accès par site ;

b. *« connaître »* le fournisseur d'accès à l'Internet du site et ses sous-traitants éventuels ;

c. limiter l'écoute passive : bannir le *WIFI* non sécurisé ;

d. maîtriser l'accès aux infrastructures réseau par :

(1) le contrôle de l'accès physique aux éléments actifs du réseau afin d'éviter le piégeage ou le détournement de trafic,

---

9 Définies notamment par la loi HADOPI.

10 Le terme *"Wi-Fi"* suggère la contraction de *Wireless Fidelity*, par analogie au terme *Hi-Fi* (utilisé depuis 1950) pour *High Fidelity* (apparu dans les années 30).

11 Tout ce qui circule sur Internet est par défaut en clair et réputé compromis. Le recours à l'architecture de type *VPN* (*Virtual Private Network* : protocole de tunnelisation) permet aux données passant d'une extrémité à l'autre du *VPN* d'être sécurisées par des algorithmes et de la cryptographie. Le terme *« tunnel »* symbolise le fait qu'entre l'entrée et la sortie du *VPN* les données sont chiffrées et donc normalement incompréhensibles pour toute personne située entre les deux extrémités du *VPN*.

12 Ceci peut faire l'objet d'une réalisation par un prestataire de services, incluant la construction d'un réseau sécurisé interne au site et la mise en œuvre des *VPN* entre le site et la France.

(2) l'identification et l'authentification des intervenants susceptibles de modifier la configuration des éléments actifs, dans le respect des contraintes traditionnelles de dureté et de temps pour les mots de passe dévolus à ce type d'intervention,

(3) la sécurisation du protocole d'administration à distance des éléments actifs.

215. Ainsi, la conception de l'architecture technique visant à fournir le service Internet de loisir découle d'une analyse des risques, spécifique à chaque environnement.

Responsabilisation des utilisateurs

216. Acteur indépendant dans son usage à titre privé de l'internet de loisir en opération, le personnel exerce librement son droit d'expression et d'opinion. Toutefois, il reste lié par **son devoir de réserve et de discrétion professionnelle.** À ce titre, sous peine de sanctions disciplinaires et pénales, les informations échangées ne doivent en aucun cas porter atteinte aux intérêts de la défense ou à la conduite des opérations[13].

217. Par ailleurs, il convient de noter que la restriction dans l'usage de cette prestation contribue à la protection de l'environnement familial des utilisateurs. Enfin, les prestations et les équipements Internet ne doivent pas constituer le support d'une infraction aux lois françaises ou du pays hôte, lorsque celles-ci sont applicables. Par conséquent, chaque utilisateur doit :

a. avant projection, prendre connaissance de la charte de l'utilisateur[14] de l'internet de loisir en opération et signer celle-ci (cf. paragraphe 2.3) ; seule la signature de ce document lui donnera la possibilité d'accéder aux prestations relatives à ce média ;

b. pendant la mission :

(1) appliquer strictement les règles définies dans la charte de l'utilisateur et par les directives spécifiques définies par le théâtre sur lequel il est projeté,

(2) ne pas commettre d'infraction par le biais d'Internet (le contenu des sites consultés doit être conforme à la loi et aux mesures spécifiques données par le théâtre). En cas de constat d'utilisation non conforme, le commandement prend toutes les mesures appropriées de nature à interdire temporairement ou définitivement l'accès au service proposé, voire à sanctionner le ou les contrevenants.

Section II – Juste besoin

218. La satisfaction des besoins relatifs à l'utilisation de l'internet de loisir dans la cadre de la CPO correspond, pour chaque théâtre d'opération, à un choix stratégique du commandement et ne doit en aucun cas perturber l'exécution de la mission.

219. À ce titre, le principe de la satisfaction du juste besoin prime sur celui de la satisfaction de tous les besoins. Ce principe vise à garantir à chaque militaire, en fonction du théâtre d'opérations concerné et sous certaines conditions, un lien avec la famille et un accès à l'information, via l'Internet de loisir.

220. Dans ce cadre, deux postulats s'imposent dans la mise en œuvre de cette prestation :

a. la séparation des réseaux Internet opérationnel et de loisir afin d'éviter toute confusion d'emploi, pouvant entraîner de graves conséquences en termes de sécurité des troupes déployées ;

b. la priorité donnée au déploiement à l'internet collectif (cybercafé).

---

[13] Les conditions d'emploi des informations soumises au secret de la défense nationale sur le réseau Internet déclinent de l'instruction ministérielle n° 8192 et leur non-respect fait l'objet d'articles du Code pénal (Article 413-9 à 413-12).

[14] Sur le théâtre d'opération, cette charte sera affichée dans tous les cybercafés et sera également consultable sur les pages d'accueil des ordinateurs du réseau mis à disposition.

Section III – Transparence

221. Le ***« devoir de savoir »*** impose de délivrer au militaire en passe d'être projeté une information relative à la prestation de l'internet de loisir offerte sur le théâtre (modalités, coûts, etc.) ainsi que les règles à respecter par l'utilisateur (confidentialité, risques encourus, etc.[15]) et les contrôles qui en découlent.

222. Sous la responsabilité de la chaîne de commandement organisatrice de la Mise en condition avant projection (MCP), cette information est délivrée à cette occasion. La présence à cette séance d'information d'un intervenant de la DPSD[16], voire du prestataire de service est fortement recommandée.

223. À mi-mandat, une information ciblée auprès du personnel déployé sera réalisée dans le but de rappeler les informations à ne pas diffuser sur *« la toile »* (lieu et date de mission, photos du dispositif militaire et de personnel, etc.) et les risques encourus en cas de non-respect des règles édictées. Cette information est à la charge du commandement de théâtre.

Section IV – Adaptation

224. Les opérations en cours montrent que, techniquement et financièrement, la mise en œuvre de l'utilisation de l'internet de loisir en opération ne peut pas être identique sur toute la zone d'opérations.

225. Le principe d'adaptation de cette mise en œuvre aux conditions d'engagements et à l'infrastructure existante est un compromis nécessaire guidé par la prise en compte des critères de choix que sont le financement, les exigences de protection, les contraintes opérationnelles, la durée du mandat et l'effectif projeté. Ces contraintes limitent *de facto* le principe d'universalité, défini dans la lettre de référence a), au personnel stationné sur un même site ou soumis au même environnement et pour lequel les conditions de la prestation doivent être identiques.

226. Ce principe d'adaptation se traduit plus particulièrement par :

a. une mise en place graduelle de cette prestation selon la phase de l'opération (déploiement initial, coercition, stabilisation, reconstruction, désengagement) ;

b. des modalités différenciées de mise en œuvre :

(1) selon la situation tactique :

(a) mise à disposition de matériels SIC[17] opérationnels permettant aux troupes déployées d'entretenir un lien avec la famille (cas d'une entrée en premier par exemple). Cette utilisation se limite à l'envoi de courriers électroniques sans pièce jointe et dans le cadre de règles d'emploi spécifiques définies par le CPCO,

(b) externalisation de la prestation de l'Internet de loisir sur les sites stabilisés, conformément au cadre du marché d'externalisation ;

(2) selon les infrastructures de la nation hôte et l'environnement technologique du site.

Section V – Financement partagé

227. Conscient de la forte attente du personnel déployé en opération, l'EMA a décidé de définir une prestation standard gratuite, à laquelle peut être associée une offre supplémentaire à financer par l'utilisateur :

---

15 Directive n°13/DEF/DGSIC, édition n°1 du 30 juin 2010.
16 Direction de la Protection et de la Sécurité de la Défense.
17 Système d'Information et de Commandement.

a. la prestation mise à disposition gratuitement par les armées répond au juste besoin de lien avec la famille et d'accès à l'information ; ce juste besoin a été évalué par les armées au travers du prisme de l'impératif de maintien de la capacité opérationnelle du combattant et des possibilités de financement sur le BOP[18] OPEX ;

b. lorsque l'environnement tactique le permet, une prestation supplémentaire est mise à disposition du personnel qui peut y recourir, à ses frais, selon une grille de tarification négociée par les armées :

(1) ce type de prestation sera assuré par un prestataire sélectionné par le commandement, en fonction des impératifs de sécurisation décrits *supra* ;

(2) cette prestation n'est pas obligatoirement équivalente aux prestations disponibles en France pour un prix équivalent, mais contribue à répondre aux besoins strictement privés de l'utilisateur dans les limites acceptables en termes de prise en compte des contraintes opérationnelles.

[18] Budget Opérationnel de Programme.

(PAGE VIERGE)

Chapitre 3
Les acteurs

301. La mise en œuvre de l'internet de loisir pour un théâtre d'opérations est une responsabilité de la chaîne de commandement sous l'autorité de l'état-major des armées.

302. La définition du besoin propre à cette prestation s'appuie sur les principes définis supra ainsi que sur des décisions de commandement, propres à chaque théâtre, prises sur la base d'un référentiel normatif (cf. partie n° 4) et tenant compte des contraintes opérationnelles de ce théâtre.

Section I – La division Soutien logistique interarmées (SLI) de l'EMA

303. Au titre de ses attributions, la division SLI de l'EMA définit, rédige et actualise, en liaison avec les états-majors, directions et services, la politique interarmées relative à l'utilisation d'Internet à des fins privées dans le cadre de la CPO.

Section II – Le Centre de planification et de conduite des opérations (CPCO) de l'EMA

304. Le CPCO est le responsable de la maîtrise d'ouvrage stratégique pour le soutien relatif à la CPO. À ce titre, il définit dans le paragraphe *« CPO »* de la Directive administrative et logistique (DAL), propre à chaque opération, les modalités générales de mise en œuvre des prestations de l'Internet de loisir et de la téléphonie CPO.

Section III – Le Centre interarmées de la coordination de la logistique des opérations (CICLO)

305. Le CPCO délègue au CICLO la conduite et le contrôle de la politique CPO sur les théâtres d'opérations. Dans le cadre de l'utilisation de l'Internet de loisir, le CICLO a la responsabilité de :

a. coordonner la rédaction du cahier des charges pour le marché d'externalisation des prestations de l'Internet de loisir et de la téléphonie CPO ;

b. coordonner le déploiement des solutions Internet CPO[19] ;

c. piloter l'exécution du marché, de la commande à l'analyse de la performance[20] ;

d. proposer au CPCO, pour chaque opération, le besoin financier annuel valorisé ;

e. centraliser et exploiter le retour d'expérience en liaison avec les états-majors d'armée ;

f. présenter une synthèse au CPCO ;

g. donner son avis au CPCO sur toute demande exprimée par le théâtre d'opérations et susceptible de modifier les termes de la DAL ou la répartition financière interthéâtres.

306. Au titre de ses attributions de contrôle, le CICLO peut être amené à conduire des audits et des contrôles sur les théâtres, selon une programmation établie avec le CPCO/*J4*.

---

[19] Systèmes d'Information et de Commandement Opérationnels (SIC OPS) ou prestataire.

[20] La performance du marché se mesure en particulier au travers des critères de conformité de ce marché par rapport au cahier des charges, de satisfaction du client, d'efficacité et d'efficience de la prestation réalisée.

Section IV – Le Service du commissariat des armées (SCA)

307. Conformément à sa mission et plus particulièrement à ses attributions dans le domaine de la passation des contrats d'externalisations au profit des opérations, le service du commissariat des armées est chargé :

a. d'élaborer la stratégie d'acquisition des prestations relatives à l'internet de loisir en opération et à la téléphonie CPO ainsi que les procédés d'évaluation, de sanction et de pilotage du marché associé, en liaison avec le coordonnateur du projet (CICLO), la DPSD et la DIRISI[21] ;

b. de proposer à l'EMA cette stratégie d'acquisition et ses procédés de suivi du marché associé ;

c. de réaliser le marché dans des délais compatibles avec l'effet à obtenir fixé par le CPCO.

Section V – La Direction interarmées des réseaux d'infrastructure et des systèmes information (DIRISI) de la défense

308. Experte des systèmes informatiques, la DIRISI a la responsabilité de conseiller l'EMA sur les aspects techniques des solutions possibles pour la réalisation de la prestation relative à l'Internet de loisir en opération. À cet effet, la DIRISI participe à la rédaction du Cahier des clauses techniques particulières (CCTP) définissant le besoin des armées en vue de la contractualisation de cette prestation.

Section VI – La Direction de la protection et de la sécurité de la défense (DPSD)

309. Dans le cadre de sa mission d'aide au commandement, la DPSD émet un avis sur le volet *« protection des informations échangées »* du CCTP relatif au marché d'externalisation des prestations de l'internet de loisir et de la téléphonie CPO. Dans le cadre de la réalisation d'un marché sensible, la DPSD émet un avis sur les entreprises candidates.

310. En cas d'anomalie constatée, la DPSD préconise au commandement les mesures palliatives à mener afin d'améliorer le dispositif de protection.

Section VII – La chaîne de commandement sur le théâtre d'opérations

311. Composante intégrale du soutien logistique des opérations, la conduite de la CPO sur un théâtre d'opérations relève de la responsabilité du commandant du contingent national (*NCC*[22]/COMANFOR[23]).

312. À ce titre, il dispose au sein de son état-major de l'ASIA[24] et du COMSICIAT[25] pour mettre en application les prescriptions et les principes énoncés dans le cadre de la politique relative à l'utilisation d'Internet à des fins privées et diffuser les directives de théâtre correspondantes.

Rôle de l'ASIA

313. Quel que soit le cadre de l'opération, l'ASIA est l'unique interlocuteur habilité auprès du CICLO et du CPCO en matière de soutien relatif à l'Internet de loisir et à la téléphonie CPO.

314. Par délégation du *NCC*/COMANFOR, il coordonne l'action du COMSICIAT et de la DPSD au titre de la mise en œuvre des prestations dont il rend compte au CPCO, notamment dans le cadre du compte rendu hebdomadaire logistique.

---

21 Direction Interarmées des Réseaux s'Infrastructure est des Systèmes d'Information.
22 *National Contingent Commander.*
23 COMmANdant de la FORce.
24 Adjoint Soutien InterArmées. Dans le cadre d'une opération nationale de faible envergure, l'ASIA et le sous-chef d'état-major soutien peuvent être la même personne.
25 COMmandant des Systèmes d'Information et de Communication InterArmées de Théâtre.

Rôle du COMSICIAT

315. Tant que la prestation relative à l'Internet de loisir en opération ne peut être externalisée, le COMSICIAT peut mettre à la disposition du contingent français, sur décision de CPCO, une prestation d'Internet de loisir ou de téléphonie dégradée, *via* l'utilisation de moyens opérationnels étatiques (cf. chapitre 5, section II et chapitre 5, section III).

316. Par ailleurs, le COMSICIAT assiste techniquement l'ASIA pour l'évaluation de la performance de la prestation externalisée mise en œuvre. Il veille également au respect des règles de sécurité relatives à la cohabitation des réseaux Internet opérationnel et de loisir.

Rôle de la chaîne de commandement déployée sur le théâtre d'opérations

317. À partir des directives de théâtre relatives à l'utilisation de l'Internet de loisir en opération, chaque niveau de commandement déployé sur le théâtre d'opérations a la responsabilité de :

a. s'assurer de la connaissance par le personnel des règles d'utilisation de cette prestation de loisir[26] ;

b. mettre en place des contrôles aléatoires de manière à dissuader toute tentative de non-respect des directives de sécurité et d'utilisation ;

c. rappeler les peines disciplinaire et pénale encourues par un utilisateur pris en flagrant délit de non-respect de la charte de l'utilisateur ou des directives spécifiques ;

d. être capable d'identifier le personnel[27] ayant commis des actes condamnables (téléchargement illégal, consultation de sites illicites, diffamation, injures, etc.) ;

e. protéger l'utilisateur des menaces auquel il peut être confronté en garantissant notamment la confidentialité des échanges ;

f. veiller au renforcement si nécessaire des mesures de protection des flux d'information sortant du théâtre ;

g. veiller au respect des règles particulières d'installation et de coexistence des réseaux Internet opérationnel et de loisir sur les sites afin d'éviter toute confusion d'emploi ;

h. limiter ou arrêter le service relatif à l'Internet de loisir lorsque le contexte opérationnel l'exige ;

i. s'assurer que l'utilisation de l'Internet de loisir ne conduise pas à des situations d'addiction ou d'isolement au détriment de la cohésion du groupe.

[26] L'utilisateur représente la vulnérabilité majeure du système.

[27] Les conditions réglementaires et légales exigent la mise en place au sein de la prestation d'un procédé de contrôle personnalisé. Ce procédé vise à mettre à disposition du commandement de théâtre les outils nécessaires à la collecte des preuves permettant d'identifier les usages abusifs et/ou illégaux afin d'engager a posteriori la responsabilité personnelle de l'utilisateur en faute et de dégager la responsabilité des armées.

(PAGE VIERGE)

401. La mise en œuvre de l'internet de loisir répond à un besoin grandissant des militaires déployés sur un théâtre d'opérations. À ce titre, elle fait intégralement partie des objectifs relatifs à la politique de condition du personnel en opération. Pour autant, la mise en place d'une telle offre nécessite certaines garanties et ne peut être exigée dès l'arrivée initiale.

402. D'une manière générale, le dispositif relatif à la mise en place de cette prestation s'effectuera en deux étapes :

a. le dispositif initial ;

b. le dispositif établi.

Section I – Dispositif initial

Thèmes	*Services*	*Niveau de service*	*Coût*	*Observations*	*Délai de mise en place*
- lien famille.	Matériels opérationnels.	Envoi de courrier électronique sans pièces jointes, uniquement.	/	Dispositions particulières régies par le COMSICIAT, après décision du CPCO.	Selon décision CPCO.
- lien famille ; - accès à l'information.	**P1 :** cybercafé 1 poste/50 pax. **P2 :** accès à partir des chambres.	**P1 :** envoi et réception du courrier électronique sans pièces jointes. **P2 :** consultation de sites.	Gratuit pour l'utilisateur.	Exploitation en régie.	15 jours.

Section II − Dispositif établi

Thèmes	*Services*	*Niveau de service*	*Coût*	*Observations*	*Délai de mise en place à partir du moment où la situation le permet*
Prestation standard : - lien famille ; - accès à l'information.	1 poste/50 pax en usage collectif (cybercafé) si connexion en chambre **ou** 1 poste/25 pax si uniquement utilisation en salle cybercafé.	**Temps illimité :** a) Envoi – réception de courrier électronique avec pièce jointe limitée en taille (calibrage à définir) ; b) Consultation de sites. **45 minutes minimum/semaine :** a) Une visioconférence par semaine et par personne en salle cybercafé ou en chambre de vie ; b) 1/3 des postes du cybercafé disponibles à cet effet (configuration adaptée à l'isolement).	Gratuit.	Exploitation en régie. Les sites isolés font l'objet d'un traitement aménagé. Il incombe au commandement local de réguler l'accès aux postes visio du cybercafé en fonction des contraintes opérationnelles des unités. Pour chaque site équipé, il y a au minimum 3 ordinateurs.	Moins de 30 jours pour un site.
Prestation associée.	Internet en accès en cybercafé ou en chambre. En collectif : 1 poste/100 pax.	**Temps et capacité de téléchargement limité.**	Service payant.	Abonnement unique offrant une capacité nettement supérieure à celle de la prestation standard. Proposé par le prestataire privé.	Moins de 30 jours.

Remarque : Ce dispositif fait l'objet par le prestataire choisi d'une gestion de la bande passante et des flux échangés selon des créneaux horaires adaptés et définis avec le commandement. Cette pratique a pour but de rendre plus homogène la performance des services mis à la disposition de chaque utilisateur.

Chapitre 5
Les situations particulières

Section I – Marine : personnel embarqué

501. Compte tenu de son cadre d'emploi, le personnel militaire embarqué est considéré comme du personnel déployé sur un théâtre d'opérations. À ce titre, le commandement met à la disposition du personnel embarqué, pour son usage privé, des outils de communication à usage opérationnel. L'emploi de ces moyens étatiques ne doit pas interférer avec les intérêts opérationnels qui restent prioritaires par rapport à la CPO. Le personnel bénéficie également de moyens non étatiques, payants et régis par les mêmes principes d'utilisation.

Figure 1 – *L'utilisateur est pleinement responsable de la gestion de ses accès*

502. Les prescriptions de la politique relative à l'utilisation de l'Internet de loisir en opération s'appliquent également au personnel embarqué moyennant les adaptations nécessaires liées aux contraintes opérationnelles et techniques[28].

Section II – Déploiement initial

503. Lors d'une opération d'Entrée en premier (EEP) réalisée dans un contexte non permissif, le déploiement initial ne permet généralement pas de mettre en œuvre rapidement une prestation d'Internet de loisir conforme au référentiel normatif décrit au chapitre précédent.

504. Dans ce cas, le commandement a la possibilité de mettre en place, *via* l'utilisation de moyens opérationnels étatiques, une prestation d'Internet de loisir ou de téléphonie dégradée permettant un lien avec la famille. Ce dispositif doit être régi par des règles précises visant à ne pas entraver la réalisation de la mission. La décision d'une telle mesure est de la responsabilité du CPCO.

Section III – Sites isolés

505. L'environnement géographique ou tactique de certains sites isolés ne permet pas techniquement et financièrement de déployer une connexion d'Internet de loisir pour le personnel déployé.

[28] Politique d'emploi de l'internet dans la marine, directive N°106 DEF/EMM/MG/AG/NP le 27 janvier 2005 .

506. Dans ces circonstances, le commandement doit veiller à mettre en place, via l'utilisation de moyens opérationnels étatiques, une prestation d'Internet de loisir ou de téléphonie dégradée permettant un lien avec la famille. Le commandement de théâtre étudiera également la possibilité de compenser cette *« prestation a minima »* par une autre prestation CPO à proposer au CICLO.

Section IV – Camp multinational

Présence d'un détachement français de faible importance

507. Un détachement français de faible importance installé sur un camp multinational peut profiter des accès à l'internet de loisir disponibles au sein de ce camp à la condition expresse de respecter les principes énoncés au chapitre 2, tout particulièrement ceux relatifs au devoir de réserve et aux règles élémentaires de protection de l'information. Le chef de ce détachement effectuera à cette occasion les rappels nécessaires en la matière.

508. Il convient de considérer toutefois que les modalités de l'utilisation d'une telle prestation dépendent de l'existence d'un éventuel arrangement technique et du coût homme/jour attribué au titre de la prise en charge CPO (Internet / téléphonie) pour le personnel déployé sur les sites français aux conditions géographiques et tactiques similaires.

Présence de plusieurs détachements importants de nationalités différentes

509. Dans le cas où plusieurs détachements importants de nationalité différente cohabitent, les militaires français sont autorisés à utiliser de façon onéreuse les offres des autres nations. Le commandant du contingent national français (*NCC*) peut être amené à interdire l'utilisation d'une prestation d'un contingent étranger par le contingent français dans le cas où les mesures de sécurisation et le respect des lois françaises ne seraient pas garantis et seraient susceptibles de compromettre la sécurité de nos troupes.

510. La prestation de service relative à l'internet de loisir réalisée au profit des forces françaises pourra être proposée aux détachements étrangers, à la condition expresse que cet élargissement du périmètre de la prestation ne dégrade pas la qualité du service mis en œuvre au profit du contingent français et demeure compatible avec les restrictions d'accès (éventuelles) aux zones françaises. La décision d'une telle mesure est de la responsabilité du CPCO.

Annexe A
Références

Textes officiels interministèriels

a. Code pénal.

b. Code des postes et des communications.

c. Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

d. Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (HADOPI[29]).

e. Loi n° 2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet (HADOPI 2).

f. Loi n° 2 011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI[30] 2).

g. Décision du Conseil constitutionnel n° 2001-625 du 10 mars 2011 relative à la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2).

h. Décret n° 21005-796 du 15 juillet 2005 relatif à la discipline générale militaire, article 19 relatif à la protection du secret.

i. Arrêté du 23 juillet 2010 portant approbation de l'instruction générale interministérielle sur la protection du secret de la défense nationale.

Textes officiels internes au ministère de la Défense

j. Directive n° 13/DGSIC [31], édition n° 1 du 30 juin 2010, relative à la directive sur la sécurité des accès aux services de l'internet et la sécurité de l'hébergement des services Internet du ministère.

k. Lettre n° 106 DEF/EMM/MG/AG/NP du 27 janvier 2005 relative à la politique d'emploi de l'Internet dans la marine.

l. Lettre n° 284/DEF/EMA/SC-ORG/NP du 7 novembre 2008 relative à la politique de la condition du personnel en opération.

m. Lettre n° 973 DEF/EMA/CPCO/CDTIDR du 15 décembre 200 8 relative à la directive sur l'emploi des moyens de communication à usage privé en opération.

n. Lettre n° 0540/DEF/EMAT/ES du 19 décembre 2008 relative à l'utilisation des moyens de communication sur les théâtres d'opérations.

o. Passeport de conseils aux voyageurs de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) de janvier 2010.

p. Note n° D-11-003442/DEF/EMA/CPI/NP du 20 avril 2011 relative à l'inadéquation pour les armées de la politique SSI nationale actuelle.

q. Rapport technique n° 2011/116576/DGA MI/SSI/IPS/AI/17S8 70162/NC du 16 avril 2011 relatif aux recommandations pour la mise en œuvre du réseau *Wifi* V0.1.

---

29 Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet
30 Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure.
31 Direction Générale des Systèmes d'Information et de Communication.

r. Instruction n° 2003/DEF/DGSIC du 20 novembre 2008 portant code de bon usage des systèmes d'information et de communication du ministère de la Défense.

Textes officiels OTAN

s. Extraits du *MC*[32] *045 (Military Committee)* relatif à la politique militaire de l'OTAN en matière d'affaires publiques :

« La généralisation de l'accès à l'Internet, y compris pour le personnel déployé dans les endroits les plus rudimentaires, donne lieu à une somme considérable d'échanges d'informations décrivant des expériences placées sur des sites Web personnels[33]*, dans des blogs, dans des courriels et sur des images fixes et vidéo téléchargées. Ces informations sont mises en ligne par des membres de la force déployée, par leurs familles et leurs connaissances, par des journalistes intégrés ou d'autres médias et par le grand public. Les informations et les images ainsi diffusées peuvent, seules ou combinées à d'autres informations, donner aux analystes ennemis une idée des opérations, de l'équipement, des capacités, des tactiques et des intentions du commandement de la force ou encore donner des informations qui mettent en péril les personnels spécialisés ou leurs familles».*

[32] *Military Committee* (OTAN).
[33] Les nouveaux outils sociaux sont d'autant plus porteurs de risque que les pages personnelles ou autres sont consultables par tous. Les limites entre sphères privée, professionnelle et publique sont encore fluctuantes.

Annexe B
Demande d'incorporation des amendements

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

État-major des armées
Division soutien
14, rue Saint Dominique
75700 PARIS SP 07

ou en téléphonant au **01 72 69 22 98** pour obtenir l'adresse électronique valide à cette époque ;

ou encore en ligne sur les sites Intradef ou Internet du CICDE à l'adresse **http://www.cicde.defense.gouv.fr**

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

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

(PAGE VIERGE)

Annexe C
Lexique

Partie I – Sigles, acronymes et abréviations

Sigles

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

Acronymes

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

Abréviations

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

Charte graphique du lexique

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

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

Liste des sigles, acronymes et abréviations utilisés dans ce document

AAP	*Allied Administrative Publication*
ANSSI	Agence Nationale de la Sécurité du Système d'Information
ASIA	Adjoint Soutien InterArmées
BOP	Budget Opérationnel de Programme
CCTP	Cahier des Clauses Techniques Particulières
cf.	*Confer*, voir, se référer à…
CICDE	Centre Interarmées de Concepts, de Doctrines et d'Expérimentations
CICLO	Centre Interarmées de la Coordination de la Logistique des Opérations
CPCO	Centre de Planification et de Conduite des Opérations
COMANFOR	COMmANdant de la FORce
COMSICIAT	COMmandant des Systèmes d'Information et de Communication InterArmées de Théâtre.
CPO	Condition du Personnel en Opération
DAL	Directive Administrative et Logistique
DÉF	DÉFense
DIRISI	Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information
DPSD	Direction de la Protection et de la Sécurité de la Défense
EEP	Entrée En Premier
EMA	État-Major des Armées
MCP	Mise en Condition du Personnel
HADOPI	Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet
PIA	Publication InterArmées
SCA	Service du Commissariat des Armées
SLI	Soutien Logistique Interarmées
ISBN	*International Standard Book Number /*

	Numéro international normalisé du livre
J	*Joint* / Interarmées
LBDSN	Livre Blanc sur la Défense et la Sécurité Nationale
LOPPSI	Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure
MC	*Military Committee* (OTAN)
n°	Numéro(s)
NCC	*National Contingent Commander*
NP	**NON PROTÉGÉ**
OPEX	Opération EXtérieure
réf.	Référence
SCA	Service du Commissariat des Armées
SD-SD	Sous-Directeur Synergie Doctrinale
SIC	Système d'Information et de Commandement
SLI	Soutien Logistique Interarmées
VPN	*Virtual Private Network* / Protocole de tunnelisation
WIFI	Le terme *"Wi-Fi"* suggère la contraction de *Wireless Fidelity*, par analogie au terme *Hi-Fi* (utilisé depuis 1950) pour *High Fidelity* (apparu dans les années 30)

Partie II – Termes et définitions

(Sans objet).

(PAGE VIERGE)

Résumé

PIA-4.1.6_UIFP-CPO(2011)

1. Le développement de l'internet de loisir dans le cadre de la Condition du personnel en opération (CPO) impose la mise en œuvre de consignes strictes d'emploi afin de limiter la divulgation d'informations susceptibles d'empêcher la réalisation de la mission.
2. Le chapitre 1 de ce document pose la problématique en insistant sur la primauté accordée à la prise en compte des contraintes opérationnelles (confidentialité des informations liées aux opérations, protection des soldats, etc.).
3. Le chapitre 2 pose quant à lui les principes de primauté de la mission, de juste suffisance, d'universalité et d'adaptation définis dans le cadre de la politique interarmées de la CPO et respectant le cadre de la lutte contre la délinquance. Ce chapitre insiste donc tout naturellement sur la responsabilité des utilisateurs et sur le partage des coûts financiers qui leur est imposé.
4. Le chapitre 3 expose le rôle et la mission des différents acteurs institutionnels dans la mise en œuvre de cette politique, en insistant tout particulièrement sur les responsabilités inaliénables de la chaîne de commandement et des cadres de contact.
5. Enfin, tandis que le chapitre 4 rappelle les normes en vigueur, le chapitre 5 traite de cas de figure particuliers comme la mise à disposition d'Internet pour le personnel embarqué, le déploiement initial, l'équipement des sites isolés et le travail sur un camp multinational. Il insiste sur le fait que l'accès à l'Internet ne constitue pas un droit et que la présente politique s'applique partout, et plus encore en cas de cohabitation avec des contingents militaires locaux, alliés ou coalisés.

Ce document est un produit réalisé par la Division Soutien de l'État-major des armées (EMA). Point de contact :

État-major des armées
Division soutien
14, rue Saint Dominique
75700 PARIS SP 07

Téléphone 01 72 69 22 98

Par principe, le CICDE ne gère aucune bibliothèque physique et ne diffuse aucun document sous forme papier. Il met à la disposition du public une bibliothèque virtuelle unique réactualisée en permanence. Les documents classifiés ne peuvent être téléchargés que sur des réseaux protégés.

La version électronique de ce document est en ligne sur le site Intradef du CICDE à l'adresse htpp://www.cicde.defense.gouv.fr à la rubrique *Corpus conceptuel et doctrinal interarmées français (CCDIA-FRA).*