Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

Pacte Défense Cyber

50 mesures pour changer d'échelle

En 2013, le ministère de la Défense a dû affronter plus de 780 incidents informatiques significatifs, contre 420 incidents en 2012. Cette hausse importante témoigne d'un renforcement des actions malveillantes dans le cyberespace. Mais ces chiffres résultent aussi d'une meilleure surveillance et d'un plus haut niveau de vigilance du ministère, qui détecte ainsi plus de menaces. Ces incidents sont en majeure partie de faible ampleur ; en cela, ils relèvent essentiellement de la cybercriminalité et de la cybercontestation. Grâce à la coopération avec l'ANSSI, en particulier, nous avons également détecté des tentatives d'intrusion ou d'attaque contre nos forces en opération, ainsi qu'à l'encontre d'experts de domaines sensibles du ministère. Certains de nos prestataires extérieurs ou industriels de défense ont par ailleurs été ciblés. C'est une réalité dont nous avons désormais pris la pleine mesure.

Le Livre Blanc pour la Défense et la Sécurité Nationale de 2013 ne s'y est pas trompé : il fait de la cyberdéfense une priorité nationale. Depuis celui de 2008, le phénomène s'est globalisé et accéléré, et les cyberattaques revêtent désormais un potentiel destructeur particulièrement fort dans nos sociétés qui n'ont jamais été aussi dépendantes du numérique. La menace d'attaques massives ou destructrices est devenue une préoccupation importante pour le ministère, pour les forces armées, pour les services de renseignement et plus largement pour l'ensemble de la communauté nationale de cyberdéfense. Plusieurs pays ont déjà été victimes d'attaques majeures ; l'espionnage massif pénétrant jusqu'au cœur de nos infrastructures et de nos grandes entreprises est aujourd'hui une réalité ; et même une attaque peu sophistiquée est capable de perturber lourdement le fonctionnement d'un organisme mal préparé et mal défendu. De plus, il faut souligner qu'aujourd'hui, toute opération militaire, et plus généralement toute confrontation, comporte un volet cyber plus ou moins développé. Les actions cyber font désormais partie de l'arsenal de nombreuses nations. C'est donc un champ stratégique nouveau que nous devons explorer, investir, maîtriser.

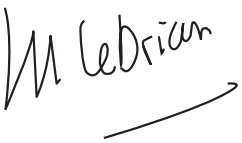
Le ministère de la Défense s'est pleinement engagé sur les enjeux de la cyberdéfense ces dernières années. Mais des efforts importants doivent encore être accomplis pour durcir sa posture, pour atteindre et maintenir dans le temps le niveau d'excellence requis par l'évolution extrêmement rapide des menaces.

C'est pourquoi je lance aujourd'hui « le Pacte Défense Cyber ». C'est à la fois une mobilisation du ministère et une main tendue à la communauté nationale de cyberdéfense et à nos partenaires étrangers. J'entends apporter un soutien sans faille à l'ANSSI, en pleine concertation et complémentarité avec les autres ministères régaliens, tout en mettant l'excellence des capacités de nos armées et services au soutien de la posture nationale de cyberdéfense.

Nous ne pourrons relever le défi des cybermenaces seuls. À travers des propositions très concrètes, cette stratégie comporte donc à la fois des mesures internes au ministère, mais aussi, sous forme d'un pacte cyber, un ensemble de mesures destinées à créer ou soutenir des projets extérieurs des collectivités locales, des grands groupes, des PME/PMI, de nos partenaires internationaux, ou des opérateurs de formation.

Parce que le cyberespace est en constante évolution, la défense tout entière doit se placer dans une démarche résolument proactive. C'est ainsi que la France restera dans le premier cercle des quelques nations qui comptent dans le cyberespace et investissent pour préserver à long terme leur souveraineté.

Jean-Yves Le Drian,
ministre de la Défense



E.M.A

DGA

COMMANDEMENT OPÉRATIONNEL DE CYBERDÉFENSE

Axe 1

Durcir le niveau de sécurité des systèmes d'information et les moyens de défense et d'intervention du ministère et de ses grands partenaires de confiance.

Axe 2

Préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle.

Axe 3

Renforcer les ressources humaines dédiées à la cyberdéfense et construire les parcours professionnels associés.

Axe 4

Développer le Pôle d'excellence en cyberdéfense en Bretagne au profit du ministère de la Défense et de la communauté nationale de cyberdéfense.

Axe 5

Cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'Alliance Atlantique et dans les zones d'intérêt stratégique.

Axe 6

Favoriser l'émergence d'une communauté nationale défense de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve.