Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°44 du 21 novembre 2008

PARTIE PERMANENTE
Administration Centrale

Texte n°2

INSTRUCTION N° 2001/DEF/DGSIC
relative à la mise en oeuvre de la lutte informatique défensive au sein du ministère de la défense.

Du *26 septembre 2008*

DIRECTION CENTRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

INSTRUCTION N° 2001/DEF/DGSIC relative à la mise en oeuvre de la lutte informatique défensive au sein du ministère de la défense.

Du 26 septembre 2008

NOR D E F M 0 8 5 2 5 3 1 J

Références :

Ordonnance n° 2005-1516 du 8 décembre 2005 (JO n° 286 du 9 décembre 2005, texte n° 9 ; BOC, p. 8645. ; BOEM 120-0.3.1).
Décret n° 2006-497 du 2 mai 2006 (n.i. BO ; JO n° 103 du 3 mai 2006, texte n° 9 ; JO/135/2006. ; BOEM 160.1).

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°44 du 21 novembre 2008, texte 2.

---

1. INTRODUCTION.

Les systèmes d'information en service au ministère de la défense sont par nature la cible d'actions visant leur disponibilité, intégrité et confidentialité, dont les conséquences peuvent remettre en cause les grandes fonctions stratégiques du ministère.

Ces agressions se produisent dès le temps de paix et sans préavis. D'une haute technicité, elles se déroulent essentiellement au cœur même des systèmes qu'elles prennent pour cible, ignorent toute notion de frontières et sont à même de se dérouler selon des cycles de temps extrêmement courts.

De par leur nature, les agressions informatiques dirigées contre les organismes et les systèmes d'information du ministère de la défense ne peuvent être contrées que par une organisation ayant un caractère permanent, centralisé, disposant d'une connaissance et d'une vision de l'ensemble des réseaux et étant en mesure d'assurer en temps contraint en liaison avec des acteurs identifiés au sein des organismes, les fonctions de :

- veille, pour assurer la prévention et l'anticipation des crises ainsi que la détection des activités hostiles;

- alerte, pour analyser, hiérarchiser et notifier tout évènement présentant un risque;

- réponse, pour déterminer et conduire les actions défensives correspondantes.

L'ensemble des actions découlant de ces fonctions est désigné sous le vocable lutte informatique défensive (LID).

Alors que la sécurité des systèmes d'information (SSI) a pour objet la protection des systèmes d'information en posture permanente de sécurité, la LID a pour but d'adapter le niveau de protection en cas d'incident avéré ou de découverte de nouvelles menaces par le renforcement ou la mise en place de nouvelles mesures.

2. OBJET DE L'INSTRUCTION.

Destinée à compléter le référentiel réglementaire et la politique de sécurité des systèmes d'information du ministère, cette instruction présente la posture adoptée pour répondre aux règles de la politique de sécurité

concernant le réseau d'alerte et le traitement des incidents.

Elle définit les modalités de mise en œuvre de la lutte informatique défensive au sein du ministère de la défense et décrit l'organisation mise en place à cet effet.

Elle se place également en complément des mesures et de l'organisation définies dans le cadre de l'instruction ministérielle relative à la mise en œuvre de la SSI au sein du ministère de la défense.

Les modalités d'application détaillées relèvent de directives techniques et opérationnelles complémentaires.

3. CHAMPS D'APPLICATION.

Cette instruction s'applique à tous les organismes du ministère de la défense et aux établissements ou organismes sous tutelle.

Certaines dispositions de cette instruction s'appliquent également aux entreprises publiques ou privées ayant un lien avec la défense détenant des informations ou supports protégés, en complément de l'arrêté du 18 avril 2005 relatif aux conditions de protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les contrats (1).

Tous les systèmes d'information relevant de la politique de sécurité des systèmes d'information (PSSI) du ministère sont concernés par cette instruction.

Pour les systèmes d'information traitant des informations sensibles non classifiées de défense, dont l'exploitation est externalisée, des clauses spécifiques relatives à la LID seront insérées dans les contrats d'infogérance ou d'hébergement.

Pour les systèmes d'information non protégés ayant des exigences fortes de disponibilité et d'intégrité, dont l'exploitation est externalisée, des clauses spécifiques relatives à la LID seront insérées dans les contrats d'infogérance ou d'hébergement.

Les systèmes d'information mis à disposition de la France par d'autres nations et les systèmes d'information interministériels mis à disposition du ministère de la défense par un autre ministère n'entrent que partiellement dans le champ d'application de cette instruction. Les fonctions de veille, alerte et réponse sont assurées pour ces systèmes mais les circuits décisionnels centraux sont spécifiques.

Dans tous les cas, les flux d'information et les procédures à appliquer sont les mêmes pour l'utilisateur du système d'information, les structures centrales chargées de LID effectuent l'aiguillage vers les centres décisionnels concernés.

4. FONCTION DE LA LUTTE INFORMATIQUE DÉFENSIVE.

La lutte informatique défensive permet de garantir la réactivité nécessaire pour adapter la protection des systèmes face à des vulnérabilités, menaces ou attaques inopinées.

Les grandes fonctions décrites ci-après détaillent les actions de prévention, d'anticipation des risques, de détection d'activités hostiles, de notification d'alertes, d'élaboration et de diffusion d'actions défensives qui participent à cette protection dynamique des systèmes d'information.

4.1. **Fonction veille.**

La fonction veille couvre la prévention et l'anticipation des risques ainsi que la détection des activités hostiles au travers des actions de :

- réalisation de stratégies de maîtrise de propagation, de plans de continuité et de reprise des activités ;

- diffusion d'un état de l'art des moyens de protection et des bonnes pratiques, en y intégrant le volet juridique ;

- contrôle et audit des systèmes d'information et de communication (SIC) ;

- maintien de bases de connaissances relatives aux SIC, incidents, vulnérabilités, menaces et techniques d'attaques s'appuyant en particulier sur une cartographie complète et détaillée des systèmes à protéger ;

- détection et recueil des incidents de sécurité, s'appuyant sur une capacité permanente de surveillance des systèmes ;

- recherche, collecte et exploitation d'informations relatives aux vulnérabilités et menaces affectant les SIC, s'appuyant sur une capacité de recherche de renseignement et d'échange avec les alliés ;

- maintien d'un référentiel du niveau de sécurité et de l'état des mises à jour des logiciels ;

- fourniture aux acteurs SSI des indicateurs sur l'état de sécurité des systèmes.

4.2. **Fonction alerte.**

La fonction alerte couvre l'analyse des situations présentant un risque, l'estimation de leurs impacts et la diffusion de l'alerte au travers des actions suivantes :

- estimation de la criticité des incidents, des vulnérabilités et des menaces, s'appuyant sur une hiérarchisation de la criticité des différents SIC de la défense ;

- analyse technique des incidents de sécurité, des vulnérabilités et des menaces;

- évaluation des dommages subis, le cas échéant ;

- estimation des évolutions potentielles du sinistre ;

- estimation des impacts techniques et des conséquences prévisibles sur les missions opérationnelles ;

- déclenchement et diffusion d'alerte vers les autorités, les acteurs techniques et opérationnels ;

- saisine des autorités judiciaires, si nécessaire.

4.3. **Fonction réponse.**

La fonction réponse permet de déterminer, diffuser et faire appliquer les actions défensives nécessaires au travers d'ordres de conduite coordonnés par des actions de :

- préparation des mesures de réaction intégrant les priorités opérationnelles des états-majors opérationnels et des autorités d'emploi ;

- réalisation d'outils informatiques défensifs spécifiques à une menace ;

- diffusion des mesures d'urgence ;

- diffusion des mesures de reprise des activités (éradication, restauration, secours) ;

- diffusion des mesures d'investigation ;

- communication de crise ;

- clôture et capitalisation du retour d'expérience.

5. ORGANISATION PERMANENTE DE VEILLE ALERTE RÉPONSE.

L'organisation permanente de veille, alerte et réponse (OPVAR) est la structure mise en place par le ministère de la défense pour conduire les actions de lutte informatique défensive nécessaires à la protection de ses systèmes d'information, incluant la mise en œuvre des plans gouvernementaux Vigipirate SSI et Piranet.

Elle répond aux exigences de permanence, de réactivité et de cohérence des actions. Elle applique le principe d'unicité de commandement et s'appuie sur du personnel formé et entraîné afin de mettre en œuvre les fonctions de veille, alerte et réponse.

Elle se compose de plusieurs niveaux qui interagissent selon les grands principes décrits ci-dessous et dont les modalités d'exécution sont précisées dans des directives techniques et opérationnelles complémentaires.

5.1. **Comité directeur.**

Le comité directeur de l'OPVAR assure la haute direction de l'organisation. Il définit ses orientations et ses priorités stratégiques, assure l'interface avec les autorités nationales et étrangères, dirige la communication de crise et arme la cellule de crise ministérielle de réponse aux agressions cybernétiques.

Il comprend :

- le fonctionnaire de la sécurité des systèmes d'information (FSSI), qui assure la coordination ministérielle entre les différentes autorités qualifiées, l'interface avec le cabinet du ministre et la coordination interministérielle ;

- les représentants des chefs d'état-major, directeurs et délégués pour le domaine des opérations ;

- les représentants des autorités qualifiées ;

- les représentants (emploi et SSI) du directeur central de la direction interarmées des réseaux, d'infrastructure et des systèmes d'information du ministère (DIRISI).

Le comité directeur crée des groupes de travail sur les sujets intéressant la lutte informatique défensive si nécessaire.

5.2. **Niveau central.**

Subordonné au comité directeur de l'OPVAR, le niveau central assure la permanence du commandement de l'organisation, la coordination ministérielle, ainsi que l'interface avec les organismes homologues interministériels et alliés.

Le niveau central est constitué d'un centre opérationnel et d'un centre technique assurant respectivement les volets opérationnel et technique des fonctions de veille, alerte et réponse.

5.2.1. ***Centre opérationnel.***

Le centre opérationnel du niveau central de l'OPVAR décide des mesures de réponse appropriées en fonction des éléments techniques fournis par le centre technique, de son analyse de la situation, et des priorités du commandement établies avec les différentes autorités d'emploi concernées.

Il coordonne l'action des différents acteurs opérationnels du ministère.

Il est l'interlocuteur privilégié des acteurs opérationnels nationaux et alliés.

Son domaine d'action s'étend aux armées, aux organismes interarmées, et à l'ensemble des organismes du ministère lorsque la réactivité et la cohérence des actions l'imposent.

Certains organismes, ayant des missions interministérielles ou nationales spécifiques peuvent se trouver dans l'impossibilité d'appliquer les ordres du centre opérationnel. Ils rendent compte de la situation et le comité directeur (ou son président) arbitre en cas de conflit.

Le centre opérationnel peut déléguer la conduite de certaines opérations au centre technique.

Le centre opérationnel du niveau central de l'OPVAR est le centre de planification et de conduite des opérations, bureau J6 SIC, cellule lutte informatique (CPCO/J6/LI).

5.2.2. ***Centre technique.***

Le centre technique du niveau central de l'OPVAR assure la fonction de veille et réalise le volet technique des fonctions d'analyse et de réponse au profit du centre opérationnel, en particulier, le suivi de la situation des réseaux, l'analyse technique des menaces, vulnérabilités et incidents ainsi que la préparation des mesures de réponse appropriées.

Il coordonne l'action des acteurs techniques du ministère.

Il est l'interlocuteur privilégié des autres acteurs techniques nationaux et alliés.

Son domaine d'action s'étend aux armées, aux organismes interarmées, et à l'ensemble des organismes du ministère lorsque la cohérence des actions l'impose.

Il peut se voir déléguer la conduite de certaines opérations par le centre opérationnel.

Le centre technique du niveau central de l'OPVAR est le centre d'analyse de lutte informatique défensive (CALID).

Il s'appuie sur une structure chargée de son soutien en expertise technique, la cellule d'expertise LID (CELEX).

Cette cellule a pour vocation de fédérer et de capitaliser l'apport en capacité d'expertise de l'ensemble des organismes du ministère avec les experts affectés dans les différents centres et les moyens techniques de communication et de travail collaboratif mis à leur disposition.

5.3. **Niveau des autorités qualifiées et des autorités d'emploi.**

Les autorités qualifiées sont responsables de la mise en place de structures répondant aux exigences du point 1 et capables d'assurer les actions de lutte informatique défensive pour leurs entités et leurs systèmes d'information. Elles peuvent déléguer tout ou partie des fonctions de veille, alerte et réponse correspondantes au niveau central de l'OPVAR en y transférant les moyens correspondants.

Ces structures assurent la remontée d'alerte sur anomalie constatée localement et garantissent une application des mesures préconisées ou ordonnées par les centres opérationnel et technique de niveau central, en cohérence avec les activités opérationnelles du moment.

Ces structures s'appuient en général sur les voies fonctionnelles, de commandement et techniques existantes qui sont rappelées infra.

5.3.1. ***Voie fonctionnelle SSI.***

Sous la responsabilité de l'autorité qualifiée, la voie fonctionnelle SSI d'un état-major, direction ou service comprend un OSSI central (coordinateur SSI pour les états-majors ou OSSI de direction), des OSSI d'organismes (avec des niveaux intermédiaires dans certains cas), des RSSI (responsables SSI de système) et des CSSI (correspondants SSI).

5.3.2. ***Voie opérationnelle.***

Sous l'autorité du chef d'état-major, du directeur, du secrétaire général ou du délégué, la voie commandement comporte plusieurs niveaux hiérarchiques. Elle s'appuie sur une chaîne opérationnelle d'organisme, utilisée dans le cadre de la lutte informatique défensive, et en particulier sur son centre opérationnel (état-major d'opération (EMO) ou équivalent) et au niveau local, sur des correspondants de site (adjoint de lutte informatique de site (ALIS) ou équivalent).

5.3.3. ***Voie technique.***

La voie technique SSI d'un état-major, direction ou service est subordonnée à la voie de commandement, elle comporte un centre technique (cellule de vigilance informatique ou équivalent) qui fournit un premier niveau d'expertise et d'assistance SSI à tous les centres d'exploitation, les administrateurs systèmes, réseaux et sécurité de ses organismes.

5.3.4. ***Centres d'exploitation technique.***

Les centres d'exploitation technique, subordonnés aux autorités d'emploi, ont un rôle prépondérant pour l'efficience de la lutte informatique défensive. C'est à leur niveau que sont effectuées les opérations techniques suivantes :

- application des mesures techniques liées à la posture permanente de sécurité (application des procédures d'exploitation de la sécurité) ;

- détection d'incidents et prise de mesures immédiates en réaction (application des fiches réflexes) ;

- mise en œuvre des mesures palliatives et correctives ordonnées par l'OPVAR.

Les centres d'exploitation technique participent activement aux fonctions de veille, alerte et réponse.

5.4. **Relations avec les industriels.**

Le système d'information d'un industriel interconnecté au système d'information du ministère entre dans le champ d'application de la présente instruction. Une structure locale est créée ou identifiée pour assurer les fonctions de veille, alerte et réponse en coordination avec les structures dédiées de l'organisme contractant.

Pour les systèmes d'information des industriels, traitant des informations classifiées de défense ou des informations sensibles du secteur défense, non interconnectés à un système du ministère, les fonctions de diffusion d'alerte et de remontée des incidents doivent être assurées. Des clauses contractuelles spécifiques décrivent le dispositif à mettre en place chez l'industriel et ses relations avec les structures OPVAR du ministère.

Dans le cadre réglementaire de l'arrêté du 18 avril 2005 (1) concernant les marchés classés ou les marchés à clause de sécurité, la direction de la protection et de la sécurité de défense, en collaboration avec les autorités contractantes, assure la remontée des incidents qu'elle est amenée à connaître, en provenance des industriels de la défense, vers le centre d'analyse de lutte informatique défensive.

6. PRÉPARATION DES PERSONNELS.

La prise en compte correcte des problèmes de lutte informatique ne peut passer que par une formation continue et des entraînements réguliers, impliquant tous les niveaux hiérarchiques au sein de tous les organismes du ministère.

6.1. **Formation.**

La formation LID doit répondre à plusieurs objectifs :

- instruire le personnel appelé à exercer des responsabilités LID ;

- sensibiliser les utilisateurs des systèmes d'information à leur rôle d'acteurs de LID.

La direction générale des systèmes d'information et de communication (DGSIC) définit la typologie des formations et vérifie l'adaptation des formations proposées aux besoins. Elle veille au maintien et à l'alimentation du vivier en spécialistes SSI, en particulier les acteurs de la LID, en liaison avec les armées, directions et services.

6.2. **Entraînement.**

Au niveau national, la LID est prise en compte dans tous les exercices pour lesquels les systèmes d'information tiennent une place prépondérante. Les ordres d'exercice concernés intègrent donc systématiquement un volet LID.

Le personnel formé aux actions de LID valide ses acquis théoriques en participant à ces exercices.

Dans les exercices multinationaux, la France cherchera à être intégrée dans les structures LID.

Le ministère participe aux exercices interministériels dédiés à la sécurité des systèmes d'information (2) conduits par le secrétariat général de la défense nationale (SGDN).

Les structures centrales de LID sont impliquées au plus tôt dans la préparation des exercices, notamment dans le développement des scénarios.

L'organisation des exercices ministériels de LID est décidée en comité directeur de l'OPVAR, qui assure la coordination avec les exercices multinationaux, les exercices interministériels et les exercices interarmées conduits par l'état-major des armées.

L'analyse après action fera effort sur les conclusions à tirer et sur les adaptations à proposer pour maintenir une capacité ministérielle en permanence adaptée à la menace.

Pour le ministre de la défense et par délégation :

L'ingénieur général des télécommunications,
directeur général des systèmes d'information et de communication,

Henri SERRES.

---

(1) n.i. BO.

(2) En interministériel, la notion de LID n'existe pas, on parle seulement de SSI.