« L'État a le devoir d'assurer la sécurité en veillant, sur l'ensemble du territoire de la République, à la défense des institutions et des intérêts nationaux, au respect des lois, au maintien de la paix et de l'ordre publics, à la protection des personnes et des biens. » (Art L111-1 du code de la sécurité intérieure).

Cette exigence de sécurité s'étend désormais également au cyberespace, tant ce dernier est au centre du fonctionnement de notre société, qui s'appuie chaque jour davantage sur les outils numériques et les réseaux interconnectés.

Au quotidien, la sécurité dans le cyberespace au service de tous, institutions publiques, acteurs économiques et citoyens - quelles que soient leur importance et leur localisation commande d'avoir une action adaptée. Il s'agit bien d'apporter une réponse à l'ensemble des menaces cyber qui portent atteinte à la sécurité et aux libertés.

Il convient donc de lutter contre tout fait, personne ou activité qui sont une cause potentielle ou avérée d'atteinte à la sécurité intérieure exercée dans le cyberespace, au moyen de l'espace numérique ou contre un système d'information.

L'ensemble des missions du ministère (lutte contre la cybercriminalité, renseignement, protection des intérêts fondamentaux de la Nation, prévention, ordre public, intelligence économique, gestion de crise, défense et sécurité des systèmes d'information,...) est concerné par cette posture de lutte contre les cybermenaces.

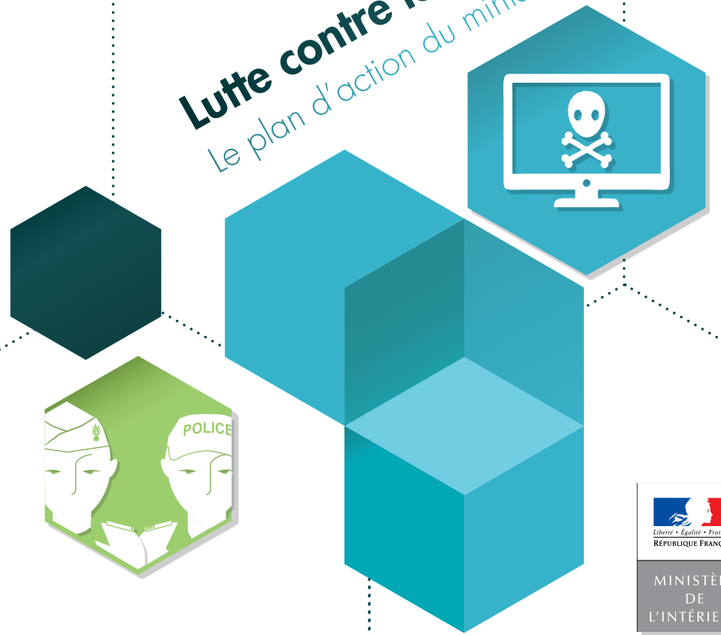
Embrassant cette vision transverse de l'action du ministère et s'intégrant dans l'environnement cyber interministériel et international très dynamique, le plan stratégique ministériel de lutte contre les cybermenaces s'articule autour de six axes.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

Lutte contre les cybermenaces
sec-cybermenaces@interieur.gouv.fr

FIC 2016

Lutte contre les cybermenaces :
Le plan d'action du ministère de l'Intérieur



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

Le plan d'action ministériel en matière de lutte contre les cybermenaces annoncé par le ministre de l'Intérieur en janvier 2015 est mis en œuvre sous la coordination de Jean-Yves Latournerie, préfet chargé de la lutte contre les cybermenaces, par les services de police, de gendarmerie, la préfecture de police, la direction générales de la sécurité civile et de la gestion des crises et le service du haut fonctionnaire de défense.

Axe 1 — Disposer en permanence d'une vision claire et actualisée de l'état des cybermenaces

Pour être en capacité d'informer les autorités de l'État, les citoyens et les acteurs économiques et d'adapter notre réponse aux atteintes à leur sécurité, il est nécessaire de bien connaître l'actualité des cybermenaces, et ceci, pour l'ensemble des domaines d'intervention du ministère : lutte contre la cybercriminalité, ordre public, protection des intérêts fondamentaux de la Nation, intelligence économique, gestion de crise, défense et sécurité des systèmes d'information et de communication du ministère. Cette démarche doit en outre permettre d'anticiper les menaces émergentes liées, par exemple, aux nouveaux usages numériques.
Le ministère de l'Intérieur s'organise donc pour disposer d'une synthèse fine et actualisée de ces cybermenaces, dans un double objectif : interne de préparation des réponses apportées, mais également externe de communication au grand public de l'état de la menace.
Afin de prendre en compte la diversité des menaces et l'émergence de nouveaux types d'atteintes, l'état des cybermenaces ne peut se limiter à un indicateur chiffré figé. Il devra davantage, dans une perspective qualitative, compléter les informations chiffrées par une appréciation des phénomènes en progression, émergents ou qui nécessitent une adaptation de la réponse (cadre juridique, partenariats à développer, messages de prévention,…).

Axe 2 — Adapter et renforcer les capacités de réponse du ministère contre les cybermenaces

Les cybermenaces sont en constante évolution. Assurer la sécurité des institutions publiques, des acteurs économiques et de nos concitoyens exige donc d'adapter en permanence les réponses du ministère, en s'appuyant sur les différents moyens dont il dispose (procédures administratives et judiciaires, renseignement, prévention, partenariats, conseil etc). Une attention particulière est portée au cadre légal.

Axe 3 — Améliorer le niveau de sensibilisation et de prévention contre les cybermenaces des particuliers, des acteurs économiques et des collectivités territoriales.

Le niveau de vulnérabilité aux cybermenaces reste élevé. Le ministère, par sa présence dans les territoires, peut contribuer significativement à rehausser le niveau de vigilance des particuliers, des acteurs économiques et des collectivités territoriales. Cette action s'inscrit dans le cadre interministériel et a vocation également à faire intervenir des acteurs non étatiques…

Axe 4 — Préparer l'avenir par un effort de recherche et développement, associant le monde académique et les industriels

Le gouvernement a inscrit la cybersécurité comme l'un des 34 plans de la Nouvelle France Industrielle, soulignant l'enjeu technologique, de souveraineté et pour l'emploi que représente ce secteur. Le ministère doit soutenir et participer activement à ces efforts, en mettant notamment en œuvre des actions partenariales. Il doit en particulier agir pour rendre plus visible la lutte contre la cybercriminalité dans les sujets traités en R&D en France et en Europe.

Axe 5 — Renforcer le niveau de sécurité des systèmes d'information propres au ministère

Le ministère ne pourra agir efficacement que s'il dispose de moyens fiables pour le traitement de l'information et l'acheminement des communications… L'exigence de robustesse et de résilience des systèmes d'information critiques se renforce sans cesse face à une menace qui pourrait cibler tout particulièrement le ministère. L'action des services en charge de la sécurité des systèmes d'information du ministère doit s'exercer en synergie avec la politique plus générale de lutte contre les cybermenaces, tant pour la connaissance de la menace que pour les partages d'expertise technique.

Axe 6 — Promouvoir l'action internationale du ministère dans le domaine de la lutte contre les cybermenaces

Le domaine cyber, en raison de sa nature, ignore les frontières. Il apparaît indispensable de prendre en compte l'environnement international et notamment européen. Alors que des synergies interministérielles se développent (SGAE, MAE ou autres) le ministère doit consolider une doctrine d'ensemble sur sa vision de l'international, promouvoir la prise en compte des besoins de ses services et sa vision des impératifs de sécurité nationale, de manière à optimiser son action aux côtés des autres acteurs institutionnels. Face à un environnement international qui évolue de manière complexe au travers des multiples enceintes de coopération, le ministère doit donc définir une stratégie ministérielle en la matière.