Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Lutte contre les cybermenaces en matière de sécurité intérieure

28 mai 2014

Référence : Lettre n°89/CAB/CR/BA du 21 février 2014

Composition du groupe de travail

- Préfecture de Police de Paris
- Direction générale de la police nationale
- Direction générale de la gendarmerie nationale
- Direction générale de la sécurité civile et de la gestion des crises
- Secrétariat général : Service du Haut fonctionnaire de défense et Direction des libertés publiques et des affaires juridiques

Synthèse

« *L'Etat 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.

Cyberdéfense, Sécurité des systèmes d'information, Cybercriminalité, Cybersécurité... quelle place dans la stratégie cyber du ministère ?

Des efforts particuliers doivent être conduits pour protéger les institutions et les intérêts nationaux, ainsi que le recommande le livre blanc de la défense et de la sécurité nationale. C'est l'objet de la **cyberdéfense**, à laquelle participe le ministère de l'intérieur aux côtés de l'ANSSI et du ministère de la défense.

Protéger les systèmes d'information du ministère, mais aussi contribuer à la protection des systèmes d'information des particuliers, acteurs économiques et collectivités territoriales est également primordial. Il s'agit à la fois d'assurer une capacité d'action permanente du ministère et de contribuer à la préservation des activités de la société civile. En découle l'exigence de **sécurité des systèmes d'information,** dont la politique générale, pour les systèmes du ministère, est assurée par le Secrétaire général, Haut fonctionnaire de défense.

La **lutte contre la cybercriminalité** constitue le volet répressif de l'action du ministère, qui mobilise aujourd'hui près de 600 enquêteurs spécialisés de la gendarmerie et de la police nationales. Son cœur de cible est constitué par les infractions spécifiques – notamment les atteintes aux systèmes de traitement automatisé de données –, mais également les infractions de diffusion de contenus illicites via des systèmes d'information et de communication ou celles plus classiques commises au moyen principal des technologies numériques.

Cyberdéfense, sécurité des systèmes d'information et lutte contre la cybercriminalité se complètent et s'interpénètrent : une stratégie globale de **cybersécurité** s'appuie sur ces trois piliers.

Une stratégie ministérielle de lutte contre les cybermenaces

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 encore plus large. Il s'agit bien d'avoir 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 du cyberespace 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.

6 axes stratégiques pour renforcer la lutte contre les cybermenaces

Embrassant cette vision transverse de la mission du ministère et s'intégrant dans l'environnement cyber interministériel et international très dynamique, le groupe de travail propose un plan stratégique ministériel de lutte contre les cybermenaces autour des six axes suivants :

6 axes stratégiques pour le plan d'action ministériel
Axe 1 : Disposer en permanence d'une vision claire et actualisée de l'état des cybermenaces
Axe 2 : Adapter et renforcer les capacités de réponse du ministère contre les cybermenaces
Axe 3 : Améliorer le niveau de sensibilisation et de prévention contre les cybermenaces des particuliers, des acteurs économiques et des collectivités territoriales
Axe 4 : Préparer l'avenir par un effort de recherche et développement, associant le monde académique et les industriels
Axe 5 : Renforcer le niveau de sécurité des systèmes d'information propres au ministère
Axe 6 : Promouvoir l'action internationale du ministère dans le domaine de la lutte contre les cybermenaces

Un délégué ministériel à la lutte contre les cybermenaces

Le groupe de travail confirme l'intérêt de la désignation d'un délégué ministériel à la lutte contre les cybermenaces, qui, à la tête d'une structure légère, pilotera la mise en place de ce plan d'action.

La nature très transverse de ce domaine et l'implication de nombreux acteurs exige cet effort de coordination.

Le délégué ministériel aura ainsi pour objectifs de :

- **piloter la mise en œuvre de ce plan d'action** et **fédérer les énergies et les initiatives** des différents acteurs ;
- **définir**, en liaison avec les directions, **les stratégies ministérielles de prévention** (action 3-1) et **de recherche et développement** (axe 4) en matière de lutte contre les cybermenaces ;
- **proposer,** en coordination avec le conseiller diplomatique et en liaison avec les directions, **la doctrine internationale** (action 6-1) en matière de lutte contre les cybermenaces ;
- constituer un **point d'entrée identifié pour les acteurs extérieurs** au ministère en matière de politique de lutte contre les cybermenaces, sans préjudice des points de contact opérationnels existants ;
- **conduire une veille juridique en matière cyber** au profit des directions du ministère ;
- **conduire les travaux de rédaction d'un rapport annuel** sur l'état des cybermenaces, sous deux versions, l'une à destination du ministre (action 1-1) et l'autre du grand public (action 1-2).

Pour mener à bien sa mission de coordination, il :

- assurera la présidence d'un **comité de pilotage** à la lutte contre les cybermenaces associant l'ensemble des acteurs concourant à ce plan d'action. Ce comité de pilotage a vocation à suivre l'avancement du plan d'action, à s'assurer de la cohérence des actions entreprises et à formuler de nouvelles propositions;
- préparera et assurera le secrétariat d'un **comité stratégique** à la lutte contre les cybermenaces, présidé par le directeur de cabinet du ministre et rassemblant les directeurs du ministère.

Son action s'effectuera dans le respect des prérogatives des différentes directions du ministère.

31 actions pour renforcer la lutte contre les cybermenaces

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

Action 1-1 : établir un état annuel des cybermenaces à destination du ministre

Action 1-2 : établir un état annuel des cybermenaces à destination du public

Action 1-3 : construire des indicateurs de suivi des faits de cybercriminalité traités judiciairement par les services de police et les unités de gendarmerie

Action 1-4 : construire des indicateurs statistiques complémentaires hors des faits constatés

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

Action 2-1 : organiser une veille juridique cyber à disposition de l'ensemble des services du ministère

Action 2-2 : donner un premier niveau de formation à l'ensemble des policiers et gendarmes en matière de lutte contre les cybermenaces

Action 2-3 : travailler à un schéma de mutualisation des formations des ICC pour la police nationale et NTECH pour la gendarmerie nationale

Action 2-4 : consolider la mission de coordination de l'OCLCTIC en liaison avec les chefs de service d'investigation

Action 2-5 : créer la sous-direction de lutte contre la cybercriminalité au sein de la direction centrale de la police judiciaire

Action 2-6 : intégrer les cybermenaces dans les actions de planification et les dispositifs de gestion de crise

Action 2-7 : alerter les ministères et les OIV des cybermenaces dont ils peuvent faire l'objet, en liaison avec l'ANSSI

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

Action 3-1 : impulser une politique de prévention et de sensibilisation à la cybersécurité

Action 3-2 : contribuer au renforcement du dispositif interministériel des observatoires de la sécurité des systèmes d'information

Action 3-3 : renforcer les compétences en sensibilisation à la cybersécurité des réseaux « Intelligence économique » et « Référents sûreté » de la gendarmerie et de la police

Action 3-4 : poursuivre le développement des actions de sensibilisation à destination

des acteurs économiques

Action 3-5 : encourager la diffusion du « Permis Internet » à destination des élèves du primaire

Action 3-6 : participer à la consolidation du dispositif de la réserve citoyenne de cyberdéfense

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

Action 4-1 : contribuer au plan « Cybersécurité » de la Nouvelle France Industrielle

Action 4-2 : assurer la prise en compte des besoins spécifiques du ministère dans les actions de recherche et développement en matière de cybersécurité

Action 4-3 : susciter une communauté de recherche dans les domaines relatifs à la lutte contre les cybermenaces et consolider les partenariats existants

Action 4-4 : échanger avec les pôles ou centres d'excellence en cyberdéfense

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

Action 5-1 : analyser régulièrement le patrimoine informationnel du ministère et actualiser la liste des systèmes d'information jugés essentiels

Action 5-2 : renforcer la chaîne de Cyberdéfense du ministère

Action 5-3 : améliorer le niveau de sensibilisation à la sécurité des systèmes d'information au sein du ministère

Action 5-4 : compléter le dispositif par une capacité d'audit de la sécurité des systèmes d'information

Action 5-5 : mettre à disposition des systèmes d'information protégés (réseaux, smartphones, tablettes), en particulier pour les usages mobiles

Action 5-6 : piloter la stratégie SSI du ministère au sein du comité stratégique SSI

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

Action 6-1 : définir une stratégie ministérielle pour le volet international de la lutte contre les cybermenaces

Action 6-2 : renforcer l'action du ministère dans les travaux internationaux et européens dans le domaine de la lutte contre les cybermenaces

Action 6-3 : développer les actions d'échange à l'international en matière de formation et de coopération technique

Action 6-4 : mobiliser les services de sécurité intérieure (postes SSI) sur la thématique de la lutte contre les cybermenaces

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'Etat, 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,...).

Action 1-1 : établir un état annuel des cybermenaces à destination du ministre

L'ensemble des directions du ministère de l'intérieur informent le ministre des problématiques cyber dont il doit avoir connaissance. Toutefois, aucun bilan annuel global, synthétisant l'ensemble des menaces cyber entrant dans le champ de compétences du ministère de l'intérieur n'est établi.

L'élaboration d'un document commun, livré annuellement au ministre de l'intérieur, recensant l'état des cybermenaces contre la France et ses réseaux gouvernementaux, ses intérêts fondamentaux, ses acteurs économiques et sa population devra être réalisé.

La délégation ministérielle pilotera les travaux de rédaction de cet état annuel, en s'appuyant sur l'ensemble des directions du ministère. Le premier rapport annuel pourra être remis dès le début de l'année 2015 et aura vocation à être actualisé chaque année.

Ce rapport ne se substitue pas aux notes d'information et comptes rendus adressés par les directions dans leurs champs de compétence respectifs.

Pilote : Délégation ministérielle, en liaison avec les directions du ministère

Action 1-2 : établir un état annuel des cybermenaces à destination du public

L'information du public sur l'état des cybermenaces ne poursuit pas le même objectif que l'information du ministre et ne porte que sur une partie des données recensées. Pour autant ces deux documents disposeront d'un dénominateur commun, notamment dans leur structure. La vocation du document d'information à destination du public sera essentiellement préventif (alerte sur les phénomènes recensés, nouvelles menaces mises à jour, bilan statistique, etc) et aura pour cible les citoyens, les acteurs économiques et les collectivités territoriales. Il constituera un outil de communication pour le ministère de

l'intérieur.

La délégation ministérielle s'appuiera sur les travaux réalisés dans le cadre de l'élaboration du rapport annuel adressé au ministre de l'intérieur, et produira une version moins détaillée des grandes tendances identifiées dans la mesure où ce rapport aura vocation à être public.

Les travaux débuteront au début du troisième trimestre 2014.

Le premier document d'analyse a vocation à être finalisé et publié au début de l'année 2015.

Pilote : Délégation ministérielle, en liaison avec les directions du ministère

Action 1-3 : construire des indicateurs de suivi des faits de cybercriminalité traités judiciairement par les services de police et les unités de gendarmerie

L'élaboration d'un outil statistique permettant de mesurer les faits constatés dans le domaine de la cybercriminalité permettra d'identifier les grandes tendances, ce que l'actuel état 4001 n'est pas en mesure de produire.

Un groupe de travail, qui regroupe la mission de préfiguration du service statistique ministériel (SSM), la DGPN et la DGGN travaille actuellement à l'élaboration de cet outil. A l'été 2014, cette mission de préfiguration sera en mesure de proposer une maquette des indicateurs relatifs à la cybercriminalité selon une vision partagée par la police et la gendarmerie nationales. Ce dispositif fera l'objet de tests préalables en accompagnement du déploiement progressif de LRPPN.

A partir de début 2015, le service statistique ministériel, qui entrera en fonction à compter du 1er septembre 2014, produira de manière régulière, les chiffres de la délinquance, notamment dans le domaine de la cybercriminalité, après avoir tiré les conséquences des tests préalables.

Ces chiffres auront notamment vocation, à terme, à alimenter le rapport annuel adressé au ministre et celui à destination du public. Leur analyse permettra la production d'un état de la menace à partir des faits judiciaires constatés.

Pilotes : SSM à compter du 1er septembre 2014.

Action 1-4 : construire des indicateurs statistiques complémentaires hors des faits constatés

Il existe à côté des outils statistiques traditionnels reposant sur le recensement des faits constatés, d'autres indicateurs, internes ou externes au ministère de l'intérieur, caractérisant des intentions malveillantes qui peuvent être repris et analysés afin d'établir au plus juste l'état de la menace (ex : attaques informatiques subies par le ministère, analyse du volume des signalements PHAROS, données issues de la banque de France sur les fraudes aux cartes bancaires, etc).

Les indicateurs utiles et pertinents devront au préalable être identifiés et seront repris dans les rapports annuels à destination du ministre et du public. Pour ce qui concerne les indicateurs externes, une évaluation attentive de leur fiabilité et de leur pérennité devra être menée.

Des premiers indicateurs internes pourront être suivis dès fin 2014. L'identification d'indicateurs externes sera réalisée par le SSM de manière progressive et méthodique dans le courant de l'année 2015.

Pilote :SSM à compter de 2015

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 nos réponses, en s'appuyant sur les différents moyens dont dispose le ministère (procédures administratives et judiciaires, renseignement, prévention, partenariats, conseil etc). Une attention particulière au cadre légal doit être portée.

Action 2-1 : organiser une veille juridique cyber à disposition de l'ensemble des services du ministère

Les directions générales du ministère de l'intérieur ont chacune mis en place de manière empirique une mission de veille juridique en matière cyber. L'objectif est de porter à la connaissance des services opérationnels, les évolutions législatives et jurisprudentielles dans le domaine cyber, que ce soit au plan national, européen et international.

Cette même mission est déclinée de façon redondante par les différentes directions et mériterait d'être organisée et centralisée, afin que les services concernés puissent accéder de manière adéquate à une actualité juridique agrégeant des sources pertinentes couvrant tout le spectre des cybermenaces.

Un recensement préalable des dispositifs existants permettra d'identifier les carences et les redondances éventuelles.

La délégation ministérielle aura vocation à élaborer une lettre mensuelle d'actualité juridique, dont le périmètre devra être défini en lien avec la DLPAJ ainsi que les directions générales de la police et la gendarmerie nationales. Elle sera diffusée à l'ensemble des directions du ministère de l'intérieur, notamment par sa mise en ligne sur le site intranet du ministère de l'intérieur.

La mise en œuvre de cette action aura lieu au cours du 4ème trimestre 2014.

Pilote : Délégation ministérielle en liaison avec les directions du ministère

Action 2-2 : donner un premier niveau de formation à l'ensemble des policiers et gendarmes 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. La formation initiale et continue des effectifs des deux forces apparaît à ce titre primordiale.

Dans cette perspective, il convient de pouvoir disposer d'un support actualisé régulièrement, couvrant l'ensemble des besoins en formation de premier niveau relatifs aux cybermenaces. Des modules d'enseignement réservés aux premiers intervenants ont été élaborés conjointement par la police et la gendarmerie nationales, sous forme principalement d'enseignement à distance.

L'objectif de l'action est de pouvoir diffuser cette formation de manière large aux policiers et gendarmes premiers intervenants, grâce à la mise en ligne du support sur les plate-formes institutionnelles d'enseignement à distance, à compter du second semestre 2014.

Elle sera également intégrée à la formation initiale dans les écoles de police et de gendarmerie entre le second semestre 2014 et le premier semestre 2015.

Pilotes : DGGN, DGPN et préfecture de police.

Action 2-3 : travailler à un schéma de mutualisation des formations des ICC pour la police nationale (investigateurs cybercriminalité) et NTECH pour la gendarmerie nationale

La police et la gendarmerie nationales disposent de formations distinctes en matière de lutte contre la cybercriminalité : les investigateurs en cybercriminalité (ICC) et les enquêteurs technologies numériques (NTECH). Même si ces formations présentent des points communs, elles sont toutefois différentes par certains aspects, ne recouvrant pas totalement les mêmes champs.

Les deux directions générales de la police et de la gendarmerie inscriront dès cette année ces formations dans le champ des études de mutualisation de formation. Il s'agira d'instruire avec méthodologie ce dossier, en examinant les doctrines d'emploi, les référentiels métiers associés, et en déduire le référentiel des activités et compétences attendues de ces personnels. L'ingénierie de formation sera enfin réévaluée.

Le calendrier de réalisation de cette action est fixé à la fin du second semestre 2015.

Pilotes : DGPN, DGGN.

Action 2-4 : consolider la mission de coordination de l'OCLCTIC en liaison avec les chefs de service d'investigation, conformément au décret fondateur de l'office

Le besoin de coordination et d'échange est réel et impose une meilleure communication entre l'ensemble des acteurs de la lutte contre la cybercriminalité. Le décret n°2000-405 du 15 mai 2000, portant création de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication lui confie une mission d'animation et de coordination, au niveau national, de la mise en œuvre de la lutte contre les auteurs et complices d'infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication.

Dans le cadre de l'exercice de cette mission, il appartiendra à l'OCLCTIC de réunir une instance de coordination opérationnelle regroupant les chefs d'unités et services centraux ou assimilés spécialisés. La tenue de ces réunions aura lieu trimestriellement. L'OCLCTIC sera en charge du secrétariat permanent de cette instance de coordination opérationnelle.

La première réunion sera organisée au cours du 4ème trimestre 2014.

Pilote : OCLCTIC

Action 2-5 : créer une sous direction de lutte contre la cybercriminalité au sein de la direction centrale de la police judiciaire

L'arrêté du 29 avril 2014, modifiant l'arrêté du 5 août 2009 relatif aux missions et à l'organisation de la direction centrale de la police judiciaire, a créé au sein de la direction centrale de la police judiciaire, une sous-direction de la lutte contre la cybercriminalité, chargée d'optimiser le dispositif existant dans ce domaine.

La réalisation de cette action portera sur la mise en place des structures composant la nouvelle sous-direction : un bureau de coordination stratégique, un état major, l'actuel

OCLCTIC, une division de l'anticipation et de l'analyse.

La mise en place de la structure est actuellement en cours de réalisation.

Pilote : DCPJ

Action 2-6 : intégrer les cybermenaces dans les actions de planification et les dispositifs de gestion de crise

Les cybermenaces doivent être prises en compte dans les travaux de planification et de gestion de crise ainsi que dans les exercices nationaux pilotés par le SGDSN, auxquels participe le ministère (plans Pirates,...)

La réalisation de cette action nécessitera une étude préalable des vulnérabilités propres aux intervenants sur un théâtre de gestion de crise tant au niveau national que territorial. Cette étude portera en particulier sur les réseaux et les systèmes d'information et de communication des services opérationnels. Elle sera conduite par le SHFD avec une échéance fixée au mois de décembre 2014. Elle doit conduire à réévaluer les plans de continuité d'activité (PCA) de ces entités, dans le courant de l'année 2015.

Le plan gouvernemental PIRANET fait actuellement l'objet d'une actualisation sous la conduite du SGDSN, et devra en particulier intégrer l'organisation territoriale de l'État. Ces travaux devraient s'achever courant 2015.

De manière plus générale, la menace cyber devra être prise en compte dans l'établissement et l'actualisation des différents plans de gestion de crise par les directions du ministère. Un appui sur les spécialistes cyber pourra être recherché par les entités en charge de ces travaux de planification.

Pilote : DGSCGC et SHFD, en liaison avec les directions du ministère

Action 2-7 : alerter les ministères et les OIV des cybermenaces dont ils peuvent faire l'objet, en liaison avec l'ANSSI

Les alertes cyber en direction des ministères et des opérateurs d'importance vitale relèvent et doivent demeurer de la compétence de l'ANSSI. Toutefois, la DGSI peut intervenir en complément et selon des procédures qui devront être définies avec l'agence.

Il conviendra que la DGSI soit informée par les autres directions générales du ministère de l'intérieur de tout élément relatif aux cybermenaces dont les ministères et les OIV peuvent faire l'objet.

La mise en œuvre de cette action nécessite au préalable que soit définie la procédure d'alerte sur les cybermenaces en complément de celle de l'ANSSI. L'échéance est fixée au mois de septembre 2014.

Pilote : DGSI

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.

Action 3-1 : impulser une politique de prévention et de sensibilisation à la cybersécurité

Les entités du ministère conduisent d'ores et déjà des actions de sensibilisation à la cybersécurité. Ces initiatives mériteraient de pouvoir s'inscrire dans un cadre ministériel, qui leur offrirait un socle de communication (logo, slogan unificateur, messages clés harmonisés) et par conséquent une force et une visibilité accrues.

Dans ce cadre, un plan de communication détaillant les cibles, les supports et les messages clés sera élaboré au cours du second semestre 2014. Il trouvera une première déclinaison début 2015 avec la mise en ligne d'un site web ministériel dédié à la lutte contre les cybermenaces, à visée pédagogique et en soutien des actions de prévention conduites sur le terrain.

Cette dynamique sera par la suite entretenue par l'organisation de campagnes de communication et d'événements permettant la diffusion des bonnes pratiques et l'échange entre les acteurs, à l'instar du Forum international de la cybersécurité.

Pilote : Délégation ministérielle en liaison avec DICOM, DGGN, DGPN, DGSI, PP

Action 3-2 : contribuer au renforcement du dispositif interministériel des observatoires de la sécurité des systèmes d'information

Les observatoires zonaux de la sécurité des systèmes d'information, placés sous l'autorité conjointe de l'ANSSI et du SHFD du ministère, constituent un premier réseau de niveau interministériel pour conduire des actions de sensibilisation.

Pleinement engagé auprès des acteurs économiques, le ministère proposera une évolution de ce dispositif pour les installer en région auprès des structures régionales en charge de la politique d'intelligence économique.

Dans le même temps, il sera recherché un renforcement de leurs moyens pour leur permettre de conduire pleinement leurs actions de sensibilisation et d'alerte auprès des acteurs économiques et des collectivités territoriales.

Pilote : SHFD

Action 3-3 : renforcer les compétences en sensibilisation à la cybersécurité des réseaux « Intelligence économique » et « Référents sûreté » de la gendarmerie et de la police nationales

La sensibilisation des acteurs économiques et des administrations à la cybersécurité mériterait de s'appuyer sur les réseaux territoriaux de prévention existants et déjà en lien avec le tissu économique des territoires : principalement les réseaux « Intelligence économique » (DGSI-DGGN) et « Référents sûreté » (DGPN-DGGN).

Des modules traitant des cybermenaces pour les entreprises seront ainsi conçus et intégrés progressivement dans les formations en place au sein de la police et de la gendarmerie, entre le 4e trimestre 2014 (IE) et le 2e trimestre 2015 (référents sûreté).

Pilotes : DGGN, DGPN et DGSI en liaison avec la PP

Action 3-4 : poursuivre le développement des actions de sensibilisation à destination des acteurs économiques

Le ministère s'apprête à signer une convention de partenariat avec la CCI-France, destinée à faciliter la promotion et la diffusion de la culture de la sécurité économique auprès des CCI, des entreprises, des filières et des pôles de compétitivité dans les territoires.

Dans ce cadre, le ministère s'attachera à y intégrer la dimension des cybermenaces qui constitue désormais un enjeu stratégique en matière de sécurité économique.

Il s'agit d'encourager la réalisation d'outils de prévention au niveau ministériel, de les proposer à la direction de la CCI-France et d'encourager leur diffusion dans le cadre de la convention et des actions menées par les services du ministère sur le terrain.

Pilotes : DGGN et DGSI

Action 3-5 : encourager la diffusion du dispositif « Permis Internet » à destination des élèves du primaire

La gendarmerie nationale a lancé, sous forme d'expérimentation, l'opération « Permis Internet » en décembre 2012. Ce dispositif vise à proposer aux enseignant un programme « clé en main » de prévention sur les risques d'Internet et de présentation de bonnes pratiques d'utilisation d'Internet, avec la participation des forces de sécurité. Grâce à un partenariat avec AXA Prévention, des matériels pédagogiques de qualité sont mis à la disposition des enseignants et des élèves.

La gendarmerie nationale va généraliser en septembre 2014 sur le territoire ce dispositif. Une extension de cette opération auprès de la police nationale est en cours d'étude.

Pilote : DGGN en liaison avec DGPN et PP

Action 3-6 : participer à la consolidation du dispositif de la réserve citoyenne de cyberdéfense

Des réseaux régionaux de la réserve citoyenne de cyberdéfense ont été déployés au cours de l'année 2013-2014, 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.

Le bilan des premiers réseaux régionaux sera dressé en septembre 2014. Il doit permettre d'envisager une extension de ces dispositifs à d'autres régions. Ce développement doit également s'inscrire en soutien de ce plan de lutte contre les cybermenaces et permettre une mise en œuvre efficace des différentes actions de l'axe 3.

Cette action rejoint l'action 46 du Plan Défense Cyber.

Pilote : DGGN, en liaison avec DGSI et EMA

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.

Action 4-1 : contribuer au plan « Cybersécurité » de la Nouvelle France Industrielle

La lutte contre les cybermenaces doit s'accompagner d'une offre industrielle de qualité et qui répond aux enjeux de sécurité identifiés. Le ministère, par l'intermédiaire de ses services, est en mesure de contribuer activement à ces réflexions.

Dans le cadre de l'action 7 du plan « Cybersécurité »[1], police et gendarmerie nationales procéderont à un état des lieux des besoins en matière de fourniture de services et de produits, particulièrement dans le domaine de l'investigation (de la réparation de disque dur à l'expertise de contenu de supports numériques, en passant par les outils d'investigation sur les réseaux). Un contact avec le responsable du plan Cybersécurité sera pris avant l'été.

Le ministère participera en outre à la mise en œuvre de l'action 5[2], en cherchant tout particulièrement à favoriser le développement du cadre juridique et des solutions techniques permettant l'identification et l'authentification électronique. Cette action contribuera directement aux réflexions sur le développement d'une véritable plainte en ligne.

Pilote : ST(SI)² en liaison avec les directions du ministère

Action 4-2 : assurer la prise en compte des besoins spécifiques du ministère dans les actions de recherche et développement en matière de cybersécurité

L'Agence nationale de la recherche (ANR) et la commission européenne ont identifié la cybersécurité comme un thème de recherche à encourager.

Le ministère contribuera, dans ce cadre et d'ici mi-juin 2014, à l'élaboration du plan d'action 2015 de l'ANR relatif à la cybersécurité.

Il sera également attentif à la prise en compte de ce domaine dans les programmes de recherche européens, et encouragera le montage de consortium dans les domaines qui l'intéresse directement.

Pilote : ST(SI)² en liaison avec les directions du ministère

Action 4-3 : susciter une communauté de recherche dans les domaines relatifs à la lutte contre les cybermenaces et consolider les partenariats existants

Convaincu de l'apport de la recherche et développement dans ce domaine, le ministère cherchera à être actif en la matière et en particulier dans le cadre de partenariats.

1 Action 7 : Identifier, à partir d'une cartographie des acteurs et des segments de marché, les forces, faiblesses, trous capacitaires et orientations en matière de R&D

2 Action 5 : Émettre un support d'identité numérique, en lien avec les enjeux nationaux et européens

Un recensement des partenariats existants sera conduit d'ici septembre 2014 et pourra donner lieu à des évolutions pour mieux épouser les objectifs stratégiques du ministère.

Ces partenariats devront en particulier permettre des collaborations de services du ministère à des thèses. Un travail en lien avec le MESR, mais également d'autres acteurs capables de co-financer des thèses, devra être entrepris dès l'automne 2014.

Enfin, le ministère cherchera à susciter courant 2015 la création d'un communauté de développement open source d'outils d'investigations numériques.

Pilote : ST(SI)²

Action 4-4 : échanger avec les pôles ou centres d'excellence en cyberdéfense

L'émergence de pôles d'excellence dans ce domaine 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.

Pilote : DGSI

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.

Action 5-1 : analyser régulièrement le patrimoine informationnel du ministère et actualiser la liste des systèmes d'information jugés essentiels

Le patrimoine informationnel (fichiers, informations opérationnelles, données en lien avec les élections,...) du ministère est le support de son activité quotidienne. Son utilisation repose sur le postulat d'une information fiable, accessible au bon moment par les bonnes personnes, et protégée en confidentialité en cas de nécessité.

Sa protection doit s'appuyer sur une démarche de gestion des risques visant à optimiser l'emploi des ressources au regard de l'atteinte du juste niveau de sécurité et de protection.

Cette démarche consiste, dans un premier temps et d'ici août 2014, à conduire avec les directions métiers un dialogue permettant d'aboutir à une liste actualisée des systèmes d'information vitaux du ministère (50 à 80 systèmes d'information).

Elle s'accompagnera ensuite de la conduite d'audits de sécurité, en accord avec les directions d'application, sur quelques uns de ces systèmes d'information. Un document cadre présentant les grands principes de maîtrise des risques informationnels dans les projets informatiques sera ensuite réalisé (2d semestre 2014).

Un examen des usages, par les agents du ministère, des services gratuits en ligne (partage de fichiers, visio-conférence, organisation de rendez-vous, géolocalisation) sera mené fin 2014-début 2015, afin de mesurer plus finement la perte de maîtrise du patrimoine informationnel sensible.

Pilote : SHFD, en liaison avec les directions du ministère

Action 5-2 : renforcer la chaîne Cyberdéfense du ministère

La chaîne de Cyberdéfense consiste à mettre en œuvre les fonctions ministérielles de veille, d'alerte et de réaction face aux incidents de sécurité informatique et de cyberattaques.

Elle s'organise d'abord autour du Centre National de Gestion SSI (CNGESSI), basé à Toulouse et relevant du Haut fonctionnaire de défense, et associe l'ensemble des fonctions de cyberdéfense des différentes directions.

Afin de consolider le rôle du CNGESSI, une actualisation de l'offre de services de cette entité sera réalisée au cours du 3e trimestre 2014.

En parallèle, une identification plus formelle des « fonctions de sécurité opérationnelle » au sein des acteurs SIC du ministère sera conduite, permettant de constituer le réseau

opérationnel d'alerte et de réaction.

Les relations entre ces acteurs et le CNGESSI, sur la base de l'offre de services, se concrétiseront par la signature de contrats de cyberdéfense d'ici fin 2014.

Pilote : SHFD en liaison avec les acteurs SIC du ministère (MGMSIC, DSIC, ST(SI)², PP, ANTS)

Action 5-3 : améliorer le niveau de sensibilisation à la sécurité des systèmes d'information au sein du ministère

La future politique SSI de l'État exigera un renforcement des actions de sensibilisation et de formation des agents. Le ministère s'engage dès à présent dans la construction d'un dispositif renforcé dans ce domaine, en distinguant plusieurs profils : les utilisateurs, les autorités, les agents SIC et les responsables SSI.

La cartographie des actions de sensibilisation et des formations SSI existantes au sein du ministère, mais également au niveau interministériel, sera dressée d'ici fin septembre 2014. Elle doit permettre d'identifier les mesures prioritaires à prendre et de proposer un plan d'action fin 2014. Une sensibilisation annuelle et obligatoire des agents sera sans doute recherchée.

D'ores et déjà, les responsables des systèmes d'information métier (RSIM), récemment désignés au sein des directions, bénéficieront d'une formation sur la prise en compte des enjeux de sécurité dans la conduite des projets informatiques.

Pilote : SHFD, en liaison avec les directions du ministère

Action 5-4 : compléter le dispositif par une capacité d'audit de la sécurité des systèmes d'information

L'audit SSI vise à vérifier le niveau de sécurité réel d'un système d'information ou de communication. Il peut être mis en œuvre au titre de la prévention ou suite à une cyberattaque. Il débouche sur des actions dont la réalisation doit être vérifiée.

Les capacités actuelles disponibles restent limitées et seront illustrées par le recensement, d'ici octobre 2014, des audits conduits récemment et des ressources consacrées à cette activité au sein des différentes directions.

Une réflexion sur le besoin d'une cellule ministérielle d'audit et ses modalités d'organisation sera alors engagée et formalisée d'ici fin 2014.

Un comité ministériel des audits pilotera cette activité.

Pilote : SHFD, en liaison avec les directions du ministère

Action 5-5 : mettre à disposition des systèmes d'information protégés (réseaux, smartphones, tablettes), en particulier pour les usages mobiles

Les usages mobiles sont appelés à progresser très rapidement au sein du ministère, compte tenu de leur potentiel en termes de services et de l'évolution du marché des terminaux (les acquisitions de tablettes ont désormais dépassé celle des ordinateurs portables dans le monde).

Le ministère doit donc faire face au challenge de permettre le développement de ces usages tout en assurant la sécurité de son patrimoine informationnel. Cela doit se traduire

par une stratégie industrielle pour les acteurs SIC en charge de la fourniture des terminaux maitrisés et de la mise à disposition d'applications mobiles.

La stratégie ministérielle sera proposée d'ici septembre 2014.

Pilote : SHFD et Mission de gouvernance ministérielle des SIC, en liaison avec les acteurs SIC (DSIC et ST(SI)²) et les directions du ministère

Action 5-6 : piloter la stratégie SSI du ministère au sein du comité stratégique SSI

Les actions développées dans cet axe 5 mobilisent de nombreux acteurs du ministère, techniques et métier. Elles représentent également des enjeux forts en terme de moyens à consacrer et de décisions d'orientation dans les projets SIC.

Il est donc proposé de réactiver le « Comité stratégique SSI », présidé par le directeur de cabinet du ministre, et dont l'objet principal sera de réaligner la stratégie SSI du ministère au regard de l'évolution des menaces, des technologies, des incidents et des cyberattaques.

Ce comité pourrait se réunir une première fois fin 2014-début 2015 pour statuer sur la stratégie en matière de gestion des risques et de maîtrise du patrimoine informationnel (action 5-1), le plan d'action de sensibilisation et de formation des agents (action 5-3) et la stratégie en matière de sécurisation du nomadisme (action 5-5).

Pilote : SHFD

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.

Action 6-1 : définir une stratégie ministérielle pour le volet international de la lutte contre les cybermenaces

En raison de la multiplicité des instances au sein desquelles le ministère de l'intérieur doit siéger et de la diversité des acteurs du ministère y participant, il convient de définir une doctrine ministérielle rappelant les lignes directrices en matière de lutte contre les cybermenaces. Cette position de référence du ministère de l'intérieur aura vocation à être communiquée à ses représentants, intervenant dans les diverses enceintes de coopération, et permettra de définir les priorités d'action et de négociation au niveau ministériel, notamment dans la mise en œuvre de la stratégie cyber de l'Union européenne.

Cette doctrine de référence sera établie au cours du second semestre 2014.

Au préalable et au plus tard à l'été 2014, un recensement, au moyen d'une cartographie des instances existantes et des travaux en cours auxquels le ministère participe, devra être établi.

Pilotes : La délégation ministérielle assure la cohérence des travaux d'élaboration de la doctrine internationale dans le domaine de la lutte contre les cybermenaces avec les priorités de l'action internationale définie par le Ministre. Elle bénéficie pour cela de l'appui de la DGPN et de la DGGN, et notamment de la DCI.

DCI, notamment pour la cartographie

Action 6-2 : renforcer l'action du ministère dans les travaux internationaux et européens dans le domaine de la lutte contre les cybermenaces

Afin d'accroître la réactivité du ministère de l'intérieur et sa capacité à anticiper et influer sur les travaux internationaux et européens, une véritable stratégie doit être mise en œuvre. Cette dernière implique une coordination des positions des différents représentants du ministère dans les groupes de décision, sous l'égide de la DCI (COSI, JAI, G7, G8, etc).

La réalisation de cette action passe par la diffusion aux directions d'un tableau de bord de suivi de l'évolution des travaux sur les dossiers cyber au plan européen et international, permettant ainsi une information transversale. L'échéance fixée pour la réalisation de l'action est fixée à la fin du premier semestre 2014. La diffusion sera réalisée trimestriellement

Les réunions internationales de haut niveau (GHN, réunions bilatérales) pourront être le moyen de solliciter nos partenaires étrangers en vue d'obtenir leur soutien pour consolider les positions de la France dans le domaine de la lutte contre les cybermenaces.

Pilote : DCI en liaison avec DGGN et DGPN

Action 6-3 : développer les actions d'échange à l'international dans le domaine de la formation et de la coopération technique, et rechercher dans ces domaines les possibilités de financements externes (européens notamment) pour des actions du ministère

Pour la réalisation de cette action, le ministère de l'intérieur doit pouvoir disposer, au préalable, d'une vision claire et exhaustive de ce qui existe en matière de formation au niveau national, européen et international. Cet état des lieux permettra d'améliorer la participation des experts français à ces formations. Un catalogue des formations cyber sera ainsi établi par la DCI au cours du second semestre 2014.

Des pays cibles seront identifiés pour y conduire les actions de coopération technique, en vue de soutenir la lutte contre la cybercriminalité. Une planification des actions et des ressources mises à disposition par les directions générales de la police et de la gendarmerie nationales sera recherchée.

Des possibilités de financement seront recherchées auprès des différents programmes européens et internationaux, au cours du second semestre 2014.

Pilote : DCI en liaison avec DGGN et DGPN

Action 6-4 : mobiliser les services de sécurité intérieure (postes SSI) sur la thématique de la lutte contre les cybermenaces

L'extranéité est un élément fondamental en matière de lutte contre les cybermenaces. Il apparaît donc indispensable de sensibiliser au mieux à cette thématique les attachés de sécurité intérieure (ASI), représentant les forces de sécurité intérieure dans les ambassades. Le réseau des ASI doit être un facilitateur des relations avec l'étranger en matière cyber.

A cette fin, plusieurs moyens vont être mis en œuvre par la DCI, au premier rang desquels figure la sensibilisation à la thématique des cybermenaces à l'occasion des rassemblements des ASI (stage d'expatriation, colloques des ASI). L'échéance de réalisation est fixée au mois de septembre 2014, lors de la tenue du prochain colloque annuel des ASI.

Au delà de cette sensibilisation générale, des pays cibles seront identifiés, afin que les lettres de mission des ASI de ces pays formalisent tout l'intérêt qui doit être porté à la thématique de la lutte contre les cybermenaces. Un dossier technique de sensibilisation sera ainsi remis à l'ASI en fonction des besoins identifiés. La définition des pays cibles sera le résultat d'une concertation avec les services opérationnels des directions générales de la police et de la gendarmerie nationales.

Le développement d'actions de coopération techniques se fera à partir des pays cibles identifiés.

L'ensemble de ce dispositif sera mis en œuvre dès septembre 2014.

Pilote : DCI en liaison avec la DGPN et la DGGN