Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE
L'INTÉRIEUR

STRATÉGIE DE LUTTE
CONTRE LES CYBERMENACES

Le mot du ministre

Si internet est un espace de liberté, cette liberté ne saurait être absolue, dès lors que cet espace est utilisé pour porter atteinte à la sécurité de l'État ou de nos concitoyens. Les attaques menées dans le cyberespace font subir aux particuliers et aux entreprises des dommages considérables. Elles peuvent aller jusqu'à porter atteinte au fonctionnement voire à l'existence de nos institutions ou des opérateurs essentiels à la vie de la Nation.

Elles constituent de ce fait des atteintes inacceptables à la sécurité de ces acteurs.

Face au développement de la cybercriminalité, le ministère de l'intérieur doit inscrire son action dans une stratégie ambitieuse de lutte contre les cybermenaces pour se protéger et protéger l'ensemble de la communauté nationale.

La stratégie nationale de sécurité du numérique qui a été rendue publique par le Premier ministre le 16 octobre 2015 constitue la réponse de l'État à cette menace.

Le ministère de l'intérieur est un acteur prépondérant du dispositif de sécurisation des intérêts de la Nation et de préservation de la confiance des citoyens dans le numérique.

Il assure une mission de prévention des infractions et de protection des victimes ; il garantit le respect de leur vie privée et la sécurité des systèmes de traitements automatisés de données mis en œuvre par l'État.

En charge de la sécurité intérieure du pays, le ministère se doit d'assurer également sa propre sécurité numérique dans un objectif de souveraineté nationale et de permanence de l'État à travers la continuité et la réactivité de ses services, et ce notamment en période de crise.

Il doit enfin contribuer à renforcer l'offre nationale et européenne de sécurité numérique en favorisant la politique industrielle de sécurité du numérique.

Le ministère de l'intérieur a d'ores et déjà pris la mesure de ces menaces, en particulier à l'occasion des actes terroristes intervenus ces dernières années, et procédé au renforcement de ses capacités, mais ce travail mérite d'être constamment actualisé.

C'est pourquoi il est essentiel qu'une vision stratégique du rôle, des missions et de l'action du ministère de l'intérieur soit déclinée en cohérence avec l'ensemble de l'action gouvernementale sur ce sujet.

La création d'une délégation ministérielle en charge de la lutte contre les cybermenaces est une première réponse à l'affirmation d'une visibilité plus forte de l'action du ministère en ce domaine. Par son rôle d'animation de l'ensemble des acteurs concernés au sein du ministère et par son action en lien avec les acteurs de la filière industrielle de sécurité, elle prend en compte la nécessité de développer un partenariat public privé fort à la hauteur des défis auxquels notre société est confrontée.

SOMMAIRE

Préambule

La stratégie du ministère, au cœur de la lutte contre les cybermenaces

1. La défense des intérêts fondamentaux de la Nation 5

ENJEU n° 1 - Organiser la réponse du ministère face aux cybermenaces 5

ENJEU n° 2 - Maîtriser les moyens d'action de nature juridique 5

ENJEU n° 3 - Protéger les systèmes d'information du ministère 6

ENJEU n° 4 - Contribuer à la protection des infrastructures stratégiques 7

ENJEU n° 5 - Garantir la continuité des missions en cas d'attaque cyber 7

ENJEU n° 6 - Coopérer avec les acteurs économiques 8

2. La confiance numérique des utilisateurs et la protection de leurs données 9

ENJEU n° 7 - Garantir aux usagers une identité numérique forte en mettant en œuvre des services électroniques de confiance 9

ENJEU n° 8 - Renforcer l'efficacité de la lutte contre la cybercriminalité 9

ENJEU n° 9 - Assurer une prise en charge des victimes de cyber-malveillances 11

3. La sensibilisation et la formation des utilisateurs à la cybersécurité 11

ENJEU n° 10 - Assurer une formation à l'ensemble des personnels du ministère 11

ENJEU n° 11 - Généraliser les actions de sensibilisation 12

4. La promotion d'une politique industrielle de sécurité du numérique 13

ENJEU n° 12 - Soutenir l'offre de cybersécurité 13

ENJEU n° 13 - Préparer l'avenir 14

5. La défense de la souveraineté numérique et de la stabilité du cyberespace 14

ENJEU n° 14 - Influencer et diffuser au niveau international 14

ENJEU n° 15 - Promouvoir le renforcement des capacités de lutte contre les cybermenaces 15

ENJEU n° 16 - Soutenir l'autonomie stratégique numérique de la France et de l'Union européenne 16

Préambule

La lutte contre les cybermenaces s'inscrit dans le temps et doit faire l'objet d'une coordination tant entre les services du ministère qu'entre les différentes composantes participant à la défense des intérêts de la nation.

A cette fin, la mise en œuvre de la présente stratégie fait l'objet d'un pilotage rigoureux reposant sur une connaissance précise de l'action du ministère, animé par la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC).

La DMISC aligne la stratégie de lutte contre les cybermenaces du ministère à l'évolution des menaces, des technologies, des incidents et des cyberattaques.

Elle s'assure de la coordination entre ses différents services et de la coopération opérationnelle avec ses partenaires. En particulier, elle renforce les liens techniques et opérationnels établis par les services du ministère avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et les autres ministères afin d'échanger sur la nature des menaces.

Elle réalise chaque année un rapport sur l'état des cybermenaces, intégrant les priorités du ministère dans la lutte contre les cybermenaces. Ce rapport est alimenté par les contributions des services du ministère.

Elle appuiera le service statistique du ministère de l'intérieur pour élaborer les outils statistiques permettant de publier régulièrement les éléments de la statistique ministérielle relative à la cybercriminalité.

Elle alimente la stratégie de sécurité des systèmes d'information du ministère, de la compétence du comité stratégique de sécurité des systèmes d'information (COSTRAT-SSI) et présidé par le secrétaire général du ministère en sa qualité de haut fonctionnaire de défense (HFD).

Le COSTRAT-SSI mobilise de nombreux acteurs du ministère, techniques et métiers ; il représente également des enjeux forts en termes de moyens à consacrer et de décisions d'orientation dans les projets liés aux technologies de l'information.

Le COSTRAT-SSI vise entre autres à assurer le pilotage de la sécurité des systèmes d'information placé sous l'autorité du HFD et à arbitrer les priorités en fonction des risques et des menaces qui pèsent sur les systèmes.

LE MINISTÈRE DE L'INTÉRIEUR
AU CŒUR DE LA LUTTE CONTRE LES CYBERMENACES

1. La défense des intérêts fondamentaux de la Nation

Le ministère de l'Intérieur assure sa propre cybersécurité, et contribue à la cyberdéfense du pays, avec l'ANSSI, le ministère de la défense et les services des hauts fonctionnaires de défense des ministères et services de sécurité des opérateurs d'importance vitale.

Pour protéger les institutions et les intérêts nationaux, le ministère de l'intérieur fait face à six enjeux :

ENJEU n° 1 - ***Organiser la réponse du ministère face aux cybermenaces***

Disposer d'une organisation permettant de faire face aux cybermenaces impose de :

1.1. Connaître de manière approfondie les cybermenaces

Le ministère conduit une politique globale d'anticipation de la menace mise en œuvre par l'ensemble de ses services. Il organise la remontée et l'analyse des signaux faibles d'attaques, en provenance des quatre principales sources internes à sa disposition :

- le renseignement ;
- les systèmes de détection relevant du centre de cyberdéfense ;
- les services en charge de la lutte contre la cybercriminalité ;
- les services de veille.

Il partage sa connaissance de la menace avec l'ensemble de ses partenaires.

1.2. Adapter la chaîne de cyberdéfense du ministère à l'évolution de la menace

La chaîne de cyberdéfense consiste à mettre en œuvre les fonctions ministérielles d'information (veille, renseignement, recherche) d'alerte et de réponse face aux incidents de sécurité et aux cyberattaques.

Organisée autour du Centre de Cyberdéfense (C2MI) relevant du HFD, elle associe l'ensemble des fonctions de cyberdéfense des directions et coordonne la gestion des incidents de sécurité en lien avec le centre opérationnel de l'ANSSI.

1.3 Assurer la protection des agents du ministère

Le ministère a le devoir d'assurer la protection de ses agents contre les cybermenaces, afin qu'ils puissent mener à bien leurs missions et éviter qu'ils ne soient victimes à titre individuel.

Il prend les mesures nécessaires pour assurer la protection de la vie professionnelle et de la vie privée de ses agents et des personnels sensibles des autres administrations ainsi que de leurs familles.

ENJEU n° 2 - *Maîtriser les moyens d'action de nature juridique*

Les cybermenaces sont en constante évolution ; leur traitement s'effectue dans le cadre de l'État de droit ; une attention particulière doit donc être portée au cadre légal.

2.1. Informer les services du ministère du droit applicable aux technologies de l'information et de la communication

La DMISC en lien avec la direction des libertés publiques et des affaires juridiques (DLPAJ), porte à la connaissance des directions opérationnelles les évolutions législatives, réglementaires et jurisprudentielles dans le domaine numérique, que ce soit au plan national, européen et international, et ce de manière organisée et centralisée.

Les services concernés peuvent ainsi accéder à une actualité juridique couvrant tout le champ des cybermenaces.

2.2. Développer une démarche d'anticipation juridique

Le ministère opère une veille juridique permettant de vérifier l'adaptation des textes législatifs et réglementaires aux évolutions technologiques et comportementales en matière cyber, notamment en ce qu'ils permettent de poursuivre et de sanctionner les nouvelles formes de cybercriminalité.

Fort de la contribution des services opérationnels, il pilote les évolutions des normes juridiques de sa compétence et s'associe aux travaux sur les textes de la compétence des autres ministères.

ENJEU n° 3 - *Protéger les systèmes d'information du ministère*

Garant des libertés publiques, le ministère de l'intérieur doit présenter une surface d'attaque minimale aux cybermenaces. Il ne peut agir efficacement au service des populations que s'il dispose de moyens fiables pour traiter l'information et acheminer les communications. Les systèmes d'information critiques doivent bénéficier d'un niveau de sécurité élevé.

3.1. Maîtriser la sécurité de ses systèmes d'information

En cohérence avec les initiatives interministérielles conduites par l'ANSSI, le ministère s'attache à concevoir et à exploiter des systèmes d'information sécurisés et adaptés à la menace, en intégrant notamment la sécurité des systèmes d'information (SSI) dans ses projets dès leur conception.

Le ministère entreprend une démarche de gestion des risques visant à adapter l'emploi des ressources au niveau de sécurité et de protection recherché.

Le ministère met en place une politique d'achat des produits de sécurité et services de confiance destinée à assurer la continuité de ses services et de ceux qui leur sont liés, ainsi qu'un plan d'actions doté d'un calendrier, et identifie les budgets de sécurisation et de défense de son système d'information. Un suivi est assuré en COSTRAT-SSI.

Le ministère veille à protéger les informations de manière adéquate. Il s'assure que l'ensemble des agents du ministère contribue à la sécurité de son patrimoine informationnel, ainsi que ceux dont il a la charge (citoyens, partenaires, fournisseurs).

3.2. Réduire sa surface d'attaque

Les attaques ciblent le plus souvent des outils du marché parmi lesquels les postes bureautiques, les outils de communication et les objets connectés des particuliers, des institutions ou des acteurs économiques.

Le ministère s'assure que l'ensemble des moyens de communication dont il a la maîtrise ne peut être compromis et servir à des attaques.

Il soutient l'action de l'administration territoriale de l'État à travers des recommandations et l'élaboration d'outils mutualisés.

Il évalue de manière régulière les accords et partenariats qu'il conclut avec les acteurs économiques nationaux ou extranationaux afin que ceux-ci ne puissent contribuer à augmenter la surface d'attaque du ministère ou celle de l'industrie française.

ENJEU n° 4 - *Contribuer à la protection des infrastructures stratégiques*

Les intérêts fondamentaux de la nation sont régulièrement la cible d'attaques à des fins mercantiles, terroristes ou d'espionnage. Les opérateurs d'importance vitale constituent une cible privilégiée et le ministère participe à leur protection et à leur défense dans le respect des compétences dévolues au secrétariat général de la défense et de la sécurité nationale (SGDSN) et à l'ANSSI.

4.1. Contribuer à la protection des systèmes critiques de l'État

Le ministère assure la mise en œuvre de la directive nationale de sécurité relative aux activités civiles de l'État. Elle vise à préparer et à structurer la protection des intérêts stratégiques de l'État, ce qui inclut ses systèmes d'information critiques.

4.2. Permettre aux opérateurs d'importance vitale d'anticiper une crise majeure

Le ministère informe les opérateurs d'importance vitale des menaces intervenant sur leurs installations critiques.

Il soutient ces opérateurs dans les actions nécessaires à l'anticipation des crises majeures ainsi que dans leur résolution.

ENJEU n° 5 - *Garantir la continuité des missions en cas d'attaque cyber*

En charge de la sécurité des populations, le ministère de l'intérieur est l'acteur clé de la réaction des institutions dès lors que survient une crise affectant le territoire national. Dans le traitement des crises, il ne peut désormais être fait abstraction de ce champ d'action.

5.1. Intégrer les cybermenaces dans les actions de planification et les dispositifs de gestion de crise

Le traitement des cybermenaces doit être pris en compte dans les travaux de planification et de gestion des crises de la direction générale de la sécurité civile et de la gestion des crises (DGSCGC) ainsi que dans les exercices nationaux pilotés par le SGDSN, auxquels participe le ministère, en particulier dans le cadre du plan Piranet.

Pour cela, les entités en charge de ces travaux de planification s'appuient sur les spécialistes SSI.

Par ailleurs, la cellule interministérielle de crise (CIC) s'appuie sur la chaîne opérationnelle SSI pour traiter le volet cyber des crises, y compris en cas de crise à cinétique lente.

5.2. Renforcer ses capacités de réponse à la crise

Le ministère teste régulièrement sa capacité de réponse aux crises majeures, notamment en participant aux exercices interministériels de gestion de crise mettant en jeu une cybermenace.

Il recourt de plus en plus à l'emploi de réservistes de la Police et de la Gendarmerie nationales dans ce domaine, dans le cadre de la Garde nationale.

5.3. Alerter les acteurs

Le ministère prend les mesures nécessaires pour avertir les populations et les acteurs économiques en cas de crise. Il indique notamment les comportements à suivre pour en limiter les impacts sur les plans économique ou social.

5.4. Analyser et prendre en compte les retours d'expérience sur les crises

Toute crise révèle la qualité du système et des procédures mises en place.

Après chaque crise, il est important d'identifier l'origine des attaques, les voies et moyens par lesquels l'attaque a réussi à endommager les systèmes visés, et les mesures à prendre pour restaurer et renforcer l'efficacité des SI.

Le ministère procède pour chaque incident majeur à une évaluation de l'usage fait par les attaquants des outils de communication électronique, et des évolutions à apporter.

ENJEU n° 6 - *Coopérer avec les acteurs économiques*

Les données sont pour l'essentiel détenues par le secteur privé. Il est de la responsabilité de l'État d'en garantir la protection.

Il convient toutefois pour le ministère de l'intérieur, dans un cadre strict, d'être techniquement en mesure d'y accéder, pour les nécessités de sa mission de sécurisation du territoire national et des populations.

La réalisation de cet équilibre suppose des échanges avec les représentants du secteur privé. Les partenariats avec le secteur privé complètent la coopération judiciaire, en facilitant la prévention, l'échange d'informations, la lutte contre les contenus illicites ou contre l'utilisation par les criminels de tout moyen leur permettant de se soustraire aux poursuites.

6.1. Consolider les structures de dialogue en place

Des échanges sont déjà structurés autour de la plate-forme PHAROS gérée par la direction centrale de la police judiciaire (DCPJ) dont l'une des finalités est de traiter les contenus illicites du web et de centraliser en un point d'entrée unique des signalements liés à l'ensemble des infractions pénales.

PHAROS est aussi l'autorité administrative désignée pour mettre en œuvre le dispositif de retrait, blocage et déréférencement de sites pédopornographiques ou faisant l'apologie ou provoquant aux actes de terrorisme.

Le ministère anime également depuis le début de l'année 2015 un Groupe de contact permanent (GCP) avec les grands acteurs du Net, visant d'une part à l'amélioration du signalement et du retrait des contenus illicites par les opérateurs

et d'autre part à une meilleure prise en compte des demandes adressées par les enquêteurs français aux fins d'obtention de données, prioritairement dans le cadre des affaires de terrorisme.

Tous ces travaux se poursuivront, afin d'améliorer encore les retours d'information vers les enquêteurs.

6.2. Élargir les espaces d'échange avec le secteur privé.

À l'image de la démarche du groupe de contact permanent, l'animation de nouveaux groupes de travail sera poursuivie ou initiée notamment en matière de fraude numérique et de cybercriminalité pour échanger sur ces questions avec les services spécialisés.

Aux niveaux tant européen qu'international, la structuration des échanges avec le secteur privé au sein de groupes de travail devra être favorisée. Le ministère soutient l'unité européenne de signalement des contenus internet (EU-IRU), qui complète l'action partenariale mise en œuvre au niveau national en matière notamment de retrait de contenus à connotation terroriste et dont PHAROS est devenue le référent naturel.

2. La confiance numérique des utilisateurs et la protection de leurs données.

L'usage du numérique provoque une forte exposition des données qui circulent. Il s'ensuit un double besoin impliquant le ministère, de confiance et de sécurité. La déclinaison ministérielle de cet objectif national se fonde sur trois enjeux.

ENJEU n° 7 - *Garantir aux usagers une identité numérique forte dans le respect des règles de libertés individuelles*

Le ministère de l'intérieur est en charge de la production et de la délivrance des titres d'identité. Il est donc compétent pour déterminer si les « identités » qui seraient utilisées dans le cyberespace présentent, pour les usages le requérant, un niveau de garantie au moins égal à celui qu'il propose à travers les moyens classiques d'identification (CNI, passeport, titre de séjour).

7.1. Délivrer une identité numérique de niveau élevé

Le ministère de l'intérieur, avec le concours de l'Agence nationale des titres sécurisés (ANTS) et des préfectures, délivrera ou fera délivrer un moyen d'identification électronique de niveau élevé utilisable par les services de l'État, les collectivités, les entreprises et les citoyens.

Il promouvra au niveau européen une identité numérique répondant à un niveau de sécurité élevé et certifié conforme à la réglementation e-idas par des méthodes reconnues au niveau international pour les échanges relatifs aux fonctions souveraines essentielles.

7.2. Proposer des services de confiance

Le ministère encourage la transformation numérique de ses services et de ceux de l'administration territoriale de l'État. En particulier, il proposera les services de confiance nécessaires à la sécurisation de la dématérialisation des échanges de l'administration et à la pérennisation de l'action administrative dans l'espace numérique.

ENJEU n° 8 - *Renforcer l'efficacité de la lutte contre la cybercriminalité*

Les acteurs opérationnels de la lutte contre la cybercriminalité au sein du ministère de l'intérieur sont la direction générale de la police nationale (DGPN), la direction générale de la gendarmerie nationale (DGGN), la direction générale de la sécurité intérieure (DGSI) et la Préfecture de police (PP).

La cybercriminalité évolue de manière préoccupante tant par la capacité de groupes criminels organisés à lancer des attaques informatiques sophistiquées que par la

possibilité d'impacter dans des volumes considérables des particuliers ou des entreprises. La surface d'attaque est d'ailleurs augmentée par le développement des objets connectés et des villes et véhicules intelligents.

Par ailleurs la banalisation du chiffrement de bout en bout des outils de communication, la facilitation des techniques d'anonymisation et l'ouverture sur le *darkweb* d'un véritable marché des services illicites en ligne à l'usage de cybercriminels peu expérimentés sont autant d'évolutions qui nécessitent d'adapter l'action publique afin d'en renforcer l'efficacité.

8.1. Le renforcement de la collaboration internationale aux fins d'identification des auteurs.

L'expérience opérationnelle montre que les cyberattaques impliquent souvent une dimension extraterritoriale (localisation d'un serveur, d'un attaquant, d'un commanditaire, etc..) Il est donc nécessaire de disposer d'une collaboration européenne et internationale renforcée. Cette coopération prend la forme de contacts bilatéraux notamment avec les pays sources de cybercriminalité.

Elle passe aussi par des échanges entre les services compétents des différents Etats au sein des instances européennes ou internationales (Europol, Interpol et avec le soutien d'Eurojust).

Outre le partage d'informations sur les cyberattaques menées par des organisations criminelles et la coordination d'opérations d'envergure, son objectif est aussi la définition d'approches et de solutions partagées et la mise en commun des bonnes pratiques des services.

Cette action est renforcée par le dialogue déjà en place avec le secteur privé, dans le cadre du GCP.

8.2. Une adaptation du dispositif juridique, national et européen, à la lutte contre les cybermenaces.

Au plan national, l'adaptation du droit aux spécificités du cyberespace doit se poursuivre, appuyée sur l'expertise des services opérationnels. Le ministère, sous le pilotage de la DLPAJ, contribue à ces évolutions afin que les services opérationnels bénéficient de pouvoirs d'investigation et d'enquête efficaces.

Ce travail d'adaptation est mené au plan national mais également dans le cadre des travaux du Conseil de l'Europe et de l'Union européenne.

En liaison avec le ministère de la Justice, le ministère participe notamment à tous les travaux en cours au niveau européen sur la preuve numérique visant à résoudre les difficultés liées à l'obtention des preuves électroniques.

Par ailleurs, confronté à la dimension transfrontière des cybermenaces, le ministère adapte ses mécanismes d'entraide judiciaire et de coopération policière aux spécificités liées à l'obtention de la preuve numérique.

8.3. Le développement des bonnes pratiques des services opérationnels de lutte contre la cybercriminalité

Les services opérationnels poursuivront leurs initiatives pour normaliser les relations avec les fournisseurs de services numériques, renforcer le maillage territorial cyber par des formations et moyens matériels adaptés, accélérer les actions de coopération internationale. Ils doivent être force de proposition dans l'élaboration de processus d'action novateurs adaptés aux enjeux de la lutte contre la cybercriminalité.

ENJEU n° 9 - *Assurer une prise en charge des victimes de cyber-malveillances*

Au-delà d'une meilleure visibilité de la menace et des faits commis, le ministère s'attache à améliorer l'assistance aux victimes de cyber-malveillances, notamment les particuliers, les petites et moyennes entreprises et les collectivités territoriales, et ce dans le cadre d'un véritable partenariat public-privé.

La prise en compte de ces victimes passe avant tout par la capacité d'un dispositif à accueillir, écouter, analyser et orienter vers le service idoine. En effet la victime est dans l'incapacité la plupart du temps de comprendre la nature de la cyber-malveillance à laquelle elle fait face.

9.1. Soutenir le dispositif national d'assistance aux victimes de cyber-malveillances

Un dispositif national d'assistance aux victimes de cyber-malveillances sera déployé, après l'expérimentation menée conjointement par le ministère et l'ANSSI, dans la Région des Hauts-de- France.

Ce dispositif vise à améliorer la prévention et l'assistance portée aux victimes, collectivités territoriales, entreprises et particuliers. Il prévoit aussi la mise en place d'un mécanisme de remontée des incidents déclarés afin d'en affiner la connaissance et le nombre.

Il repose essentiellement sur la mise en place d'une plate-forme numérique interactive accessible via Internet qui comportera des contenus à vocation préventive ainsi que des services, notamment la mise en relation avec une assistance technique de proximité, basée sur des prestataires enregistrés et tenus par une charte d'engagements.

9.2. Améliorer l'accueil des victimes de cyber-malveillances

Toute victime de cyber-malveillance doit être accueillie par le ministère et pouvoir déposer plainte si elle le souhaite ou fournir des informations qui seront exploitées.

Outre la formation de tous les acteurs chargés de l'accueil des victimes et une charte d'accueil du public enrichie intégrant la composante numérique, les services opérationnels adapteront les systèmes d'information judiciaire pour mieux partager et exploiter les données relatives à la cybercriminalité et finaliseront des prototypes de dispositifs de plainte ou de signalement en ligne.

3. La sensibilisation et la formation des utilisateurs

Le manque de maitrise des utilisateurs reste la faille principale des cyberattaques. Il est de la responsabilité du ministère de sensibiliser et de former à la lutte contre les cybermenaces non seulement ses personnels, mais aussi les populations.

ENJEU n° 10 - *Assurer une formation à l'ensemble des personnels du ministère*

10.1. Garantir un premier niveau de formation à l'ensemble des personnels du ministère en matière de lutte contre les cybermenaces

Les évolutions technologiques permanentes conduisent les services de police et unités de gendarmerie à adapter leurs méthodes de travail et la conduite des investigations aux nouvelles formes de délinquance que constituent les cybermenaces.

Le ministère veille donc à intégrer des modules d'enseignement en matière cyber à la formation initiale dans les écoles de police et de gendarmerie, mais aussi, au-delà des agents des services enquêteurs, au profit de tous les agents du ministère.

Il s'assure que ses agents puissent accéder à des modules de sensibilisation et de formation en matière cyber, à distance, tout au long de leur vie professionnelle.

10.2. Développer un programme de formation capable d'appréhender la dimension numérique dans les métiers d'investigation du ministère de l'Intérieur

L'augmentation exponentielle des technologies de l'information et de la communication (TIC) dans la société induit la prise en compte de l'enquête numérique dans l'ensemble des thématiques criminelles traitées. L'évolution des pratiques conduit à proposer la mise en place d'un cursus du numérique et à créer des synergies indispensables avec l'ensemble des directions métiers confrontées à ces évolutions.

10.3. Améliorer le niveau de sensibilisation à la sécurité des systèmes d'information au sein du ministère

La politique SSI de l'État et la politique SSI du ministère qui en découle exigent un renforcement des actions de sensibilisation et de formation des agents.

10.4. Diffuser une culture de la donnée au sein du ministère

Le ministère veille à ce que chaque agent dispose des connaissances minimales permettant de déterminer la sensibilité ou l'absence de sensibilité des données qu'il manipule et de s'approprier les opportunités et les risques liés à leur possession.

ENJEU n° 11 - *Généraliser les actions de sensibilisation*

Le ministère, par sa présence dans les territoires, est un acteur majeur de la sensibilisation des particuliers, des acteurs économiques et des collectivités territoriales. Cette action, inscrite dans un cadre interministériel, a vocation à faire intervenir également des acteurs non étatiques.

11.1. Structurer et multiplier les initiatives de sensibilisation

Le ministère conduit d'ores et déjà des actions de sensibilisation à la cybersécurité. Ces initiatives s'inscrivent dans un cadre ministériel qui leur offre un socle de communication et par conséquent une force et une visibilité accrues, notamment auprès des publics sensibles (jeunes, seniors...).

Par ailleurs, il participe à l'organisation de campagnes de communication et d'événements permettant la diffusion des bonnes pratiques.

Dans ce domaine, la coordination des actions mais également des différents acteurs est essentielle. Le ministère travaille tout particulièrement en lien avec les coordinateurs territoriaux placés sous l'autorité de l'ANSSI qui constituent le premier réseau de niveau interministériel.

11.2. Participer à la consolidation du dispositif de la réserve citoyenne de cyberdéfense

Des réseaux régionaux de la réserve citoyenne de cyberdéfense ont été déployés comme relais pour diffuser les bonnes pratiques. Ils constituent des réseaux d'acteurs d'horizons divers particulièrement impliqués dans la diffusion de l'esprit de cyberdéfense. La généralisation de ces dispositifs à d'autres régions sera poursuivie.

11.3. Participer à la sensibilisation des opérateurs économiques sensibles.

Le ministère participe à la sensibilisation et à la mission de conseil auprès des opérateurs d'importance vitale et dans les secteurs sensibles en complément des autres services de l'État.

4. La promotion d'une politique industrielle de sécurité du numérique

Les enjeux de sécurité dans le cyberespace rendent impératif qu'en sus de son action propre, l'État soutienne la filière industrielle de cybersécurité. Il en va de la préservation de la souveraineté nationale aussi bien que du soutien de l'emploi industriel en France.

ENJEU n° 12 - *Soutenir l'offre de cybersécurité*

12.1. Soutenir l'offre de cybersécurité sur le territoire national

Il est essentiel de disposer d'un tissu industriel solide, qui soit à même de proposer des solutions de cybersécurité éprouvées et qui répondent aux différents besoins et préservent la souveraineté nationale.

Le ministère de l'intérieur est en position privilégiée pour identifier les besoins ; il constitue aussi un excellent terrain d'expérimentation afin d'éprouver les solutions et servir de référence.

Dans le prolongement des actions engagées au titre des solutions de la « Nouvelle France Industrielle » et dans le cadre des travaux menés au sein du Comité de filière des industries de sécurité (COFIS), le ministère de l'intérieur veille à mobiliser toutes les énergies en faveur de l'émergence d'une offre française et européenne de cybersécurité.

12.2. Assister l'exportation de l'offre de cybersécurité

Le ministère soutient les nombreuses entreprises qui produisent de la sécurité numérique et qui développent des solutions innovantes pour la France, tant en termes de produits que de services. Il coordonne le réseau des attachés de sécurité intérieure et en lien avec Business France et le ministère des Affaires Etrangères et du Développement International, contribue au développement des exportations. Il met en valeur la contribution des industriels en produits et services à la cybersécurité du pays**.**

ENJEU n° 13 - *Préparer l'avenir*

Le gouvernement a inscrit la cybersécurité comme une priorité de la Nouvelle France Industrielle, soulignant l'enjeu technologique, de souveraineté et pour l'emploi que représente ce secteur.

Le ministère soutient et participe activement à ces efforts au profit de la confiance numérique, en mettant notamment en œuvre des actions partenariales, dont certaines visent à assurer sa propre cybersécurité.

13.1. Une démarche tant nationale qu'européenne

Le ministère est actif en matière de recherche et développement (R&D) portant sur la lutte contre les cybermenaces et en particulier dans le cadre de partenariats.

L'Agence nationale de la recherche (ANR) et la Commission européenne ont identifié la cybersécurité comme un thème de recherche à encourager, pour lequel le ministère est force de proposition afin de valoriser les expressions de besoins, notamment en matière de lutte contre la cybercriminalité.

Il agit en particulier pour rendre plus visible la lutte contre la cybercriminalité dans les sujets traités en R&D en France et en Europe.

Le ministère est attentif à la prise en compte de la lutte contre les cybermenaces dans les programmes de recherche européens, et encourage la création de consortia dans les domaines qui l'intéressent directement.

13.2. Une interaction indispensable avec les pôles ou centres d'excellence en cyberdéfense

L'émergence de pôles d'excellence en matière de lutte contre les cybermenaces doit conduire le ministère à s'intégrer dans ces démarches et à favoriser l'échange de connaissances.

Ces relations doivent permettre également le développement de projets en commun, une participation aux enseignements ou événements organisés par ces pôles.

5. La défense de la souveraineté numérique et de la stabilité du cyberespace.

Le domaine cyber, par nature, ignore les frontières ; il est donc indispensable de prendre en compte l'environnement international et notamment européen.

Les représentants du ministère portent les enjeux et actions de la présente stratégie dans l'exercice de leurs missions en relation avec l'international, notamment au travers des pilotages et actions de la direction de la coopération internationale.

ENJEU n° 14 - *Influencer et diffuser au niveau international*

14.1. Participer de manière structurée et systématique aux travaux internationaux

Outre les coopérations engagées au sein principalement du Conseil de l'Europe, des Nations Unies, de l'Organisation pour la sécurité et la coopération en Europe, du G7, d'Europol ou d'Interpol, le ministère suit également les travaux de l'Union européenne. Cette dernière contribue à son niveau aux efforts internationaux, tant par sa stratégie de cybersécurité, que par son agenda de sécurité intérieure, qui constituent des cadres naturels d'action pour les acteurs du ministère chargés de la lutte contre les cybermenaces.

Le ministère de l'intérieur participe à la plupart de ces travaux, avec pour objectif constant le retour en sécurité intérieure. Il s'appuie sur deux principes fondamentaux : d'une part la réalisation des besoins opérationnels, avec des outils juridiques et avec le soutien de la coopération technique ou structurelle ; et d'autre part la préservation des intérêts fondamentaux de la Nation, par la promotion de l'expertise française et la réaffirmation d'une nécessaire souveraineté dans les problématiques du numérique.

Il suit également les travaux des instances mondiales de normalisation en matière de cybersécurité.

14.2. Adapter le droit international à la lutte contre les cybermenaces

Il est impératif d'agir auprès des structures internationales pour améliorer les capacités d'entraide dans le but d'interpeller les auteurs d'agissements malveillants.

Le ministère soutient, au premier chef dans le cadre de l'Union européenne, les propositions d'ajustements des outils juridiques visant à fluidifier la coopération judiciaire et les échanges avec les services étrangers, afin d'améliorer l'efficacité des enquêtes judiciaires et en particulier en promouvant l'extension de la convention de Budapest de 2001 sur la lutte contre la cybercriminalité à un maximum de pays.

Le ministère s'attache au renforcement des actions de coopération opérationnelle de ses services spécialisés en améliorant les accords de coopération bilatérale et multilatérale.

ENJEU n° 15 - *Promouvoir le renforcement des capacités de lutte contre les cybermenaces*

Le ministère s'attache au renforcement capacitaire des pays souhaitant accroître la sécurité de leurs systèmes d'information, notamment en matière de protection des infrastructures critiques et de lutte contre la cybercriminalité.

15.1. Développer les capacités des partenaires du ministère

Le ministère développe les actions d'échange à l'international dans le domaine de la formation et de la coopération technique, et recherche dans ces domaines les possibilités de financements externes pour ces actions, auprès des différents programmes européens et internationaux

Le renforcement des compétences des personnels français sera également assuré au moyen de formations internationales communes aux administrations chargées de la lutte contre la cybercriminalité, organisées notamment au sein de l'UE.

15.2. Mobiliser le réseau international du ministère

Des pays cibles sont identifiés pour y conduire les actions de coopération technique, notamment en vue de soutenir la lutte contre la cybercriminalité.

La coopération technique avec nos partenaires participe à la promotion d'une expertise qui va de pair avec la reconnaissance de nos bonnes pratiques professionnelles ; elle contribue au rayonnement de nos entreprises à l'international. Elle doit informer voire rapprocher nos partenaires étrangers de nos procédures, ce qui facilite les coopérations opérationnelles conjointes

ENJEU n° 16 - *Soutenir l'autonomie stratégique numérique de la France et de l'Union européenne*

L'autonomie stratégique numérique de la France et de l'Union européenne revêt une importance particulière dans la mesure où l'outil numérique, en abolissant les traditionnelles barrières technologiques, modifie de manière intrinsèque la manière des individus et des organismes d'appréhender la vie en société. Elle est la seule réponse, à ce jour, pour disposer d'une garantie pérenne en matière de droits fondamentaux et individuels et, *in fine*, préserver les cultures française et européenne.

16.1. Lutter contre les ingérences

Le ministère contribue à l'identification des menaces contre cette autonomie ainsi qu'à la mise en place de mécanismes efficaces de lutte contre celles-ci.

Le ministère développe sa capacité de lutte contre les ingérences étatiques, commerciales ou criminelles ou les tentatives de déstabilisation susceptibles de porter atteinte à l'autonomie stratégique de l'Europe.

Il s'assure que les activités économiques puissent se développer dans un cadre serein et concurrentiel, libre de toute pression.

16.2. Négocier et appliquer les traités internationaux

L'autonomie stratégique de l'Union dans le domaine numérique ne doit pas pouvoir être empêchée par des textes de nature supérieure. Par conséquent, cette autonomie doit être appréhendée dans un contexte international avec l'ensemble des partenaires de l'Union volontaires.

Le ministère s'assure que les traités internationaux ne puissent porter atteinte aux droits fondamentaux et individuels des acteurs européens tant lors de leur élaboration que lors de leur mise en œuvre. Le cas échéant, il initie ou participe à leur révision aux côtés des autres services de l'État et des institutions européennes.

Il s'assure du respect des traités internationaux de son champ de compétence aux niveaux national, européen et international.

16.3. Favoriser le développement des facteurs-clés d'autonomie

Le ministère fera une application stricte de la feuille de route à venir en matière d'autonomie stratégique de l'Union dans le domaine numérique.

Il soutiendra les dispositifs matériels, financiers et humains nécessaires pour garantir la pérennité de son action publique et de ses activités économiques. En particulier, il soutiendra les actions liées à la promotion d'un schéma européen de certification des outils numériques sur la base de critères communs et s'assurera que les normes techniques élaborées aux niveaux européen et international ne portent pas atteinte aux industries européennes et demeurent utilisables, sans frais, par celles-ci.

Il mettra à disposition des institutions les experts nécessaires à la défense des positions nationales ou européennes.

Il évaluera l'opportunité et, le cas échéant, participera à l'instauration d'un fond de sauvegarde des entreprises du secteur cyber pour garantir l'autonomie stratégique des technologies essentielles de la Nation.