Politique ministérielle de
lutte informatique défensive (LID)

1 / Un défi collectif

- Le cyberespace est à la fois un espace de vulnérabilité et d'opportunité : l'anticipation et la maîtrise du risque cyber constituent les paramètres clefs de la LID.
- La cyberdéfense s'articule autour de six grandes missions : prévenir, anticiper, protéger, détecter, réagir, attribuer.
- La LID au sein du ministère des Armées regroupe l'ensemble des actions conduites pour faire face à un risque, une menace ou à une cyberattaque réelle. Elle couvre principalement les missions : anticiper, détecter et réagir et complète les missions : prévenir, protéger et attribuer.

Les opérations de LID sont planifiées et conduites par le COMCYBER, en coordination avec l'Agence nationale de la sécurité des systèmes d'information, les services de renseignement et éventuellement d'autres partenaires (nationaux ou internationaux).

2 / Une organisation adaptée et optimisée au sein du ministère des Armées

- Au sein de la cyberdéfense de l'État sous responsabilité du directeur général de l'Agence nationale de la sécurité des systèmes d'information ; la cyberdéfense militaire est pilotée et coordonnée par le COMCYBER chargé de l'organisation et des opérations de LID pour l'ensemble du ministère des Armées selon une chaîne de commandement, unifiée, centralisée et spécialisée.
- Chaque responsable de cyberdéfense au sein du ministère s'appuie sur une structure opérationnelle de type security operating center (SOC) chargée de la supervision de ses systèmes. Le Centre d'analyse en lutte informatique défensive (CALID) assure une « hypervision » technique d'ensemble à l'échelle du ministère.

Au sommet de la chaîne LID, le COMCYBER s'appuie sur le centre des opérations cyber (CO Cyber) pour orienter le travail du CALID et des SOC.

➜ La particularité de la menace cyber et de la rapidité de transformation de son milieu impose une LID partagée et cordonnée avec nos partenaires extérieurs ; les rôles et responsabilités des différents acteurs sont conventionnés.

3 / La posture permanente cyber (PPC) pour la défense de nos systèmes numérisés

➜ Le cyberespace étant un milieu de confrontation, une vigilance de tous les instants est nécessaire, d'où la nécessité d'une 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. Elle identifie quatre niveaux de menace :

- jaune et orange : risques potentiels plus ou moins importants ;
- rouge : risques hostiles jugés plausibles ;
- écarlate : risques majeurs et simultanés.

COMCYBER
COMMANDEMENT DE LA CYBERDÉFENSE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES ARMÉES