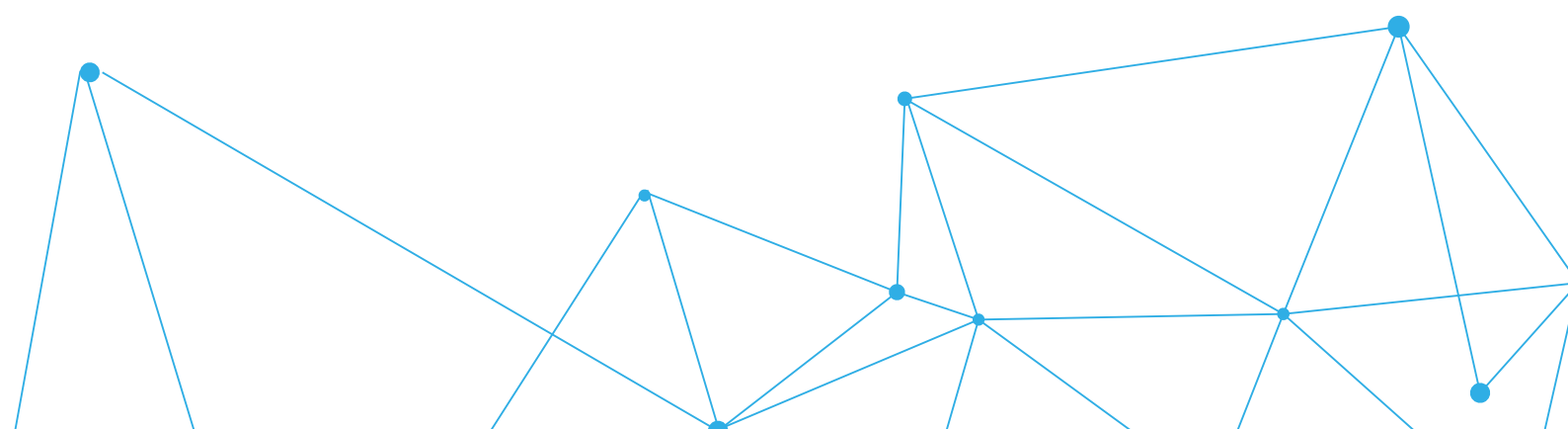
Politique ministérielle de lutte informatique défensive

COMCYBER
COMMANDEMENT DE LA CYBERDÉFENSE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES

SOMMAIRE



1. LA LUTTE INFORMATIQUE DÉFENSIVE : UN DÉFI COLLECTIF

La protection des réseaux informatiques et des systèmes d'information constitue le premier rempart pour empêcher une attaque informatique. Si ce premier rempart est indispensable, la dynamique de numérisation des systèmes qui soutiennent les activités du ministère, y compris au profit de son engagement opérationnel *via* ses systèmes de commandement et ses systèmes d'armes, offre de nouvelles opportunités aux attaquants ; elle nous impose donc de développer de nouveaux modes de défense, adaptés à ces nouvelles menaces.

C'est sur la base de ce constat que le ministère des Armées a souhaité redéfinir sa politique en matière de lutte informatique défensive (LID). Cette politique ministérielle de LID, présentée sous forme d'une instruction ministérielle, nr.101000/MINARM du 01 décembre 2018, développe des principes de réponse à ces questions, en précisant l'organisation et les missions qui s'appliquent à tous les organismes placés sous l'autorité de la ministre des Armées, ainsi que les attentes et contraintes de ceux qui contribuent, par des services ou des capacités, à son engagement (industriels...).

Les grands axes de cette nouvelle politique LID sont résumés dans cette synthèse.

1.1 Le cyberespace : espace de vulnérabilité et espace d'opportunité

Si nos adversaires n'ont pas fondamentalement changé leurs objectifs – espionnage, sabotage ou encore manipulation – les modes opératoires et techniques utilisés pour y répondre sont sans cesse renouvelés par l'émergence continue de nouvelles pratiques et technologies liées au numérique, ainsi que l'hyper connectivité de nos équipements et réseaux.

Le cyberespace possède une dynamique qui lui est propre : instantanéité des échanges, diffusion en réseau, massivité de données accessibles à tous, effacement des frontières... Il est aussi un multiplicateur d'efficacité pour peu que l'on dispose des bonnes données et informations, qui sont devenues une ressource critique, au cœur du fonctionnement politique, économique et social des sociétés modernes.

Or, nos adversaires ont parfaitement compris l'avantage politique, économique ou opérationnel qu'ils pouvaient obtenir de l'exploitation des vulnérabilités de cette numérisation galopante, touchant aussi le champ de bataille.

L'anticipation et la maîtrise de ce risque constituent les deux paramètres clefs d'une LID devenue indispensable pour préserver le fonctionnement quotidien

du ministère ainsi que sa supériorité opérationnelle dans les conflits où les armées sont engagées.

1.2 Les six missions de la cyberdéfense

Pour atténuer leur vulnérabilité, les systèmes militaires doivent offrir le meilleur niveau de « défendabilité » possible. Il s'agit, d'une part, de s'assurer de la bonne prise en compte du risque d'attaque cyber et des potentielles conséquences sur les organisations ou individus visés et, d'autre part, d'être en mesure d'adapter notre capacité d'action et de réaction à une attaque cyber, en fonction du contexte opérationnel ou de la réalité de la menace.

Au-delà de la notion de « défendabilité » de nos systèmes, la cyberdéfense au sein du ministère des Armées est déclinée en pleine cohérence avec les six missions définies par la revue stratégique de cyberdéfense publiée en février 2018 :

- prévenir : il s'agit de faire prendre conscience aux utilisateurs du risque représenté par la numérisation des organisations ou des équipements qu'ils servent. Cette mission incombe au Haut fonctionnaire correspondant de défense et de sécurité (HFCDS) du ministère ;
- anticiper : il s'agit d'évaluer en permanence les probabilités de cyberattaques et prendre des mesures préventives lorsque la menace paraît suffisamment forte. Cette mission incombe à l'Agence nationale de sécurité des systèmes d'information (ANSSI), en coordination avec les services de renseignement et le Commandement de la cyberdéfense (COMCYBER) sur le périmètre du ministère des Armées ;
- protéger : il s'agit de diminuer la vulnérabilité de nos systèmes informatiques, à la fois en compliquant la tâche des attaquants potentiels et en facilitant la détection des cyberattaques. La protection est nécessaire tout au long du cycle de vie des systèmes ;
- détecter : il s'agit de rechercher des indices d'une éventuelle cyberattaque en cours. Cette mission relève de la responsabilité du COMCYBER et des unités subordonnées à la ministre des Armées. Pour compléter ses informations, il sollicite ses partenaires nationaux et internationaux ;
- réagir : il s'agit de résister à une cyberattaque afin qu'elle n'empêche pas la poursuite de notre activité. Dans la plupart des cas, le COMCYBER déclenche alors une opération de LID, en liaison avec l'ANSSI. Elle peut

entraîner l'emploi de moyens qui sortent du domaine de la cyberdéfense, voire du ministère des Armées (saisie de la justice, action diplomatique, rétorsion économique, etc.) ;

- attribuer : il s'agit de préciser l'auteur d'une cyberattaque par des preuves ou un faisceau d'indices. Les services de renseignement sont au cœur de ce processus de recueil d'indices d'attribution. La décision d'attribution appartient aux plus hauts responsables politiques.

Les actions de prévention et de protection concernent les systèmes informatiques du ministère des Armées (zone amie).

Les missions d'anticipation, de détection et de réaction s'intéressent aux systèmes informatiques appartenant aux autres catégories d'acteurs (zones neutre et ennemi).

1.3 La LID au sein du ministère des Armées

La LID regroupe l'ensemble des actions, techniques et non techniques, conduites pour faire face à un risque, une menace ou à une cyberattaque réelle, en vue de préserver notre liberté d'action.

La LID couvre principalement trois de ces missions : anticiper, détecter et réagir et complète les missions : prévenir, protéger et attribuer. Elle contribue ainsi à la résilience des armées et plus globalement à l'élaboration des stratégies de réponse aux niveaux ministériel et interministériel.

Au sein du ministère des Armées, les opérations de LID sont planifiées et conduites par le COMCYBER, en coordination avec l'ANSSI, les services de renseignement, et éventuellement d'autres partenaires (nationaux ou internationaux).

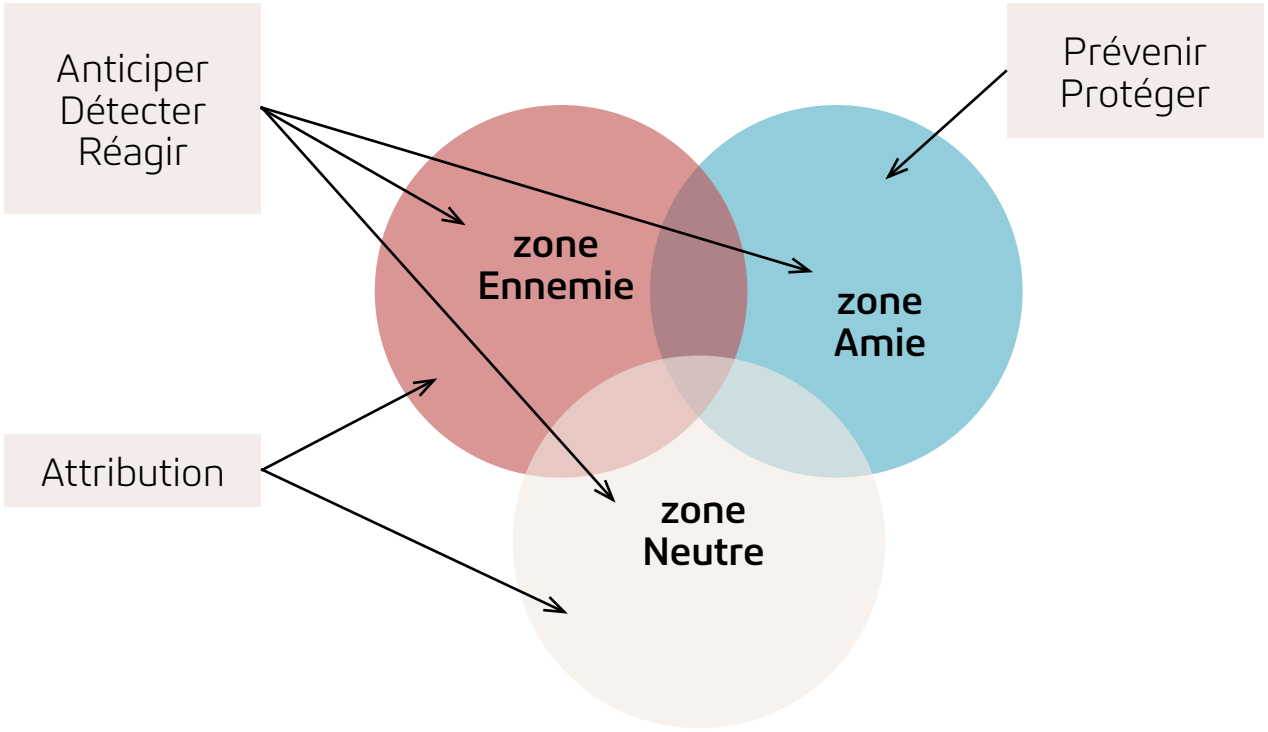


Figure 1 : champs d'application des six missions de cyberdéfense

2. LA LUTTE INFORMATIQUE DÉFENSIVE AU SEIN DU MINISTERE DES ARMEES : UNE ORGANISATION ADAPTÉE ET OPTIMISÉE

2.1 La cyberdéfense militaire au sein de la cyberdéfense de l'État

La cyberdéfense de l'État relève de la responsabilité du directeur général de l'ANSSI.

Pour le ministère des Armées, la conduite de la cyberdéfense de ses systèmes d'information est de la responsabilité du chef d'état-major des armées (CEMA).

Le COMCYBER, subordonné au CEMA, est pour sa part chargé de l'organisation et des opérations de LID pour l'ensemble du ministère.

Le COMCYBER assiste et conseille la ministre des Armées dans son domaine de compétence.

Il se coordonne très étroitement avec l'ANSSI dans l'exercice quotidien de ses missions de cyberdéfense.

Dans un souci de cohérence et d'efficience, la chaîne de commandement de cette cyberdéfense est dite unifiée, centralisée et spécialisée pour tout le ministère. C'est-à-dire qu'elle est pilotée et coordonnée par le COMCYBER et que, composée d'experts de la cyberdéfense, elle doit en outre favoriser les synergies entre les différentes organisations de LID tout en permettant de disposer d'une vision globale de la situation cyber.

La mobilisation rapide des moyens et des compétences disponibles passe par le partage des procédures et des outils de gestion de crise. De même, une cyberdéfense efficace passe par une plus grande intégration avec les partenaires nationaux et une forte coordination avec les partenaires internationaux et les industriels. Ces interactions imposent de renforcer l'interopérabilité des organisations et des capacités à tous les niveaux, techniques et décisionnels.

2.2 Subsidiarité dans l'action de cyberdéfense militaire

Au sein du ministère, chaque état-major, direction et service, met en place les moyens de LID sur son périmètre de responsabilité en application du principe de subsidiarité. Chaque responsable de cyberdéfense au sein du ministère doit pouvoir s'appuyer sur une structure opérationnelle de type *security operating centre* (SOC) chargée de la supervision de ses systèmes. Les SOC constituent le premier niveau de détection des attaques cyber.

A l'échelle du ministère, sous les ordres du COMCYBER, le Centre d'analyse en lutte informatique défensive (CALID) assure une « hypervision » technique d'ensemble, qui synthétise et partage l'information des situations cyber produites par l'ensemble des SOC ou par ses moyens propres.

Au sommet de la chaîne de LID, le COMCYBER s'appuie sur le centre des opérations cyber (CO Cyber) pour orienter le travail du CALID et des SOC. En particulier, il partage l'état de la menace cyber et des nouvelles vulnérabilités découvertes afin d'optimiser l'efficacité de la chaîne de cyberdéfense et de protection du ministère. Le CO agit aussi en soutien du CALID dans la gestion d'un incident cyber.

2.3 Connectivité et rapidité de transformation du milieu cyber : deux clés de la modernisation du ministère qui imposent une LID partagée et coordonnée

La transformation numérique du ministère se caractérise à la fois par la rapidité à laquelle elle est conduite et une connectivité entre les systèmes toujours plus importante, au sein du ministère, mais également avec nos différents partenaires dont les industriels de la Défense.

Ainsi, pour une meilleure efficacité contre la menace, ces partenaires extérieurs au ministère doivent être parties prenantes de la LID du ministère. En effet, l'attaquant recherche toujours un point faible ou indirect pour pénétrer les systèmes militaires.

Face à ces attaques potentielles, le ministère, par le biais de la Direction Générale de l'Armement (DGA) et du COMCYBER, proposera aux industriels de Défense, en étroite liaison avec l'ANSSI, une convention qui précise les rôles et responsabilités des différents acteurs, en matière de prévention et de gestion d'attaque cyber touchant directement ou indirectement les systèmes et équipements qu'ils développent.

3. LES OPERATIONS DE LUTTE INFORMATIQUE DÉFENSIVE : UNE POSTURE PERMANENTE CYBER POUR LA DÉFENSE DE NOS SYSTÈMES NUMÉRISÉS

La LID du ministère obéit à des règles d'engagement et de confidentialité édictées par le COMCYBER.

Une opération de LID peut nécessiter de dégrader ou d'interrompre un service. Cette décision relève généralement du chef de l'unité qui utilise le système en question. Néanmoins, si la gravité ou l'urgence de la situation l'exige, la coupure peut être imposée par un échelon supérieur ou le COMCYBER.

Le cyberespace est un milieu de confrontation pour les Etats ou les organisations non gouvernementales dans lequel le risque d'attaque est considéré comme permanent, y compris en temps de paix. La tension générée par ces attaques cyber, cycliques ou soudaines, de gravités variables, impose l'adoption d'une vigilance de tous les instants, qui s'incarne à travers la posture permanente de cyberdéfense (PPC) pour le ministère des Armées.

La PPC est constituée de l'ensemble des dispositions adoptées pour assurer en permanence (24h/7j) la défense des systèmes informatiques du ministère dans le *continuum* paix-crise-guerre. Elle est placée sous le commandement du COMCYBER.

La revue stratégique de cyberdéfense de février 2018 a établi un classement des attaques informatiques qui tient compte de la caractérisation de l'impact (de négligeable à extrême) et de la possibilité de caractériser juridiquement cette attaque comme une agression armée. En cohérence avec ce classement, la PPC identifie quatre niveaux de menace à l'encontre des systèmes informatiques du ministère : jaune et orange, identifiant des risques potentiels plus ou moins importants, rouge, des risques hostiles jugés plausibles et écarlate, des risques majeurs et simultanés.

Cette échelle de risques, qui associe niveau de menace et objectifs de protection des systèmes, est complétée par un stade d'alerte, « vigilance », « renforcé », ou « crise », qui précise si l'attaque est à venir ou en cours, pour adapter en conséquence les mesures à prendre au sein du ministère, qui peuvent ainsi ponctuellement varier d'une zone ou d'un domaine particulier à l'autre.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES