MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

STRATÉGIE MINISTÉRIELLE
De
LUTTE CONTRE LA CYBERCRIMINALITÉ

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

Depuis mon arrivée Place Beauvau, je me suis fixé une seule mission : rétablir l'ordre. Pour cela, j'ai assumé d'ouvrir de nombreux chantiers. Contre l'immigration non maitrisée, contre la criminalité organisée et le narcotrafic, contre la délinquance du quotidien.

Aussi différents soient-ils, ces fléaux ont un point commun : ils se prolongent tous dans l'espace numérique. De la pédopornographie aux trafics de drogues et d'armes en passant par les arnaques multiples et diverses, le cyberespace est devenu le nouveau terrain de chasse des délinquants et des criminels. C'est donc là que, nous aussi, nous devons aller, pour ouvrir un nouveau front dans la bataille contre l'insécurité que nous livrons.

Cette bataille, nous nous donnons les moyens de l'emporter. Nous disposons de compétences humaines enviées dans le monde entier et de capacités techniques de haut niveau. Nous avons récemment installé le commandement du ministère de l'Intérieur pour le cyberespace, le COMCYBER-MI, qui coordonne désormais l'action de nos unités spécialisées de police et de gendarmerie. Et nous venons enfin de nous doter d'une stratégie globale et cohérente pour lutter contre la cybercriminalité. Cette première stratégie, qui constituera le cadre de notre action pour les trois années à venir, s'inscrit dans une ambition plus large encore, celle de notre stratégie nationale de cybersécurité.

Dans les mois et années à venir, nous continuerons à investir les opportunités qu'ouvrent les nouvelles technologies. Nous poursuivrons le développement de nos compétences techniques, de nos partenariats et de nos coopérations européennes et internationales. Nous adapterons notre cadre juridique, pour ne rien rater des prochaines évolutions technologiques.

Parce que chacun de nos compatriotes, parce que chacune de nos entreprises et de nos institutions peut être la cible des cybercriminels, la mobilisation de l'ensemble des services du ministère de l'Intérieur doit être totale. Elle l'est d'ores et déjà, pour que nulle part, l'impunité ne puisse prospérer.

Monsieur Bruno Retailleau
Ministre d'État, ministre de l'Intérieur

Quel Français, disposant au moins d'un smartphone, n'a jamais été confronté à la cybercriminalité ? Pas même une tentative, un mail frauduleux, un sms sur une livraison imaginaire ? Quelle entreprise ou collectivité, quel établissement peut aujourd'hui se dire à l'abri du risque cybercriminel ? Sont-ils tous préparés à la paralysie de leur réseau informatique et/ou au pillage de leurs données ?

Le cyberespace est le nouveau terrain de jeu des criminels : la cybercriminalité affiche depuis des années une forte hausse continue (+40% de faits constatés entre 2019 et 2023). Les cybercriminels se diversifient et se professionnalisent ; les organisations criminelles se développent et se structurent. Les outils sont de plus en plus performants, le délinquant s'améliore et se spécialise, industrialise ses process, mettant lui aussi à profit les nouvelles technologies. Ainsi, l'intelligence artificielle permet des atteintes plus nombreuses et plus abouties … sur une surface d'attaque qui ne cesse de se développer, à mesure que la société se numérise.

« La cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet. »[1].

Deux grandes catégories d'infractions se dégagent :

- les infractions spécifiques aux Technologies de l'Information et de la Communication (TIC), aussi appelées **infractions cyberdépendantes** (atteintes aux systèmes de traitement automatisé de données, vol et revente de données personnelles, violation des correspondances électroniques, infractions relatives à la cryptologie, aux cartes bancaires, etc.) ;
- les infractions dont la commission est liée ou facilitée par l'utilisation des TIC, ou **infractions cyberfacilitées** (escroquerie, extorsion, harcèlement, usurpation d'identité, haine en ligne, pédopornographie, atteinte à la vie privée, etc.).

La cybercriminalité regroupe donc une large gamme d'infractions (dont beaucoup existaient avant les TIC), et son périmètre ne cesse d'évoluer, à mesure que de nouvelles technologies ou de nouveaux modes d'action de l'adversaire apparaissent.

La cybercriminalité est une forme de criminalité souvent très fortement imbriquée avec la criminalité organisée « traditionnelle », qui s'y intéresse comme à un nouveau marché, très lucratif, une nouvelle opportunité de diversification, ou de blanchiment.

Par nature transfrontalière, la cybercriminalité subit aussi fortement l'influence, dans son intensité comme dans le choix de ses cibles, de l'actualité internationale et de la situation géopolitique. Les frontières entre les groupes cybercriminels, les hacktivistes de tous bords, et certains intérêts étatiques deviennent alors plus floues. La cybercriminalité est devenue une arme d'emploi, autant dans le cadre d'un conflit ouvert entre États, que d'actions hybrides, sous-traitées auprès de groupes criminels spécialisés et plus ou moins affiliés, tels des cybermercenaires.

La lutte contre la cybercriminalité doit répondre à ces menaces, protéiformes et évolutives, dans un espace encore peu réglementé, avec des moyens comptés, dans un contexte concurrentiel et compétitif, ponctué d'avancées technologiques permanentes.

1. Définition proposée par le rapport « Protéger les Internautes », rédigé par un groupe de travail interministériel présidé par le Procureur général Marc Robert, 2014.

Une stratégie de lutte contre la cybercriminalité doit intégrer les enjeux qui la contraignent :

- enjeux de **compétence** et d'**attractivité**, dans un contexte très concurrentiel où la ressource est comptée ;
- enjeux **technologiques**, autant pour le développement d'outils que pour la prise en compte des avancées voire des ruptures technologiques, objets d'une forte compétition internationale ;
- enjeux d'**anticipation** et de **connaissance** d'une menace évolutive et d'adversaires polymorphes, aux objectifs variés ;
- enjeux de **partenariats** et de **coopération**, avec le privé, les pays partenaires, les organisations internationales ;
- enjeux **normatifs**, avec l'absolue nécessité de créer ou faire évoluer des textes nationaux et internationaux protégeant la population et les entreprises, tout en renforçant l'efficacité de l'action des enquêteurs.

Le commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) a reçu pour mission d'élaborer la stratégie ministérielle de lutte contre la cybercriminalité.

Cette stratégie a été construite avec la participation active de l'ensemble des directions et services spécialisés concernés au sein du ministère de l'Intérieur : COMCYBER-MI, OFAC, UNCyber, BL2C et PP, DGSI, DTNUM, DEPSA, DAEI, SHFD.

La stratégie ministérielle décline, pour ce qui relève de la lutte contre la cybercriminalité, la stratégie nationale de cybersécurité, et s'inscrit donc en totale cohérence avec son contenu.

Elle a vocation à être déclinée en plans d'actions par les directions (notamment DGGN, DGPN, PP), et mise en œuvre par l'ensemble des acteurs du ministère de l'Intérieur.

Cette stratégie exclut le périmètre des domaines réservés de la DGSI.

La présente stratégie ministérielle de lutte contre la cybercriminalité est structurée en 4 piliers, déclinés en 12 axes stratégiques, eux-mêmes détaillés en 84 actions structurantes.

01

PILIER 1 :

ANTICIPATION ET RÉSILIENCE

PILIER 1 :

ANTICIPATION ET RÉSILIENCE

01

1 Axe stratégique anticipation et état de la menace

La cybercriminalité est en croissance rapide et en évolution permanente, dans ses moyens comme dans son organisation. La connaissance en amont de la menace, de ses modes d'action, de ses structures, est indispensable à la neutralisation judiciaire des groupes criminels. Il s'agit donc de recueillir au plus tôt le renseignement d'intérêt cyber, de l'analyser pour structurer l'adversaire, d'en organiser le partage et la diffusion, en particulier auprès des services d'enquête, tout en gardant un temps d'avance par la veille prospective et le développement d'outils.

Détection

- Détecter les cyberattaques et les revendications des groupes cybercriminels ; recueillir, traiter et exploiter les données techniques et non techniques ; alerter les partenaires institutionnels et informer les victimes, en lien avec l'ANSSI.
- Réaliser ces missions à l'occasion de grands événements, en relation avec les structures interministérielles.
- Identifier les nouveaux usages/mésusages du numérique, déceler les nouveaux outils développés ou utilisés par les cybercriminels (notamment les applications et solutions de téléphonie chiffrée).

État de la menace

- Améliorer la connaissance des groupes cybercriminels organisés et de leurs modes d'action, déceler et identifier les groupes sur lesquels une action judiciaire est souhaitable et possible, en y associant l'autorité judiciaire.
- Organiser le partage de la connaissance de la menace entre les services du MI ; organiser la diffusion des informations issues de l'analyse de cette menace au sein du MI, auprès des partenaires, et à destination du grand public.
- Rédiger et diffuser chaque année un rapport d'état de la menace cyber.
- Développer des partenariats avec les acteurs privés ou publics d'intérêt en matière de partage de renseignement d'intérêt cyber.
- Produire des analyses croisées sur l'état de la menace sur des thématiques d'intérêt pour les services partenaires.
- Enrichir et recouper l'état de la menace établi au niveau national avec les productions d'Europol (notamment les rapports SOCTA et IOCTA), d'Interpol, du Conseil de l'Europe, et de tout autre cadre de discussion multilatéral ; y contribuer ; utiliser ces vecteurs pour promouvoir notre modèle de connaissance et d'anticipation du risque cyber.

Prospective et développement des outils

- Animer et renforcer une veille technologique cyber MI.
- Veiller les productions et projets de l'Union européenne.
- Développer des outils dédiés au renseignement d'intérêt cyber et aux recherches en sources ouvertes : capacité à récupérer, traiter et analyser les données liées à la cybercriminalité ; montée en puissance de l'outillage cyber ministériel d'analyse de la menace.

2 Axe stratégique gestion de crise et résilience

La cybercriminalité peut engendrer des crises d'ampleur, volontairement ou non, par son action directe ou par ses conséquences. La gestion d'une crise cyber est certes un sujet de cybersécurité, mais elle emporte également une part de lutte contre la cybercriminalité lorsque la crise est d'origine criminelle. Il s'agit donc de participer en amont de la crise, en s'appuyant sur les préfets de département dans les territoires, à la préparation, à la formation, à l'amélioration de la résilience, de la connaissance de la menace et de ses conséquences concrètes, tout en intégrant nativement la composante judiciaire. Il s'agit ensuite de tirer les enseignements des crises cyber par un retour d'expérience (RETEX) et de les partager.

Doctrine de gestion de crise

- Participer à la préparation et à la conduite de gestion de crise des directions et services du MI, notamment à l'occasion d'exercices inter-services de gestion de crises d'origine cybercriminelle, en intégrant en particulier des composantes renseignement, conduite des investigations voire renfort capacitaire.
- Appuyer les préfets de départements et de zones dans la préparation à la gestion de crises cyber sur leurs territoires.

Retex

- Contribuer aux RETEX de gestion de crise cyber à l'échelle ministérielle afin de renforcer les capacités de résilience de la nation.
- Accompagner la diffusion du RETEX des victimes sur des cyberattaques d'origine criminelle d'ampleur ou des phénomènes émergents dans le but d'informer les entreprises, collectivités et établissements, voire le grand public.

Favorisation la résilience de nos partenaires

- Mener des actions de prévention et de sensibilisation au profit des services déconcentrés de l'État sur la gestion d'une crise cyber.

02

PILIER 2 :

OPÉRATIONNEL

PILIER 2 :

OPÉRATIONNEL

02

1 Axe stratégique contact numérique

La réponse opérationnelle du Ministère pour lutter contre la cybercriminalité débute par le développement de contacts avec les acteurs, plateformes du numérique et grand public. Il s'agit d'abord d'informer la population, victime potentielle, des outils existants et mis à sa disposition par l'État pour l'aider dans la connaissance ou le traitement des difficultés ou infractions cyber auxquelles elle peut être confrontée. Il s'agit ensuite de mettre en place des collaborations et des modes d'action innovants, facilitant le contact avec les usagers de plateformes numériques d'intérêt.

Promouvoir les outils à destination du grand public

Ma Sécurité Application Grand Public

- Facilitateur de contact, de signalement et canal privilégié de diffusion des fiches conseil prévention cyber du MI à destination des citoyens.

MonAideCyber INNOVATION ANSSI

- Outil de diagnostic développé par l'ANSSI.

17 CYBER

- Outil de diagnostic et d'accompagnement des victimes de cybermalveillance.

PHAROS

Pharos
(contenus illicites)

PERCEV@L

Perceval
(fraudes à la carte bancaire)

POLICE JUDICIAIRE
THESEE

Thésée
(escroqueries)

- Plateformes de signalement et de plainte en ligne.

Renforcer la collaboration avec les acteurs des plateformes numériques

- Développer des partenariats avec les plateformes d'intérêt (jeux en ligne, ventes entre particuliers, metavers, etc.), et des dispositifs juridiques et techniques, afin de faciliter la mise en place de points de contacts privilégiés avec les FSI (notamment via leurs outils dédiés) dans les espaces publics de l'Internet.

2 Axe stratégique prévention

Les actions de prévention menées par les directions et services du MI sont nombreuses et variées. Il s'agit de les coordonner, les prioriser, aider à leur construction et à leur diffusion, tout en développant des partenariats spécifiques permettant de mieux prendre en compte et accompagner les victimes de cybercriminalité.

Articuler et orienter les actions de prévention

- Cartographier l'ensemble des actions de prévention cyber menées par les acteurs du MI, pour favoriser lisibilité, coordination et complémentarité.
- Constituer une base documentaire de fiches conseils destinées aux usagers, co-construites et mises à disposition de tous les cyber-préventionnistes du MI.
- Dynamiser les actions de prévention cyber dans les territoires, en s'appuyant sur les objectifs fixés par la PPG Cyber et le rôle de coordinateur confié aux préfets.
- Développer des partenariats et une offre de prévention cyber adaptée par secteurs d'activités et publics cibles en s'appuyant sur les correspondants des autres institutions et acteurs clés de l'écosystème visé.
- Mieux prendre en compte les publics les plus vulnérables et promouvoir des dispositifs pour permettre à l'ensemble des FSI de disposer localement d'un support de prévention adapté aux évolutions des usages.
- Participer à des actions de prévention à forte visibilité à l'occasion du cybermois, en lien avec ACYMA.

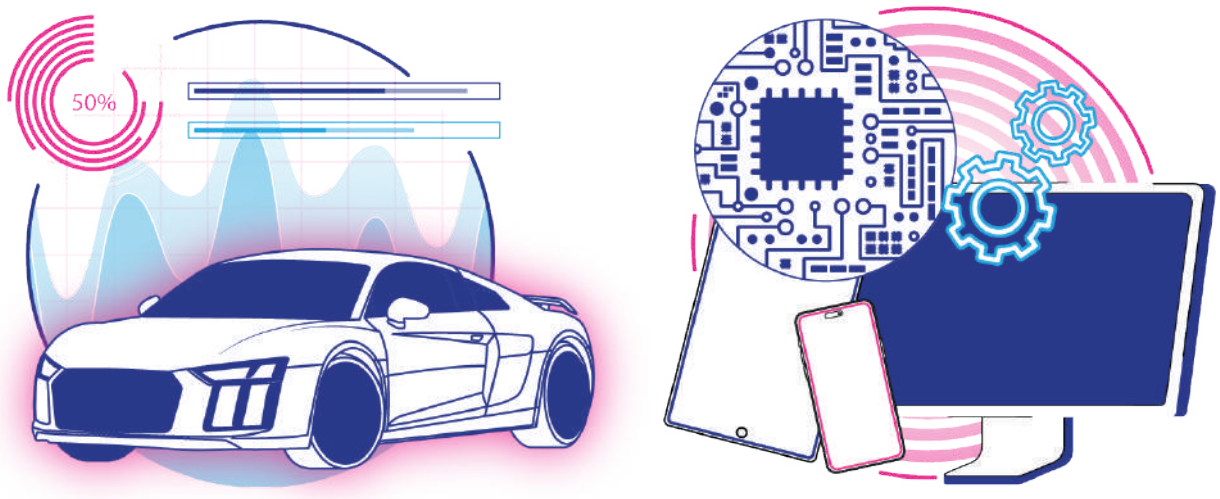
Accompagner les victimes

- Participer aux études sur le parcours victime cyber, pour orienter les actions des FSI vers une meilleure prise en compte et améliorer la perception de la qualité du service public dans ce domaine.
- Engager des partenariats d'intérêt avec les associations d'aide aux victimes cyber pour améliorer la visibilité des actions du MI et l'orientation des usagers.

3 Axe stratégique enquêtes

La conduite d'investigations menant à la répression des activités des groupes cybercriminels est l'objectif opérationnel vers lequel convergent toutes les actions de la lutte contre la cybercriminalité. Ces investigations sont conduites par les unités des forces de sécurité intérieures et plus particulièrement par des services spécialisés (OFAC, UNCyber, BL2C) s'appuyant sur un maillage territorial d'antennes, l'animation et la coordination opérationnelle nationale relevant de l'OFAC. Il s'agit de fluidifier les échanges entre ces unités et avec d'autres services d'enquête, la cybercriminalité étant fortement imbriquée avec d'autres formes de criminalité organisée.

- Renforcer la connaissance mutuelle et la coordination entre les unités spécialisées.
- Contribuer, avec les offices centraux chefs de file de leur périmètre, à la lutte contre les trafics de produits illicites en ligne, organisés via le Darkweb, les messageries chiffrées et les réseaux sociaux.
- Intensifier la lutte contre le blanchiment en ligne en renforçant la connaissance de ses mécanismes et de l'usage des crypto-actifs, afin d'optimiser le traçage et les saisies.
- Améliorer la détection des atteintes aux personnes, notamment de la pédocriminalité et du cyberharcèlement, par le développement de partenariats avec les modérateurs des grands sites français et internationaux.
- Veiller à une meilleure exploitation des traces numériques dans les contentieux de droit commun et de la criminalité organisée en s'appuyant sur le maillage territorial des services spécialisés en charge de la lutte contre la cybercriminalité.



4 Axe stratégique expertises et appuis spécialisés

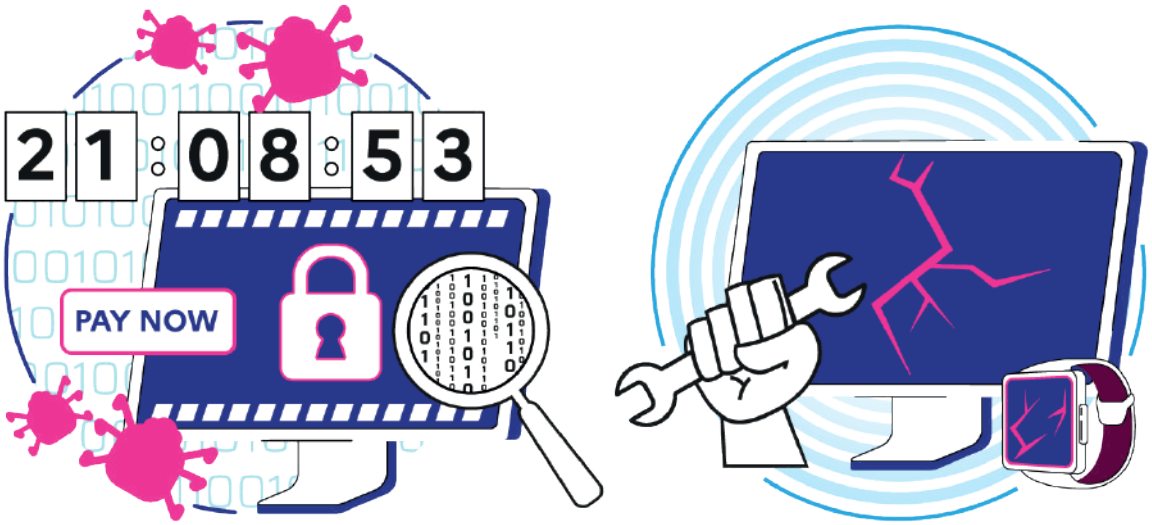
La conduite d'investigations cyber nécessite de disposer d'expertises et de compétences rares, détenues pour partie au sein des unités spécialisées des forces. Parmi ces compétences rares, le COMCYBER-MI met en œuvre des compétences de haut niveau notamment dans les domaines des crypto-actifs, du traitement de données de masse et de l'extraction de données, au profit de l'ensemble des services d'enquête du Ministère. Le développement de capacités mettant à profit la puissance de l'intelligence artificielle (IA), qui constitue autant une menace qu'une opportunité, est aujourd'hui un facteur de réussite incontournable pour la lutte contre la cybercriminalité.

Compétences de haut niveau

- Développer et maintenir à un haut niveau d'expertise les appuis spécialisés du COMCYBER-MI à destination de l'ensemble des services d'enquête du MI.
- Assurer une veille technologique permettant d'identifier les besoins de nouvelles compétences rares.
- Appuyer par l'investigation technique et le management de la donnée les priorités du MI dans la lutte contre la criminalité.

Intelligence artificielle appliquée au cyber

- Analyser les risques actuels et futurs et identifier les besoins métiers afin d'orienter les projets.
- Améliorer l'efficacité des outils et le pilotage des projets.
- Monter en compétence en assurant des formations et en développant des partenariats avec des entreprises et écoles spécialisées.
- Consolider les outils CyberIA sur les plans éthique et juridique.



03

PILIER 3 :

PARTENARIATS, COOPÉRATIONS ET PILOTAGE

PILIER 3 :

PARTENARIATS, COOPÉRATIONS ET PILOTAGE

03

1 Axe stratégique partenariats

De nombreux partenaires ont développé des compétences intéressantes ou peuvent être intéressés par des compétences développées au sein du MI. Dans une optique de convergence des efforts dans la lutte contre la cybercriminalité, le développement de partenariats d'intérêt avec certains acteurs privés, avec des structures de formation notamment européennes, et avec d'autres acteurs institutionnels, permet de gagner en efficacité et de s'appuyer mutuellement.

Coopération écosystème privé

- Intensifier les partenariats avec les acteurs privés en développant les synergies.
- Mobiliser et animer la présence du MI au profit des associations partenaires.

Coopération écosystème formation cyber

- Ancrer la contribution européenne du MI en matière de conceptions pédagogiques en investigation numérique par une participation active au sein de l'European Cybercrime Training and Education Group (ECTEG).
- Accueillir au CNF-Cyber du MI des forces de l'ordre et des magistrats étrangers en formation en France ou concourir à leur formation par des actions de coopération bilatérale ou multilatérale.

Formation à la lutte contre la cybercriminalité des partenaires institutionnels français

- Élargir les publics accueillis au CNF-Cyber aux fins de formations.

2 Axe stratégique coopération internationale

La cybercriminalité est par nature transfrontalière. La lutte contre la cybercriminalité ne se conçoit donc que dans un cadre international, ce qui nécessite le développement de coopérations, multilatérales et bilatérales, très en amont des phases opérationnelles. Les dispositifs européens, doivent être mis à profit et valorisés. Ils sont complétés par des échanges de renseignements, de compétences, de formations, de recherches, et in fine opérationnels. La coopération internationale structurelle met en place des conditions permettant ou facilitant la coopération internationale opérationnelle ; elle s'inscrit donc à la fois dans une logique de réponse aux besoins de la lutte contre la cybercriminalité, et de cohérence avec les priorités de la diplomatie française.

Coopération internationale multilatérale

- Investir et mettre à profit les dispositifs éprouvés de l'UE pour mutualiser les efforts entre partenaires, y compris ceux n'étant pas membres de l'UE.
- Faire la promotion systématique des ressources européennes au sein des différents cadres de coopération multilatérale.
- Participer à l'élaboration des normes européennes et internationales.
- Prioriser les partenariats internationaux pour renforcer la coopération opérationnelle et les capacités des pays ciblés en matière de lutte contre la cybercriminalité.
- Renforcer la présence du MI auprès des instances stratégiques européennes et internationales.
- Développer les échanges avec les FSI des pays européens sur l'état de la menace.
- Développer les échanges opérationnels dans les différentes instances européennes et internationales.
- Piloter des programmes européens de recherche et développement sur des volets d'action prioritaires.

Coopération internationale bilatérale

- Accompagner la mise en place d'un réseau d'officiers de liaison Cybercriminalité (ODL Cyber) du MI.
- Contribuer au développement des dialogues bilatéraux de la France, en lien avec le MEAE, en matière de cybercriminalité. Faire émerger des canaux de coopération forte avec les pays identifiés comme stratégiques.

3 Axe stratégique pilotage et performance

Plusieurs leviers concourent au pilotage et à la performance de la stratégie ministérielle. Il s'agira tout d'abord de définir des indicateurs et agrégats statistiques partagés, constituant un tableau de bord, permettant d'évaluer l'avancement et l'efficacité de la stratégie et de ses déclinaisons. La définition de besoins communs aux fins de rationalisation et d'économie, et le fait de porter une stratégie juridique permettant d'anticiper ou de répondre aux besoins opérationnels, constituent aussi des facteurs d'efficacité majeurs.

Évaluation et pilotage de la performance

- Construire un tableau de bord sur la base d'agrégats cyber permettant un pilotage de la performance optimisé avec des indicateurs communs au sein du MI.
- Mesurer régulièrement la qualité du service public rendu dans le domaine de la lutte contre la cybercriminalité ; conduire des études sur la victimologie cyber française (associations, chercheurs, etc.).
- Assurer le suivi de la déclinaison de la stratégie par les directions, avec la mise en place d'une comitologie semestrielle afin de suivre l'avancée de la réalisation des objectifs fixés et les freins à lever.

Investissements

- Définir les moyens capacitaires, et envisager ensuite le financement du développement et/ou de l'acquisition des solutions utiles.

Intelligence juridique cyber : contribuer aux évolutions du cadre juridique national et international

- Anticiper les besoins du MI en matière d'évolutions législatives et réglementaires.
- Participer, dans un cadre interministériel, à l'élaboration de textes nationaux et internationaux conformes aux besoins et à la stratégie du MI.
- Participer à la création d'un encadrement juridique français pour les traitements de données issus de recherches en sources ouvertes.

04

PILIER 4 :

COMPÉTENCE ET ATTRACTIVITÉ

PILIER 4 :

COMPÉTENCE ET ATTRACTIVITÉ

04

1 Axe stratégique attractivité

Dans un contexte de forte compétitivité dans le recrutement d'une ressource qualifiée rare, il s'agit de susciter des vocations au plus tôt, y compris durant les scolarités, de déceler les talents internes et externes afin de constituer un vivier au profit des services du Ministère, tout en étant attractif sur le plan salarial, pour le recrutement d'agents qualifiés comme pour la valorisation des formations qualifiantes en interne.

Susciter des vocations

- Développer des campagnes de communication et de recrutement ciblées sur la filière au sein du MI ; développer une gamme d'outils à cette fin (exercices gamifiés en forensics, live forensics dans des scénarios réalistes ; mobiliser les auteurs et scénaristes de fictions pour faire découvrir les métiers cyber du MI).
- Conduire annuellement, à l'occasion du cybermois par exemple, une action commune de communication en faveur du recrutement des métiers cyber du MI ; développer une Journée nationale des métiers du cyber au MI s'appuyant sur une communication innovante, ouverte au public.
- Aller au contact des écoles du numérique, faire connaître les métiers proposés au sein du MI, proposer des stages ciblés et des partenariats facilitant le recrutement.
- Développer un dispositif d'accompagnement financier au profit d'étudiants cyber méritants et contractualiser leur engagement futur au profit du MI.

Détecter les talents internes et externes

- Organiser annuellement un challenge CTF (Capture The Flag) interne aux agents du MI de tous statuts pour détecter les talents.
- Organiser annuellement un challenge externe ouvert au public sur une thématique d'intérêt (OSINT, IA, etc.).
- Accueillir des stagiaires et apprentis sélectionnés notamment au regard des compétences à acquérir et des projets prioritaires à conduire.

2 Axe stratégique montée en compétence des agents

La connaissance de l'environnement cyber, des outils et dispositifs existants, ainsi que la maîtrise de savoir-faire spécifiques sont indispensables à l'efficacité des FSI dans la lutte contre la cybercriminalité et nécessitent des actions de formation et d'information, pour les généralistes comme pour les spécialistes.

- Densifier la formation initiale de tous les policiers et gendarmes en cyber-investigations et cyber-prévention, s'appuyer sur le CNF-Cyber en lien avec l'Académie PN, le CEGN et les autres centres de formations du MI.
- Élaborer, actualiser et diffuser des contenus de formation destinés aux services de la gendarmerie et de la police nationales en matière de prévention et de lutte contre la cybercriminalité, en s'appuyant sur le CNF-Cyber, en lien avec les centres de formation des forces de sécurité intérieure et les structures de formation des directions du ministère.
- Assurer une meilleure visibilité des offres de formation interne ouvertes aux agents du MI.
- Former aux techniques numériques d'enquête au-delà des seules unités spécialisées en cybercriminalité (enquête sous pseudonyme, extraction et analyse de données téléphoniques, détection/saisie de crypto-actifs, etc).
- Améliorer l'identification des faits cyber par les FSI, notamment les gendarmes et policiers chargés d'accueil, en lien avec l'académie PN, le CEGN et le CNF-Cyber (parcours victime).
- Améliorer la connaissance des dispositifs existants (17Cyber, PHAROS, THESEE, Perceval, plainte en ligne, etc.) au profit des gendarmes et des policiers via différents supports (vidéos de présentations, fiches récapitulatives, fiches de criblage, etc.).

3 Axe stratégique fidélisation et parcours de carrière

La ressource spécialisée, une fois recrutée et/ou formée, constitue le principal facteur de réussite dans la lutte contre la cybercriminalité. Il s'agit donc d'identifier au mieux les besoins du Ministère afin de disposer des compétences adaptées, de bâtir des parcours de carrière permettant de combiner l'évolution des agents au sein du Ministère avec les besoins des services, dans une logique de décloisonnement et de partage. Une étude des situations ayant conduit certains spécialistes au départ permettra de disposer d'éléments pour envisager les réponses à y apporter dans le cadre des politiques RH.

- Mieux identifier les besoins en compétence cyber au sein du MI en lien avec la DRH MI, et les DRH des FSI.
- Développer l'agilité des process de recrutement, et veiller à optimiser l'utilisation des grilles indiciaires existantes pour les contractuels qualifiés, afin de disposer d'une réactivité compatible avec la tension du marché.
- Favoriser une progression salariale valorisant l'expérience acquise ainsi que les formations qualifiantes au sein des FSI.
- Favoriser des parcours de carrières croisés au sein des directions et services cyber et numériques du MI, en prévoyant, dans une logique de fidélisation et de progression, la possibilité de mobilités « cyber » ou numérique entre services et directions du MI (recrutements et stages croisés, mises à disposition, détachements ...) pour favoriser le décloisonnement, la montée en compétence rapide, ainsi qu'un partage opérationnel et technique entre les services du MI.
- Mener une réflexion sur les parcours de carrière cyber au sein du MI pour permettre de mieux appréhender les mécanismes sociologiques conduisant aux départs des agents et experts et accompagner les politiques RH au MI.

Cette première stratégie ministérielle de lutte contre la cybercriminalité est établie pour une durée de 3 ans.

Elle est rédigée au regard des technologies, modes d'action et structures existantes lors de son écriture, elle est donc susceptible de modification ou de refonte en cas d'évolutions structurantes.

Elle est en particulier soumise aux conséquences d'évolutions techniques majeures, voire de l'apparition de technologies de ruptures modifiant profondément les notions de cyberespace ou de cybercriminalité.

Il pourrait s'agir par exemple d'avancées majeures de l'intelligence artificielle, dont l'évolution rapide pourrait avoir des conséquences imprévues, ou de l'avènement de l'informatique quantique, dont la puissance annoncée ébranlerait les systèmes de chiffrement sur lesquels repose aujourd'hui une bonne partie de la sécurité des communications, des systèmes de données, ou des transactions.

Pour le suivi de la stratégie, un comité de pilotage (COPIL), constitué des représentants des services contributeurs, se rassemblera, sous la présidence du COMCYBER-MI, autant que nécessaire et a minima deux fois par an.

Ce COPIL sera chargé du suivi de l'avancement et de l'efficacité des actions de la stratégie ministérielle et de ses déclinaisons.

Il définira pour cela les indicateurs et agrégats statistiques partagés, dont il assurera le suivi en lien avec le SSMI.

Le COPIL préparera la tenue d'un comité stratégique (COSTRAT) annuel, qui sera présidé par le directeur de cabinet du ministre de l'Intérieur.

Capture The Flag (CTF) :
Compétition de cybersécurité dans laquelle les participants s'affrontent pour résoudre des énigmes et des problèmes de sécurité informatique.

Crypto-actif :
Actif numérique utilisant notamment la cryptographie et la technologie blockchain pour sécuriser et vérifier les transactions.

Cryptologie :
Étude, science (conception, analyse) des messages secrets, des cryptogrammes.

Cyberespace :
Espace de communication immatériel et sans frontière constitué par l'interconnexion d'équipements de traitement automatisé de données numériques.

Cyberharcèlement :
Acte ou propos intentionnel d'un individu ou d'un groupe d'individus au moyen de formes de communications électroniques, de façon répétée à l'encontre d'une victime, occasionnant une dégradation des conditions de vie de celle-ci.

Darkweb :
Partie cachée du web accessible avec des logiciels spécifiques. De nombreuses activités illicites y sont disponibles, notamment la mise en vente de logiciels malveillants ou l'échange de contenus illégaux.

Données à caractère personnel :
Éléments d'identification se rapportant à une personne physique identifiée ou identifiable (nom, prénom, date de naissance, numéro de sécurité sociale, etc.).

Forensics :
Consiste à investiguer un système d'information après une cyberattaque. Les analystes collectent l'ensemble des données brutes (fichiers effacés, sauvegardes, journaux des systèmes, etc.), puis les étudient pour établir leur rapport d'analyse.

Hacktiviste :
Pirate informatique qui agit par activisme.

Metavers :
Un métavers est un monde virtuel. Le terme est régulièrement utilisé pour décrire une version futuriste d'Internet où des espaces virtuels, persistants et partagés, sont accessibles via interaction 3D ou 2D en visioconférence.

OSINT :
L'OSINT ou « Open Source Intelligence » signifie en français « Renseignement de Source Ouverte ». Il s'agit d'une information accessible à tous et non classifiée.

PPG :
Politique prioritaire gouvernementale.

Système d'information :
Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

Système de traitement automatisé des données (STAD) :
Ensemble d'éléments physiques et applicatifs utilisés pour le traitement de données (réseaux, supports informatiques, etc.).

17 CYBER : Service public d'assistance en ligne destiné aux particuliers, entreprises, associations et collectivités victimes de cybermalveillance

ACADÉMIE PN: Académie de la Police Nationale

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

BL2C : Brigade de Lutte contre la Cybercriminalité de la Préfecture de Police de Paris

COMCYBER-MI : Commandement du ministère de l'Intérieur dans le cyberespace

CEGN : Commandement des Écoles de la Gendarmerie Nationale

CNF-Cyber : Centre National de Formation Cyber

DAEI : Direction des Affaires Européennes et Internationales

DEPSA : Direction des Entreprises et Partenariats de Sécurité et des Armes

DGGN : Direction Générale de la Gendarmerie Nationale

DGPN : Direction Générale de la Police Nationale

DGSI : Direction Générale de la Sécurité Intérieure

DTNUM : Direction de la Transformation Numérique

EUROPOL : Agence de l'Union Européenne pour la coopération des services répressifs

FSI : Forces de Sécurité Intérieure

GIP ACYMA : Groupement d'Intérêt Public Action contre la Cybermalveillance

INTERPOL : Organisation internationale de police criminelle

MEAE : Ministère de l'Europe et des Affaires Étrangères

MI : Ministère de l'Intérieur

OFAC : Office Anti-Cybercriminalité de la Police Nationale

PERCEVAL : Plateforme Électronique de Recueil de Coordonnées bancaires et de leurs conditions d'Emploi rapportées par les Victimes d'Achats frauduleux en Ligne. Plateforme de signalement suite à une fraude à la carte bancaire

PHAROS : Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements. Plateforme gouvernementale de signalement des contenus et comportements illicites en ligne

PP : Préfecture de Police de Paris

RAPPORT SOCTA : Serious and Organised Crime Threat Assessment - Document prospectif qui évalue les changements dans le contexte de la criminalité grave et organisée

RAPPORTS IOCTA : Internet Organised Crime Threat Assessment - Évaluation unique axée sur les services de détection et de répression des nouvelles menaces et des principaux faits nouveaux dans le domaine de la cybercriminalité au cours de l'année écoulée

SHFD : Service du Haut Fonctionnaire de Défense

THÉSÉE : Traitement Harmonisé des Enquêtes et Signalements pour les E-Escroqueries. Plateforme de signalement et de dépôt de plainte pour les escroqueries sur internet

UE : Union Européenne

UNCYBER : Unité Nationale Cyber de la Gendarmerie Nationale

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

Commandement du ministère
de l'Intérieur dans le cyberespace