INTERPOL

Guide sur la stratégie nationale de lutte contre la cybercriminalité

JAIF
Japan-ASEAN Cooperation

Avril 2021

Avant-propos

À mesure que les technologies de l'information s'ancrent dans notre société, la cybercriminalité devient une menace commune à l'échelle mondiale. Avec plus de 4,5 milliards de personnes connectées, la moitié de population mondiale est susceptible d'être victime de la cybercriminalité.

La pandémie de COVID-19 a accéléré la fusion des mondes physique et virtuel, et accru la dépendance à la connectivité pour la plupart de nos activités quotidiennes, tant professionnelles que personnelles.

L'environnement cybercriminel de plus en plus complexe et les difficultés inhérentes aux enquêtes transnationales exercent une pression supplémentaire sur les services chargés de l'application de la loi du monde entier.

Si le secteur privé a su se transformer, le secteur public reste confronté à des difficultés liées à un manque d'informations, de stratégies, de ressources, d'infrastructures et de partenariats.

Il est essentiel que les services chargés de l'application de la loi reconnaissent que les mesures, pratiques et politiques actuelles ne suffisent probablement pas pour lutter contre la cybercriminalité, qui ne cesse d'évoluer, et déterminent les mesures à prendre afin de combler ces lacunes.

Le secteur public doit s'améliorer en termes de préparation, d'efficacité et d'orientation en vue d'atteindre une cyber-résilience collective. La cybersécurité est à la fois la responsabilité de tous et un objectif commun que nous devons sans cesse œuvrer à réaliser.

La plateforme mondiale d'INTERPOL prend tout son sens lorsque des techniques et tactiques sont répliquées pour perpétrer des attaques dans différents secteurs à l'échelle mondiale, car c'est là qu'elle aide les enquêteurs à échanger des informations de manière sécurisée et à intervenir rapidement.

Dans le cadre des initiatives visant à fournir un appui à nos pays membres, j'ai l'honneur de vous présenter le **Guide sur la stratégie nationale de lutte contre la cybercriminalité d'INTERPOL**.

Le monde est de plus en plus connecté et INTERPOL continuera à jouer un rôle central et unique au sein de la communauté mondiale des services chargés de l'application de la loi en matière de lutte contre la cybercriminalité.

Jürgen Stock

Secrétaire général d'INTERPOL

Introduction

Nous sommes entrés dans une ère où les mondes physique et virtuel fusionnent, et où la transformation numérique accroît notre dépendance à la connectivité.

Les services chargés de l'application de la loi du monde entier ont été les premiers témoins des tendances criminelles uniques nées de la pandémie de COVID-19, notamment la diversification et l'intensification de l'impact de la cybercriminalité. Ce phénomène nous a amenés à repenser notre stratégie mondiale et à adapter notre réseau international de services chargés de l'application de la loi.

Un rapport d'INTERPOL publié en août 2020, qui étudiait l'impact de la pandémie de coronavirus sur le contexte mondial des cybermenaces, a déterminé que les stratégies nationales de lutte contre la cybercriminalité permettaient d'accroître la résilience des infrastructures et services nationaux, de combattre efficacement les cybermenaces et de protéger les populations des cyberattaques pendant la pandémie et au-delà.

Dans le cadre de sa mission de réduction de l'incidence de la cybercriminalité et de protection des populations pour un monde plus sûr, la Direction de la Cybercriminalité d'INTERPOL fournit des capacités policières en matière de lutte contre la cybercriminalité. L'un de ses principaux objectifs est de renforcer et d'améliorer les capacités des pays membres afin qu'ils puissent prévenir et détecter les cyber-infractions et enquêter sur celles-ci.

Ce Guide constitue une ressource précieuse pour les pays membres d'INTERPOL dans le cadre de l'élaboration ou de l'actualisation de leur stratégie nationale de lutte contre la cybercriminalité. Il fournit des informations sur leur stratégie actuelle en la matière et des solutions pour élaborer une stratégie plus robuste ainsi qu'un programme visant à surmonter les difficultés qui les empêchent d'apporter une réponse plus efficace.

Je recommande à nos pays membres d'utiliser ce Guide en vue d'accroître leur résilience et de gagner en agilité dans ce monde résolument numérique, et ainsi de lutter efficacement contre la cybercriminalité.

Craig JONES

Directeur de la Cybercriminalité

Table des matières

Acronymes

ASEAN – Association des nations de l'Asie du Sud-Est

ACCDP – Projet de renforcement des capacités de lutte contre la cybercriminalité de l'ASEAN

CERT – Équipe d'intervention informatique d'urgence

CSIRT – Cellule d'intervention en cas d'atteinte à la cybersécurité

DDoS – déni de service distribué

Europol – Agence de l'Union européenne pour la coopération des services répressifs

TIC – Technologies de l'information et de la communication

IdO – Internet des objets

IP – Protocole Internet

UIT – Union internationale des télécommunications

MLAT – Traité d'entraide judiciaire

SMART – Spécifique, mesurables, atteignable, réalisable et temporel

ONUDC – Office des Nations Unies contre la drogue et le crime

Auteurs

Shane Cross, Simon Hirrle (INTERPOL)

May-Ann Lim (TRPC Pte Ltd)

Remerciements

Ce Guide est le fruit des efforts consentis par de nombreuses personnes tout au long de son élaboration. Plusieurs consultations, ateliers, examens par des pairs et réunions de participation ont été organisés ; le Projet de renforcement des capacités de lutte contre la cybercriminalité de l'ASEAN (ACCDP) tient à remercier les personnes ci-dessous pour leur participation à l'élaboration du Guide :

- Steve Honiss (Aardwolf Consulting Ltd)
- Benjamin Ang (S. Rajaratnam School of International Studies, Université de technologie de Nanyang, Singapour)
- Claire Pluckrose
- Anthony Teelucksingh (Département de la Justice des États-Unis)
- Aysha Ahmed Bin Haji (ministre de l'Intérieur du royaume de Barheïn)
- Jeannie Tsang *et al.* (police de Hong Kong)
- Dr Cristos Velasco
- Yoichi Kumota (*National Center of Incident Readiness and Strategy for Cybersecurity*, Japon)
- Ismamuradi Abdul Kadir (CyberSecurity Malaysia)
- Représentants des pays de l'ASEAN lors de l'atelier de lancement de l'ACCDP
- Dong Uk Kim, Pei Ling Lee, Wei Xian Tee (INTERPOL)

Mentions légales

Le présent guide sur la stratégie nationale de lutte contre la cybercriminalité (le « Guide ») contient des informations générales et des recommandations en matière de compréhension et de lutte contre la cybercriminalité d'un point de vue stratégique, dans le but d'élaborer ou d'améliorer la stratégie nationale y afférente. Les informations figurant dans ce Guide sont issues des pays membres, de partenaires privés et de sources ouvertes. L'expertise et les conseils fournis dans ce Guide s'appuient sur ces informations et sont soumis à la réflexion du lecteur.

Les exemples, descriptions et examens qu'il contient sont uniquement mis à l'étude et ne constituent pas des recommandations, incitations ou propositions définitives. Toute action, proposition, mesure ou politique développée sur la base de ceux-ci doit respecter la législation en vigueur et doit être vérifiée et éprouvée par les lecteurs habilités dans leur juridiction. INTERPOL ne saurait en aucun cas être tenue pour responsable d'une telle action ou mesure, ni de tout document créé à partir de ce Guide.

Les liens vers des publications ou sites Internet externes figurant dans ce Guide sont uniquement fournis à titre de référence ; ils ne signifient pas qu'INTERPOL promeut ces publications ou leur contenu. Il incombe à l'utilisateur d'évaluer le contenu de ces autres publications/sites ainsi que l'utilité des informations qui en proviennent.

La description des dispositions relatives à certains instruments juridiques est uniquement fournie pour examen et ne constitue pas, ni ne saurait être considérée comme, une proposition d'interprétation pratique des instruments juridiques en question.

Le modèle de stratégie de lutte contre la cybercriminalité inclus dans ce Guide est uniquement fourni à des fins pédagogiques et à titre d'exemple / de suggestion. Il n'est en aucun cas contraignant ou approuvé par INTERPOL comme étant une stratégie efficace. Son utilisation reste à la discrétion du lecteur et doit tenir compte des politiques et lois en vigueur ainsi que de la situation particulière du pays concerné. INTERPOL ne saurait être tenue pour responsable de tout dommage ou préjudice résultant de son utilisation.

Avis relatif aux droits d'auteur

1. Introduction

Contexte

Ce Guide a été élaboré dans le cadre de la phase deux du Projet de renforcement des capacités de lutte contre la cybercriminalité de l'ASEAN (ACCDP II). L'ACCDP est un projet financé par le Fonds d'intégration Japon-ASEAN (JAIF) 2.0 via le secrétariat de l'ASEAN, le promoteur du projet étant le ministère singapourien de l'Intérieur. INTERPOL fait office d'organisme d'exécution.

Ce projet vise à renforcer la capacité des pays à lutter contre la cybercriminalité et à coopérer aux niveaux régional et international. L'ACCDP répond précisément à la nécessité pour les autorités judiciaires de développer leurs compétences, leurs connaissances et des partenariats régionaux en matière de cybercriminalité par le biais d'activités et d'outils sur-mesure.

L'ACCDP s'inscrit dans le cadre des initiatives mondiales de lutte contre la cybercriminalité d'INTERPOL et contribue à la mise en œuvre de sa stratégie mondiale y afférente. INTERPOL soutient les initiatives nationales de lutte contre la cybercriminalité et considère qu'il s'agit d'un domaine prioritaire à l'échelle mondiale, au même titre que le terrorisme et la criminalité organisée.

Méthode d'élaboration du Guide

Les conclusions synthétiques tirées des évaluations pays (bilans nationaux en matière de cybercriminalité) réalisées au cours de la première phase de l'ACCDP ont révélé que la plupart des États membres de l'ASEAN (EMA) avaient cruellement besoin d'une stratégie de lutte contre la cybercriminalité. C'est pourquoi ce Guide a été élaboré dans le cadre de la phase deux de l'ACCDP.

L'élaboration du Guide a commencé par un atelier d'une semaine, auquel ont participé des représentants des services chargés de l'application de la loi, des agences nationales de cybersécurité et des conseillers externes, puis s'est poursuivie avec la consultation d'experts d'INTERPOL et de ses pays membres.

Les informations contenues dans ce Guide ne concernent pas une région en particulier, mais décrivent les bonnes pratiques appliquées à l'échelle internationale.

Finalité du Guide

Le Guide est destiné à être utilisé par les pays souhaitant élaborer, actualiser ou améliorer leur stratégie nationale de lutte contre la cybercriminalité.

Le projet a noté une grande disparité entre les initiatives, lois et procédures en matière de lutte contre la cybercriminalité dans les pays membres d'INTERPOL et a insisté sur la nécessité de les harmoniser davantage avec les bonnes pratiques internationales.

Ce Guide vise à fournir une méthodologie pour l'élaboration ou l'actualisation d'une stratégie de lutte contre la cybercriminalité, qui peut s'avérer être une tâche ardue.

2. Cybercriminalité et cybersécurité

2.1 La définition complexe de la cybercriminalité

Il n'existe pas de définition communément admise de la cybercriminalité. La méthode la plus courante consiste à définir les termes-clés utilisés dans les enquêtes sur les cyber-infractions. L'examen de ces définitions permet d'identifier les grands concepts et d'utiliser ces définitions de manière cohérente dans le cadre d'une stratégie nationale de lutte contre la cybercriminalité.

Un exemple de cette méthode est la Loi type du Commonwealth relative à l'informatique et à la criminalité informatique de 2017 (la « Loi type du Commonwealth »)[1]. Ce texte de loi commence par définir quelques termes-clés : « données informatiques », « support de stockage de données informatiques », « fournisseur de services » et « données relatives au trafic ». Après avoir défini ces termes-clés, la Loi type du Commonwealth énumère les principales infractions considérées comme entrant dans le périmètre de la cybercriminalité : 1) accès illégal, 2) atteinte à l'intégrité des données, 3) atteinte à l'intégrité des systèmes informatiques, 4) interception illégale de données, 5) dispositifs illégaux et 6) contenu à caractère pédosexuel.

Cette approche est très similaire à celle adoptée par la Convention sur la cybercriminalité du Conseil de l'Europe (Convention de Budapest)[2], qui contient une première définition des termes « système informatique », « données informatiques », « fournisseur de services » et « données relatives au trafic ». La Convention identifie ensuite quatre catégories d'infractions commises au moyen de systèmes informatiques et de technologies de l'information, à savoir :

- Titre 1 : Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques (accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité des systèmes, abus de dispositifs) ;
- Titre 2 : Infractions informatiques (falsification informatique, fraude informatique) ;
- Titre 3 : Infractions se rapportant au contenu (infractions se rapportant à la pornographie enfantine) ;
- Titre 4 : Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes ;
- Titre 5 : Autres formes de responsabilité et de sanctions (tentative et complicité, responsabilité des personnes morales).

Tableau 1 : Comparaison des termes-clés relatifs à la cybercriminalité

Terme défini	Loi type du Commonwealth	Convention de Budapest
Données informatiques	« Données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction.	« Données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous un format adapté au traitement par un système informatique, y compris un programme permettant à un système informatique d'exécuter une fonction.
Support de stockage de données informatiques	« Support de stockage de données informatiques » désigne tout objet ou matériel (ex. disque) à partir duquel des informations peuvent être reproduites, avec ou sans l'utilisation d'un autre objet ou dispositif.	(Pas de définition de ce terme)

[1] https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf
[2] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Terme défini	Loi type du Commonwealth	Convention de Budapest
Système informatique	« Système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés (y compris Internet), qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ou toute autre fonction.	« Système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.
Fournisseur de services	« Fournisseur de services » désigne : a) toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et b) toute autre entité traitant ou stockant des données informatiques pour cette entité ou ses utilisateurs.	« Fournisseur de services » désigne : i) toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et ii) toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
Données relatives au trafic	« Données relatives au trafic » désigne les données informatiques a) ayant trait à une communication passant par un système informatique, b) produites par ce dernier en tant qu'élément de la chaîne de communication, et c) indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de services sous-jacents.	« Données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

La réussite d'une enquête sur la cybercriminalité peut dépendre de la qualité du recueil, de l'analyse et de l'attribution des éléments de preuve numériques. Le terme « élément de preuve numérique » est utilisé de manière interchangeable avec le terme « élément de preuve électronique » et désigne les informations et données stockées sur, reçues depuis ou transmises par un dispositif électronique. Il comprend les éléments de preuve issus d'appareils numériques ou de relevés obtenus auprès de fournisseurs de services en ligne.

2.2 Criminalité dépendant d'Internet *vs* infractions traditionnelles commises à l'aide d'Internet

Outre la définition des termes-clés relatifs à la cybercriminalité (qui est un terme général couvrant une multitude d'infractions), il est important de faire la distinction entre la criminalité dépendant d'Internet, également appelée « cybercriminalité pure », et les infractions traditionnelles commises à l'aide d'Internet. La série de recherches et de rapports d'analyse intitulée « *Cybercrime: a review of the evidence* »[3], publiée par le *Home Office* britannique, constitue une référence utile et fait la distinction entre ces deux concepts :

- La criminalité dépendant d'Internet (ou « cybercriminalité pure »), qui désigne les infractions ne pouvant être commises qu'à l'aide d'un ordinateur, d'un réseau informatique ou d'autres types de technologies de l'information et de la communication (TIC). Il s'agit notamment de la diffusion de virus et autres logiciels malveillants, du piratage et des attaques par déni de service distribué (DDoS). Ce sont des activités qui ciblent directement les ordinateurs ou réseaux, bien qu'elles puissent avoir des répercussions secondaires. À titre d'exemple, les données recueillies en piratant un compte de messagerie électronique peuvent ensuite être utilisées pour commettre une fraude[4].

[3] https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence
[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

- Les infractions traditionnelles commises à l'aide d'Internet, dont la portée ou l'ampleur peut être amplifiée grâce à l'utilisation d'ordinateurs, de réseaux informatiques ou d'autres types de TIC. Contrairement à la criminalité dépendant d'Internet, qui s'appuie exclusivement sur les TIC, les infractions traditionnelles commises à l'aide d'Internet peuvent l'être sans avoir recours aux TIC. Les deux types d'infractions traditionnelles commises à l'aide d'Internet les plus courants sont la fraude et le vol[5]. C'est notamment le cas des courriels frauduleux qui tentent d'inciter les destinataires à virer de l'argent à un expéditeur inconnu.

2.3 Cybersécurité *vs* cybercriminalité

Bien que les termes « cybersécurité » et « cybercriminalité » soient corrélés et que leurs intérêts se recoupent la plupart du temps, ils n'ont pas la même signification et leur périmètre diffère sur les plans technique, juridique et politique.

Le tableau ci-dessous décrit le périmètre de ces deux domaines réglementaires.

Tableau 2 : Définition de cybersécurité et cybercriminalité

Cybersécurité	**Cybercriminalité**
Définition	
La cybersécurité désigne généralement la protection de la confidentialité, de l'intégrité et de l'accessibilité des données et systèmes informatiques en vue de renforcer la sécurité, la résilience, la fiabilité et la confiance dans les TIC. Cette notion englobe généralement des aspects politiques (sécurité et intérêts nationaux), techniques et administratifs.	La cybercriminalité désigne les infractions commises à l'encontre de données informatiques, de supports de stockage de données informatiques, de systèmes informatiques et de fournisseurs de services. Cette notion englobe généralement des infractions telles que l'accès illégal, l'atteinte à l'intégrité des données et systèmes informatiques, la fraude et la falsification, l'interception illégale de données, les dispositifs illégaux, l'exploitation des enfants et les atteintes aux droits de propriété intellectuelle.
Objectif réglementaire	
La réglementation relative à la cybersécurité vise à protéger les infrastructures nationales ainsi que les secteurs public et privé contre les cyberattaques. Un positionnement solide en matière de cybersécurité permet de protéger les systèmes informatiques contre les accès non autorisés, la détérioration ou l'inaccessibilité. Le but est d'atténuer le risque de cyberattaque et de prévenir l'exploitation non autorisée des systèmes, réseaux et technologies via le recours à des technologies, procédés et contrôles sur les plans technique, procédural et institutionnel. La cybersécurité concerne les politiques et procédures de sécurisation et de protection des systèmes et ressources.	La réglementation relative à la cybercriminalité vise à définir ce que le pays considère comme des infractions dépendant d'Internet et des infractions traditionnelles commises à l'aide d'Internet, à doter le pays d'instruments de criminalisation des infractions et à autoriser la conduite d'enquêtes et de poursuites dans le cadre de cyber-infractions. Cette réglementation se concentre sur le droit matériel (ex. abus de dispositifs), le droit procédural (ex. préservation des données), ainsi que d'autres aspects comme les traités d'entraide judiciaire et le recueil d'éléments de preuve. Sa mise en application a pour but de protéger les citoyens en identifiant les auteurs des infractions, en contrecarrant leurs activités et en traduisant ces individus ou ces groupes criminels organisés en justice.
Chronologie	
La réglementation relative à la cybersécurité vise généralement à empêcher les attaques *avant* qu'elles ne surviennent. La sécurité est un cycle permanent qui comprend l'intervention en cas d'incident et la révision des procédés *après* la détection d'une violation.	La réglementation relative à la cybercriminalité définit et détecte les activités cybercriminelles *a posteriori* et confère aux services chargés de l'application de la loi des pouvoirs d'enquête sur ces infractions *après* leur survenance en vue de traduire leurs auteurs en justice.

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Une stratégie de lutte contre la cybercriminalité doit impérativement s'accompagner d'une stratégie de cybersécurité. Lors de certains incidents de cybersécurité, il n'est pas toujours évident de savoir s'il s'agit d'un incident de cybersécurité touchant des infrastructures personnelles, institutionnelles ou nationales, s'il s'agit d'un incident cybercriminel associé à la commission d'une infraction, ou s'il s'agit d'une combinaison des deux.

- En cas d'incident cybercriminel, il incombe aux services chargés de l'application de la loi et au système de justice pénale d'intervenir (ex. service chargé d'enquêter sur la cybercriminalité).
- En cas d'incident de cybersécurité, le service ou l'entité chargé(e) de la cybersécurité doit être déployé(e), à savoir une équipe d'intervention informatique d'urgence (CERT) ou une cellule d'intervention en cas d'atteinte à la cybersécurité (CSIRT).

Le rapport 2017 de l'Agence de l'Union européenne pour la cybersécurité (ENISA) intitulé « *Tools and methodologies to support cooperation between CSIRTs and law enforcement* »[6] a confirmé que les CSIRT et les services chargés de l'application de la loi échangeaient régulièrement des informations lors de la gestion de / l'enquête sur un incident, tant de manière formelle qu'informelle. La confiance est considérée comme un facteur clé de succès pour une coopération efficace. Le rapport a mis en évidence qu'en dépit de la divergence des objectifs et des méthodes de recueil et de traitement des informations entre les CSIRT et les services chargés de l'application de la loi, une compréhension mutuelle des besoins était en train de s'instaurer[7].

Si un pays n'a pas encore élaboré et mis en œuvre une stratégie de cybersécurité, le « *NCSS Good Practice Guide* » de l'ENISA peut être utile à cette fin[8].

3. Facteurs propices à la cybercriminalité

Plusieurs facteurs contribuent à créer un environnement lucratif pour les cybercriminels et une vaste population de victimes potentielles, notamment :

3.1 La connectivité : un plus grand nombre de personnes connectées ayant une conscience limitée de la sécurité numérique

Le nombre d'internautes ne cesse d'augmenter, avec comme conséquence directe le recours aux appareils mobiles, au e-commerce, ainsi qu'aux transactions et à la communication électroniques. La conscience généralement limitée de la cybersécurité et de l'hygiène informatique, en particulier chez les utilisateurs vulnérables comme les personnes âgées, **entraîne une hausse considérable du nombre de victimes de la cybercriminalité**.

[6] https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement
[7] https://www.enisa.europa.eu/publications/csirts-le-cooperation/at_download/fullReport
[8] https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

- Une étude menée en 2018 par une université américaine a révélé que la plupart des internautes à domicile avaient une conscience limitée de la cybersécurité, à savoir qu'ils ne connaissaient pas la différence entre un logiciel antivirus et un pare-feu, ainsi qu'une mauvaise hygiène informatique (ex. 67 % des personnes interrogées n'avaient pas de logiciel antivirus à jour, voire pas de logiciel antivirus installé). Par ailleurs, bon nombre d'utilisateurs n'hésitent pas à communiquer leurs mots de passe et à partager des informations personnelles sur les réseaux sociaux[9].

3.2 La mobilité : entreprises connectées avec du personnel travaillant à distance via des réseaux moins sécurisés

Une mobilité accrue et un accès élargi aux réseaux s'accompagnent d'une forte augmentation des salariés travaillant à distance, notamment depuis chez eux. Conséquence directe, de plus en plus de communications et transactions commerciales et officielles sont effectuées via des systèmes et réseaux informatiques domestiques ou publics moins sécurisés (ex. personnes travaillant depuis un café). **Cela accroît la vulnérabilité des réseaux d'entreprise et élargit ainsi la surface d'attaque pour les cybercriminels.**

- Une étude publiée en août 2020 par INTERPOL a révélé que le hameçonnage, les escroqueries en ligne, la fraude et d'autres cybermenaces avaient augmenté de pas moins de 59 % du fait de la COVID-19[10].
- Parmi les autres menaces, le Forum économique mondial (FEM) a indiqué en mars 2020 que les entreprises devaient instaurer des conditions pour le télétravail afin que leurs salariés puissent se connecter de manière sécurisée aux applications critiques. Il convient également de protéger les points de terminaison des appareils utilisés par les salariés pour accéder aux ressources professionnelles en ligne, notamment via une authentification multifacteur[11].

3.3 L'interconnectivité : villes et maisons connectées, qui créent de nouvelles formes de vulnérabilité

Villes intelligentes

L'accessibilité accrue et la miniaturisation des composants informatiques engendrent une accélération du déploiement des réseaux et infrastructures liés aux villes intelligentes. Parmi ces réseaux de villes interconnectées, citons l'*ASEAN Smart Cities Network*[12] et la *Smart Cities Mission*[13] que s'est donnée l'Inde. Si le développement des villes intelligentes constitue un objectif majeur pour bon nombre d'économies, il élargit dans le même temps la **surface d'attaque potentielle pour les cybercriminels ciblant des dispositifs intelligents vulnérables**.

- En 2017, les attaques par rançongiciel comme WannaCry et NotPetya ont révélé la menace que ce type d'attaque pouvait représenter pour les réseaux interconnectés, puisqu'elles compromettent un grand nombre d'appareils[14].

[9] https://par.nsf.gov/servlets/purl/10083310
[10] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
[11] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/
[12] https://asean.org/asean/asean-smart-cities-network/
[13] http://smartcities.gov.in/content/innerpage/strategy.php
[14] https://www.wsj.com/articles/how-hackers-could-break-into-the-smart-city-11568776732

Maisons intelligentes

Les villes intelligentes ne sont pas le seul exemple de la multitude de possibilités offertes par l'Internet des objets (IdO). La disponibilité croissante d'appareils domestiques intelligents accroît le nombre d'appareils potentiellement vulnérables. La plupart des utilisateurs de ces appareils ne changent pas le mot de passe par défaut ou ne mettent pas régulièrement à jour le logiciel, ce qui en fait des cibles faciles. Des objets domestiques du quotidien, tels que les serrures et les réfrigérateurs, peuvent désormais être connectés à Internet et sont autant de nouvelles opportunités pour les cybercriminels.

- En 2019, Kaspersky a indiqué que, sur les six premiers mois de l'année, plus de 100 millions d'attaques ciblant des dispositifs intelligents avaient été détectées. Ce chiffre représente une hausse considérable par rapport à l'année précédente, qui comptait 12 millions d'attaques détectées[15]. Le rapport précise par ailleurs que les cybercriminels privilégient les appareils domestiques aux dispositifs d'entreprise[16], car ce sont généralement des cibles plus faciles.
- En 2020, les pièges à pirate de Kaspersky (à savoir des réseaux de copies virtuelles de divers appareils connectés à Internet et applications) ont détecté 426 millions d'attaques sur des objets connectés provenant de 742 000 adresses IP uniques au cours des six premiers mois de l'année. Le nombre d'attaques a été multiplié par quatre et le nombre d'adresses IP par 2,5 par rapport à la même période de l'année précédente.

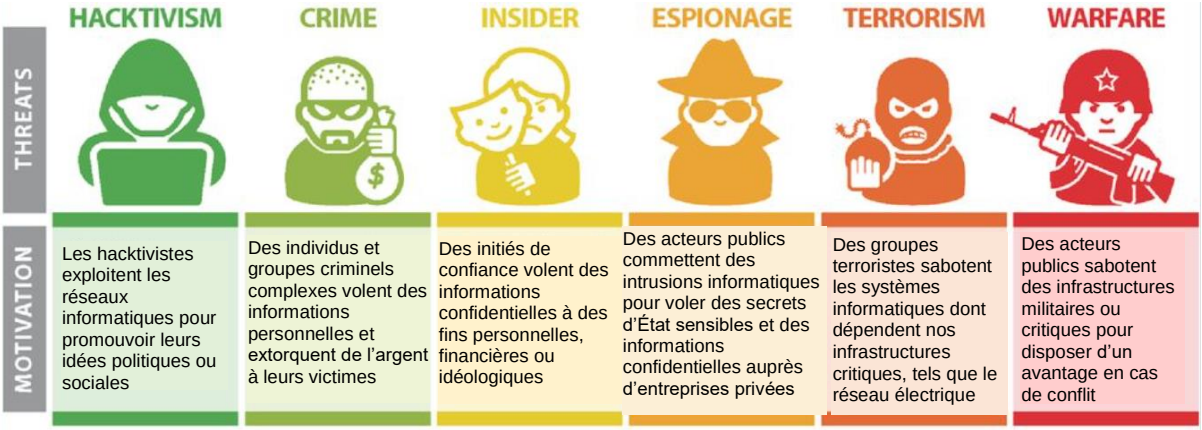
3.4 La sophistication : cybercriminels perfectionnant leurs compétences et leurs tactiques

Les cyber-infractions sont commises par des individus aux motivations diverses, tels que :

- les hacktivistes, qui utilisent Internet comme moyen de protestation ;
- les criminels, et notamment :
    - les débutants opportunistes ou curieux qui testent leurs compétences ;
    - les auteurs d'abus pédosexuels sur Internet ;
    - les groupes criminels organisés qui visent à gagner de l'argent ;
- les groupes de menace persistante avancée (APT) financés par les États aux fins d'espionnage, de levée de fonds ou d'attaque des infrastructures critiques.

Illustration 1 : Spectre des cybermenaces

[15] https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019
[16] https://securelist.com/iot-a-malware-story/94451/



Source : inconnue.

Ces dernières années, l'on a observé l'essor de la cybercriminalité en tant que service, dans le cadre de laquelle la « sociétisation de la cybercriminalité » met ces services à la portée de toute personne disposée à payer. Ces transactions interviennent généralement sur le Darknet, la face cachée d'Internet uniquement accessible via des navigateurs spécifiques. Les cybercriminels profitent de l'anonymat sur les marchés et les forums de discussion du Darknet pour proposer leurs compétences et leurs outils.

Un exemple de cybercriminalité en tant que service est le logiciel malveillant Satan, qui appartient à la famille des rançongiciels Gen:Trojan.Heur2.FU. Le logiciel Satan est mis à la disposition du public via une plateforme de rançongiciels en tant que service (RaaS)[17].

Les opérations à grande échelle menées à l'aide de rançongiciels entraînant de vastes perturbations et la destruction d'infrastructures personnelles, institutionnelles et nationales sont de plus en plus courantes :

- En 2020, la société Garmin, spécialisée dans le suivi de l'activité physique, a été attaquée par le rançongiciel WastedLocker. La société a déclaré avoir payé une rançon de 10 millions USD aux malfaiteurs pour récupérer ses systèmes et empêcher la diffusion publique des données de ses utilisateurs[18].
- En octobre 2020, la *Cybersecurity & Infrastructure Security Agency* (CISA) américaine a publié une alerte concernant la hausse de l'activité des rançongiciels ciblant les secteurs de la santé et de la santé publique[19].

3.5 Le signalement insuffisant : réticence à signaler les cyber-infractions

Dans la plupart des cas, les entreprises et personnes victimes de la cybercriminalité ne signalent pas l'incident aux autorités. **L'absence de signalement de ces infractions entraîne un manque de données sur le mode opératoire des cybercriminels et les technologies utilisées pour leur commission.** Malheureusement, ce phénomène est extrêmement répandu[20].

[17] https://www.zdnet.com/article/satan-ransomware-as-a-service-starts-trading-in-the-dark-web/
[18] https://www.wired.com/story/garmin-ransomware-hack-warning/
[19] https://us-cert.cisa.gov/ncas/alerts/aa20-302a
[20] https://www.zdnet.com/article/cyber-crime-under-reporting-of-attacks-gives-hackers-a-green-light-say-police/

- Les particuliers victimes ne savent souvent pas comment ou à qui signaler une cyber-infraction, pensent qu'il est inutile de la signaler ou ont honte d'avoir été victimes d'une escroquerie[21]. La plupart du temps, l'incident n'a pas entraîné de décès ou de perte de biens matériels (il s'agit généralement de données ou informations à caractère personnel) ; de fait, les victimes n'ont pas nécessairement conscience d'être victimes d'un acte criminel et ne le signalent pas aux autorités.
- Les entreprises victimes sont souvent réticentes à signaler les cyber-infractions car la diffusion d'une telle information auprès du grand public nuit à leur réputation et peut ébranler la confiance des investisseurs ou du marché[22]. Dans de nombreux pays, la réglementation relative à la protection des données remédie à ce problème en rendant obligatoire le signalement des incidents de cybersécurité.
- Dans certains cas, les victimes de cyber-infractions estiment que la procédure de signalement est contraignante ou opaque et renoncent ainsi à signaler l'incident.

3.6 La législation et la compétence : absence de criminalisation des cyber-infractions et complexité liée à la compétence

La cybercriminalité nécessite généralement la conduite d'enquêtes transfrontalières étant donné que les victimes, les malfaiteurs et les infrastructures se situent souvent dans des pays différents. Cela représente une difficulté pour les enquêteurs, qui peuvent ainsi se rendre compte que les autres pays n'ont pas nécessairement de lois criminalisant ce type d'infractions, que d'autres éléments sont requis pour prouver la commission de l'infraction, ou que la durée de conservation des données des utilisateurs n'est pas la même. Dans certains pays, il n'y a pas de législation, et donc de criminalisation, relative à la cybercriminalité, ce qui fait de ces pays un repaire sûr pour les cybercriminels.

Il est par ailleurs important que le cadre juridique national accorde suffisamment de temps pour le recueil, l'analyse et la diffusion des éléments de preuve numériques. Des délais trop courts peuvent empêcher l'obtention d'éléments de preuve essentiels, leur analyse correcte et leur réception dans les temps, et entraîner l'abandon des poursuites à l'encontre des cybercriminels.

Afin de mener des enquêtes efficaces dans plusieurs juridictions, il convient de collaborer avec les homologues des autres pays pour faire avancer l'enquête. Cette collaboration peut consister à effectuer des fouilles et des saisies d'éléments de preuve physiques et/ou numériques, ou à présenter des autorisations judiciaires telles que des mandats à des entités du secteur privé (ex. sociétés de télécommunication et fournisseurs d'accès à Internet).

Ce n'est qu'un aperçu des difficultés liées à la conduite d'enquêtes efficaces dans plusieurs juridictions en vue de traduire les cybercriminels en justice.

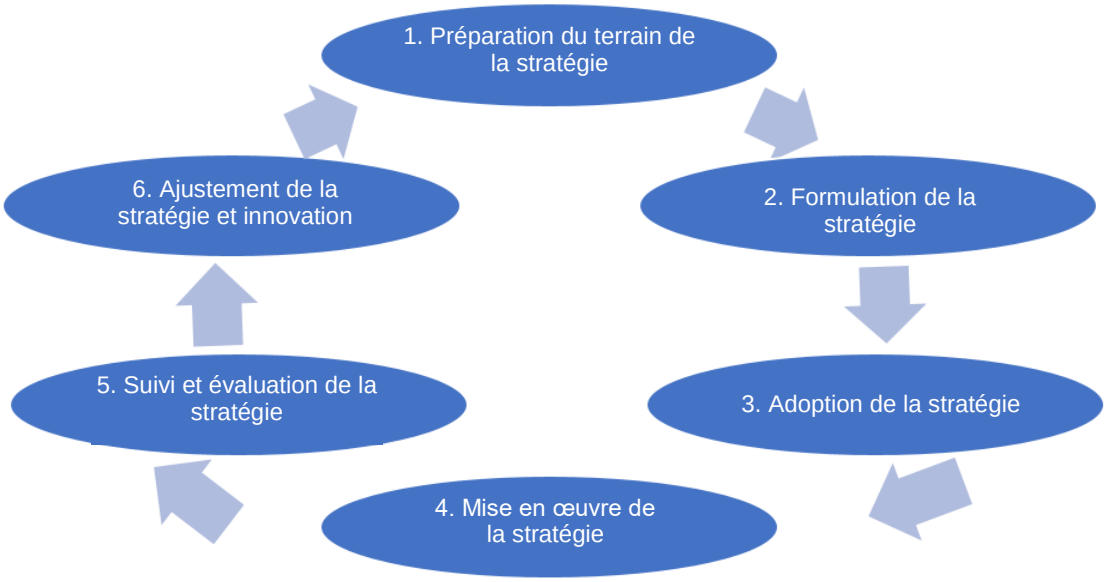
[21] https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html
[22] https://www.infosecurity-magazine.com/opinions/organizations-failing-report/

4. Méthodologie : élaboration d'une stratégie de lutte contre la cybercriminalité

L'élaboration d'une stratégie de lutte contre la cybercriminalité peut sembler insurmontable, mais cela ne l'est pas si l'on suit un processus de conception.

Il existe de nombreux modèles de formulation de politiques, dont la plupart reprennent les étapes ci-dessous :

Illustration 2 : Cycle de vie d'une stratégie



Source : TRPC, 2020

4.1 Préparation du terrain de la stratégie

Avant de commencer à élaborer une stratégie de lutte contre la cybercriminalité, il est important de comprendre sa raison d'être.

La cybercriminalité est l'une des formes de criminalité transnationale qui connaît l'expansion la plus rapide au sein des pays membres d'INTERPOL. La croissance rapide des TIC s'est accompagnée d'un développement économique et social, mais la dépendance accrue à Internet a aussi multiplié les risques et les vulnérabilités et a ouvert de nouvelles perspectives aux activités criminelles.

La cybercriminalité est un phénomène qui s'affranchit des frontières. En conséquence, les services chargés de l'application de la loi doivent relever les défis liés aux enquêtes transfrontalières, aux différences entre les systèmes juridiques et à la disparité des capacités.

Une stratégie claire est nécessaire pour qu'un pays puisse surmonter ces difficultés et protéger efficacement ses citoyens de la cybercriminalité.

Les raisons et avantages de l'élaboration d'une stratégie de lutte contre la cybercriminalité sont nombreux, comme nous allons le voir ci-après.

4.1.1 La cybercriminalité sape l'économie

Lors de la cyberattaque mondiale NotPetya en juin 2017, le rançongiciel a frappé de grands opérateurs logistiques et leurs clients. La redirection de dernière minute, l'indemnisation et le maintien de la chaîne d'approvisionnement mondiale ont coûté pas moins de 300 millions USD à la société Maersk[23]. Le préjudice ne s'est pas limité à cette société, puisque ses clients ont également été gravement touchés par l'incident. Entre autres, la société pharmaceutique Merck a perdu 870 millions USD, TNT Express (qui appartient à FedEx), 400 millions USD, et le chocolatier Cadbury, 188 millions USD.

Cet effet domino de la cybercriminalité a été tout aussi visible lors de l'attaque à grande échelle par DDoS via le réseau de machines zombies Mirai contre le fournisseur de noms de domaine Dyn en 2016, paralysant ainsi l'activité de la plupart des 178 000 clients dont le domaine Internet était hébergé par la société[24]. Ces incidents illustrent la sophistication et la contagiosité accrues des nouvelles méthodes cybercriminelles qui ont évolué par rapport aux attaques d'ancienne génération comme Stuxnet, un virus informatique qui a infecté au moins quatre sociétés pétrolières et gazières : Baker Hughes, ConocoPhillips, Marathon et Chevron[25].

Le *Global Risk Report* 2020 du Forum économique mondial estime que le coût des dommages causés par la cybercriminalité pourrait atteindre 6 000 milliards USD en 2021[26].

Une stratégie de lutte contre la cybercriminalité définit les mesures à prendre en vue d'instaurer une bonne gouvernance des données dans les entreprises et une bonne hygiène informatique personnelle afin de limiter les répercussions économiques.

4.1.2 La cybercriminalité facilite la commission d'autres infractions

D'après l'Office des Nations Unies contre la drogue et le crime (ONUDC), les incidents cybercriminels sont fréquemment orchestrés par des réseaux criminels sévissant en ligne, qui utilisent le produit des rançons et les bénéfices illégaux pour financer d'autres formes de grande criminalité ou le terrorisme[27].

Une stratégie de lutte contre la cybercriminalité soutient les initiatives en matière d'antiterrorisme et de lutte contre le blanchiment de capitaux (AT/LBC), et court-circuite les mécanismes de financement des réseaux criminels organisés.

4.1.3 La cybercriminalité paralyse les services publics et peut coûter des vies

Les cyberattaques par rançongiciel causent des ravages dans l'ensemble des secteurs d'activité. Elles touchent bien souvent les services essentiels, comme les hôpitaux et les organismes de santé ; des vies peuvent alors être en jeu à cause de la neutralisation des systèmes informatiques. À titre d'exemple, en 2017, l'attaque menée avec le rançongiciel WannaCry a frappé le *National Health Service* (NHS) du Royaume-Uni, neutralisant dans certains cas les systèmes médicaux alors que des médecins étaient en train d'effectuer des opérations critiques comme une chirurgie cardiaque[28].

[23] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[24] https://www.corero.com/blog/financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data/
[25] https://isssource.com/stuxnet-hit-4-oil-companies/
[26] http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
[27] https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html
[28] https://www.dailymail.co.uk/news/article-4503420/It-s-life-death-NHS-patients-say-cyber-attack.html

De même, en septembre 2020, un hôpital de Düsseldorf, en Allemagne, a été victime d'une attaque par rançongiciel. En raison du verrouillage des systèmes de l'hôpital, une patiente atteinte d'une maladie mortelle a dû être transférée vers un autre hôpital, où elle est décédée à cause de sa prise en charge tardive[29].

Une stratégie de lutte contre la cybercriminalité doit aller de pair avec une stratégie de cybersécurité afin d'assurer la continuité des services essentiels.

4.1.4 Avantages de la stratégie

Parmi d'autres avantages, la stratégie :

- informe toutes les personnes pouvant y contribuer et en retirer des bénéfices ;
- permet de mieux cerner les vulnérabilités d'un pays ;
- favorise l'innovation en matière de lutte contre la cybercriminalité ;
- fournit un cadre établi de prévention, de détection et d'intervention
- permet de sensibiliser.

4.1.5 Prérequis de la stratégie

4.1.5.1 Désigner un responsable de projet

L'élaboration d'une stratégie nationale de lutte contre la cybercriminalité nécessite la coopération de nombreux acteurs. L'une des principales difficultés consiste à obtenir et maintenir l'engagement des parties concernées.

Il est donc important de désigner un « responsable de projet », comprenant un haut dirigeant (idéalement un ministre) et une équipe de projet chargés d'élaborer, de mettre en œuvre et de réviser la stratégie de lutte contre la cybercriminalité.

Le haut dirigeant est responsable du document et doit veiller à ce que :

- l'équipe de projet bénéficie de la coopération de l'ensemble des parties prenantes ;
- des ressources suffisantes soient affectées à la mise en œuvre de la stratégie.

À titre d'exemple, le haut dirigeant pourrait être le ministre de l'Intérieur et l'équipe de projet pourrait se composer de membres de l'unité nationale chargée de la cybercriminalité, ou prendre la forme d'une cellule spéciale conjointe.

Le responsable de projet siège également au comité de pilotage (cf. point 4.2.1).

➔ Il est crucial d'avoir un bon dirigeant et une bonne équipe de projet pour assurer la réussite de la stratégie de lutte contre la cybercriminalité.

4.1.5.2 Obtenir une coopération intragouvernementale

L'élaboration efficace d'une stratégie nécessite une coopération interservices. Cela peut s'avérer difficile : il faut un bon encadrement, une collaboration efficace et, bien souvent, des compromis. Cette coopération interservices est absolument essentielle à toutes les étapes du projet, telles que l'élaboration et la mise en œuvre de la stratégie de lutte contre la cybercriminalité.

Le responsable de projet doit consulter les services partenaires concernés afin d'obtenir leur avis et leur soutien.

[29] https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

Une fois que le concept de projet est validé par tous, il est recommandé que le responsable de projet instaure un mécanisme de coopération intragouvernementale. Ce mécanisme peut prendre la forme de réunions périodiques avec l'ensemble des parties prenantes, par exemple dans le cadre d'un comité de pilotage (cf. point 4.2.1).

➔ Assurez-vous d'avoir le soutien des services partenaires avant d'initier le projet.

4.1.5.3 Prévoir un budget et des ressources suffisants

Il n'est pas rare que les organismes publics soient confrontés à des restrictions budgétaires et de ressources. Cela peut nuire au déroulement du projet et à la mise en œuvre d'une stratégie nationale de lutte contre la cybercriminalité.

La réussite du projet dépend entièrement de la planification et de l'affectation de ressources dédiées et adéquates, à la fois financières (ex. budget dédié) et humaines (ex. équipe dédiée au projet).

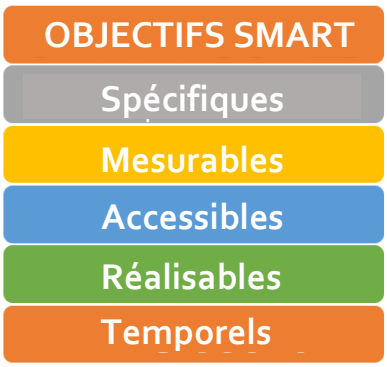
De même, l'affectation adéquate des ressources humaines et financières est essentielle pour la mise en œuvre de la stratégie de lutte contre la cybercriminalité (cf. point 4.4).

➔ Assurez-vous de disposer de ressources suffisantes avant d'initier le projet.

4.1.5.4 Définir des objectifs SMART

Le cycle de vie de la stratégie de lutte contre la cybercriminalité doit s'appuyer sur des objectifs SMART[30], c'est-à-dire des objectifs spécifiques, mesurables, atteignables, réalisables et temporels. Le projet doit donc commencer par la définition d'objectifs spécifiques à atteindre selon un calendrier précis, avec des étapes mesurables et des dates butoirs.

Illustration 3 : Objectifs SMART



Un objectif SMART pourrait être l'identification des acteurs concernés aux différentes étapes du cycle de vie de la stratégie de lutte contre la cybercriminalité dans un délai de six semaines.

➔ Cette méthode vous permettra de clarifier vos idées, de concentrer vos efforts, d'optimiser l'utilisation de votre temps et de vos ressources, et ainsi d'accroître les chances de réussite de votre projet et de la stratégie de lutte contre la cybercriminalité.

4.2 Formulation de la stratégie

C'est le processus de conception et de rédaction de la stratégie de lutte contre la cybercriminalité pour les raisons et avantages mentionnés au point 4.1.

[30] https://www.achieveit.com/resources/blog/the-history-and-evolution-of-smart-goals

4.2.1 Désignation du comité de pilotage et identification des parties prenantes

Des études ont montré que la réussite des politiques publiques dépendait souvent fortement de l'implication et de la gestion des parties prenantes[31]. Les stratégies qui ne bénéficient pas de l'engagement, du soutien ou de l'adoption des parties prenantes manquent généralement de ressources et d'attention et ne sont pas considérées comme prioritaires.

La première étape consiste à créer un comité de pilotage, composé du responsable de projet et d'autres hauts dirigeants sélectionnés en fonction de leur capacité à fournir une supervision et une orientation stratégiques au cours des différentes étapes du cycle de vie de la stratégie de lutte contre la cybercriminalité.

Le comité de pilotage est chargé d'identifier les acteurs devant être impliqués dans la formulation de la stratégie de lutte contre la cybercriminalité. Ces acteurs (les « consultants ») sont généralement issus d'organismes publics et d'entités non gouvernementales.

Organismes publics :

- L'unité nationale chargée de la cybercriminalité, afin de partager son expérience et ses connaissances en matière d'enquête dans ce domaine de criminalité ;
- Le service responsable de la cybersécurité, afin de partager son expérience en matière d'intervention dans le cadre d'incidents de cybersécurité et d'élaboration des politiques y afférentes (dont des stratégies) ;
- D'autres services chargés de l'application de la loi, afin d'aider à la compréhension des obstacles et processus régionaux en matière d'enquête sur les cyber-infractions, tels que le recueil d'éléments de preuve électroniques ;
- Un ou plusieurs hauts dirigeants des ministères compétents, en particulier ceux pouvant donner du poids et apporter un soutien à l'élaboration ou l'adoption de la stratégie de lutte contre la cybercriminalité. Il peut notamment s'agir du ministère de l'Intérieur et du ministère de la Justice ;
- Des représentants du ministère public et des autorités judiciaires pouvant conseiller sur l'application des lois informatiques dans le pays ;
- D'autres représentants et membres des pouvoirs publics, comme les services chargés d'enquêter sur la fraude ou des représentants des ministères responsables des TIC, de la sûreté publique et de la sécurité, etc.

Entités non gouvernementales :

- Universitaires / groupes de réflexion pouvant apporter des connaissances sur les enjeux actuels et mettre à disposition des compétences rédactionnelles et en matière de recherche ;
- Organisations technologiques/sectorielles en mesure d'identifier les principales menaces qui pèsent sur les entreprises ;
- Groupes de la société civile afin de sensibiliser le grand public ;
- Organismes régionaux et internationaux, afin d'échanger des points de vue sur les menaces cybercriminelles à l'échelle régionale.

La sélection des consultants adéquats permettra de répondre à l'ensemble des besoins des parties prenantes et constituera un fondement solide pour l'élaboration de la stratégie de lutte contre la cybercriminalité. Les parties prenantes n'ayant pas été consultées dès le départ et embarquées à un stade plus avancé peuvent être sources de perturbations, voire saper les efforts antérieurs.

[31] http://www.oecd.org/gov/regulatory-policy/BPPs-for-Public-Consultation.docx

À la suite de l'identification des consultants, un petit groupe de personnes les mieux ciblées pour la rédaction (les « rédacteurs ») est constitué en vue de produire la stratégie (cf. point 4.2.3, « Rédaction »).

4.2.2 Inventaire, évaluation et analyse

Il est crucial que le pays fasse l'inventaire des procédures, ressources et compétences disponibles en matière de lutte contre la cybercriminalité. Cet exercice permettra également de mettre en lumière les domaines lacunaires. Après cela, le pays aura une meilleure vision de son environnement cybercriminel et pourra commencer à travailler sur ses objectifs en termes de renforcement des capacités de lutte contre la cybercriminalité.

L'inventaire doit porter sur les catégories suivantes :

4.2.2.1 Ressources humaines et matérielles

Cet audit a pour but de recenser les ressources humaines disponibles ou occupant des fonctions en lien avec la cybercriminalité, telles que le personnel spécialisé dans la cybercriminalité, la criminalistique numérique, ou encore la cybersécurité comme les CERT.

Exemples de services appartenant à cette catégorie :

- Police nationale (services et unités) ;
- Service chargé de la cybersécurité (le cas échéant) :
    - Cellule nationale d'intervention en cas d'atteinte à la cybersécurité (CSIRT) et/ou CERT ;
- Autorités judiciaires nationales, régionales et locales ou ministère de la Justice :
    - Juges spécialisés dans la cybercriminalité
    - Procureurs spécialisés dans la cybercriminalité
    - Service d'enquête ;
- Autorité centrale responsable des traités d'entraide judiciaire ;
- Service national chargé de la sécurité ou du renseignement ;
- Autres services nationaux spécialisés dans les infractions traditionnelles commises à l'aide d'Internet (ex. fraude, exploitation, etc.) ;
- Autres services de police nationaux ou locaux disposant d'unités d'enquête actives dans le domaine de la cybercriminalité.

Chacun de ces services doit fournir les informations suivantes :

- Un résumé de la structure et de la mission de leur service et des unités concernées ;
- La description des formes de cybercriminalité ciblées par le service ;
- Le cadre juridique au sein duquel il évolue ;
- Les initiatives de lutte contre la cybercriminalité actuellement menées par le service.

Il convient également de s'interroger sur les capacités technologiques de ces services : disposent-ils du matériel adéquat et ont-ils été formés ?

4.2.2.2 Procédures : évaluation du contexte législatif et réglementaire

Il s'agit de faire l'inventaire des mécanismes législatifs et réglementaires actuels en matière de lutte contre la cybercriminalité dans le pays. Il couvre la législation y afférente, les accords de coopération internationale, les normes et procédures opérationnelles internes, les coutumes et pratiques locales, etc.

Ces mécanismes peuvent être répartis dans les catégories suivantes :

- **Droit matériel** : lois relatives à la protection de la vie privée ou des données à caractère personnel, lois criminalisant des infractions comme le piratage informatique et le vol de données, lois criminalisant la vente d'outils ou de services de piratage, lois sanctionnant le harcèlement sur Internet, ou encore lois déterminant les critères de protection des infrastructures critiques.
- **Droit procédural** : lois relatives au recueil et à l'exploitation d'éléments de preuve électroniques, règles relatives à la fouille et à la saisie d'éléments de preuve électroniques, règles relatives à la surveillance électronique.
- **Accords de coopération internationale** : traités d'entraide judiciaire, adhésion à la Convention de Budapest[32], recours actif à INTERPOL pour exploiter les systèmes de coopération internationale.

Les consultants sont chargés d'examiner la législation actuelle et d'identifier les lacunes dans le cadre juridique du pays. Dans certains cas, il peut être nécessaire de fusionner plusieurs lois ou d'actualiser les lois afin de criminaliser les cyber-infractions, mais aussi la réglementation qui légalise et prescrit la fouille, la saisie et la recevabilité des éléments de preuve électroniques dans le cadre des enquêtes judiciaires. Outre la législation relative à la cybercriminalité, il convient parfois de passer en revue les pouvoirs d'enquête dont jouissent les services chargés de l'application de la loi, les questions de compétence, ainsi que les lois relatives à la protection des données et de la vie privée, sans oublier le droit commercial relatif à la confiscation des produits issus de la cybercriminalité.

4.2.2.3 Auto-évaluation et analyse

Une fois l'inventaire réalisé, il convient de procéder à une évaluation en vue d'identifier les vulnérabilités et les axes d'amélioration. Plusieurs boîtes à outils existent pour conduire des évaluations nationales et mesurer la capacité de lutte contre la cybercriminalité d'un pays.

L'Union internationale des télécommunications (UIT) réalise une évaluation périodique de cette capacité pays par pays, qui permet de suivre et de comparer les engagements des différents pays en matière de cybersécurité via l'examen de cinq piliers : le cadre juridique, le cadre technique, le cadre organisationnel, le renforcement des capacités et la coopération. Cette évaluation tient également compte des résultats obtenus à l'aide d'autres outils d'évaluation, tels que le modèle de maturité de la capacité (CMM) et le *Cyber Readiness Index* du Potomac Institute. Le produit qui en résulte s'appelle l'Indice de cybersécurité dans le monde (GCI)[33].

Depuis 2017, la Banque mondiale propose un outil d'auto-évaluation approfondie (*Combatting Cybercrime Assessment Tool*) et son guide (*Toolkit*). Cette ressource[34] se compose donc d'un outil d'évaluation[35] sous forme de fichier Excel automatisé, qui permet à l'utilisateur d'identifier les lacunes en matière de lutte contre la cybercriminalité et les domaines auxquels affecter les ressources. Le guide qui l'accompagne (*Toolkit*[36]) vise à contextualiser l'outil d'évaluation. La première utilisation de l'outil d'évaluation fournit un indicateur de référence qui peut ensuite être contrôlé régulièrement. L'outil d'évaluation et le guide doivent être utilisés conjointement.

L'Indice de cybersécurité dans le monde de l'UIT est généralement publié une fois par an, mais les pays peuvent effectuer une auto-évaluation à l'aide de l'outil d'évaluation et du guide de la Banque mondiale quand ils le souhaitent.

---

[32] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[33] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[34] https://www.combattingcybercrime.org/
[35] https://www.combattingcybercrime.org/#assessment
[36] https://www.combattingcybercrime.org/#toolkit

Les résultats de cette auto-évaluation mettront en évidence les vulnérabilités et les axes d'amélioration, qui doivent être considérés comme des axes prioritaires de la stratégie, comme évoqué au point suivant.

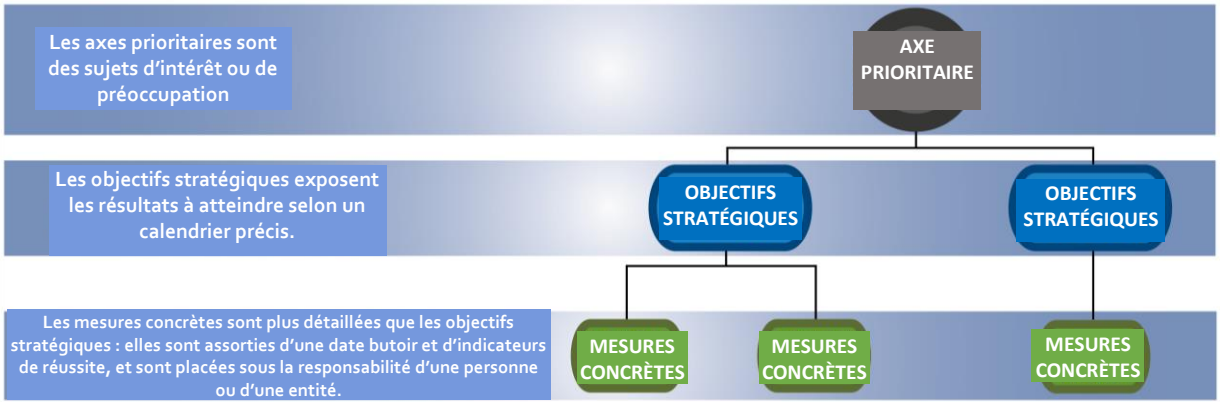
En fonction de l'outil d'évaluation utilisé et des résultats obtenus, il peut être utile de structurer ces derniers à l'aide de méthodes d'analyse éprouvées, telles que :

- FFPM : forces, faiblesses, possibilités et menaces ;
- PESTLE : politique, économique, social, technologique, juridique et environnemental.

La méthode choisie doit permettre aux décideurs politiques de déterminer quelles lacunes parmi celles identifiées lors de l'auto-évaluation doivent être priorisées pour agir à court, moyen et long termes.

4.2.2.4 Axes prioritaires, objectifs stratégiques et mesures concrètes

Illustration 4 : Axes prioritaires, objectifs stratégiques et mesures concrètes



Le pays identifie les axes prioritaires qu'il souhaite traiter, tel que le cadre juridique, grâce à l'auto-évaluation et à l'analyse (point 4.2.2.3). Il définit ensuite des objectifs stratégiques pour cet axe prioritaire, par exemple « Instaurer un cadre juridique plus efficace en matière d'enquête et de poursuites des cyber-infractions ». De ces objectifs découleront une ou plusieurs mesures concrètes devant être prises par leurs responsables, par exemple actualiser les lois en vigueur et en rédiger de nouvelles sur la cybercriminalité.

Les axes prioritaires, autrement dit les domaines que le pays souhaite améliorer, constituent la pierre angulaire de la stratégie que le pays élabore en s'appuyant sur les résultats de l'auto-évaluation et de l'analyse. C'est la première étape de création d'une structure qui permettra au pays de lutter plus efficacement contre la cybercriminalité.

Les axes prioritaires sont les grands thèmes de la stratégie et ont une durée de vie plus longue que les objectifs stratégiques et les mesures concrètes.

Les objectifs stratégiques énoncent clairement les résultats que le pays souhaite atteindre selon un calendrier défini.

Les mesures concrètes sont identifiées par le responsable de projet et les acteurs concernés (point 4.2.1, « consultants ») en fonction de leur adéquation avec les objectifs stratégiques. Les mesures concrètes doivent suivre le modèle SMART (point 4.1.5) et répondre le mieux possible aux questions suivantes :

- De quelle manière l'objectif stratégique peut-il être atteint ?
- Existe-t-il des programmes ou mécanismes contribuant à l'objectif stratégique ?
- Comment les programmes ou mécanismes actuels peuvent-ils être améliorés ?

- Quels programmes ou mécanismes doivent être créés ou développés ?
- Comment seront-ils mis en œuvre ?
- Quel est le calendrier ?
- Comment leur efficacité sera-t-elle mesurée (indicateurs de réussite) ?

Une fois que les axes prioritaires, les objectifs stratégiques et les mesures concrètes ont été clairement définis, ils peuvent être synthétisés dans un tableau de référence, comme le tableau ci-dessous :

Tableau 3 : Exemple de tableau synthétique des axes prioritaires, des objectifs stratégiques et des mesures concrètes

Axes prioritaires	Objectifs stratégiques	Mesures concrètes
Cadre juridique	Instaurer un cadre juridique plus efficace en matière d'enquête et de poursuites des cyber-infractions	• Rédiger et promulguer des lois relatives à la cybercriminalité dans un délai de 18 mois (service responsable : ministère de la Justice) • Adhérer à la Convention de Budapest sur la cybercriminalité dans un délai de deux ans (service responsable : cellule spéciale conjointe entre le ministère de la Justice et le ministère des Affaires étrangères)
Renforcement des capacités	Renforcer les capacités des fonctionnaires, en particulier des services chargés de l'application de la loi, du ministère public et des autorités judiciaires	• Développer et mettre en place un programme de formation sur la cybercriminalité destiné aux services chargés de l'application de la loi dans un délai de 12 mois (service responsable : ministère de l'Intérieur / de la Sécurité publique ou assimilé) • Développer et organiser une formation sur les principes de base relatifs aux éléments de preuve numériques, destinée aux juges et aux procureurs, dans un délai de 12 mois (service responsable : bureau du procureur général, ministère de la Justice)
Partenariats	Promouvoir les alliances et les accords de partage d'informations nationaux et internationaux	• Instaurer des accords de partage public-privé en matière de cyber-renseignement dans un délai de huit mois (service responsable : unité cybercriminalité de la police) • Instaurer un système d'alerte des cybermenaces entre les secteurs public et privé dans un délai de neuf mois, en priorisant les secteurs stratégiques (service responsable : cellule spéciale conjointe entre l'unité cybercriminalité et le ministère de l'Industrie et du Commerce, en collaboration avec les autres ministères compétents)

4.2.3 Rédaction

La rédaction de la stratégie de lutte contre la cybercriminalité est l'étape du cycle de vie qui nécessite le plus de temps. Pour vous aider dans cette tâche, un modèle est fourni au chapitre 5 de ce Guide.

4.2.3.1 Consultation des parties prenantes

Il convient de mettre en place un processus itératif dans le cadre d'échanges sur les axes prioritaires avec les parties prenantes (« consultants »). Cela permet aux participants à la stratégie de donner leur avis sur la manière de progresser sur les axes prioritaires et, ce faisant, de définir les objectifs stratégiques (cf. point 5.4).

4.2.3.2 La première version de la stratégie de lutte contre la cybercriminalité

C'est l'étape au cours de laquelle le groupe de rédacteurs précédemment constitué (point 4.2.1) rédige une première version de la stratégie de lutte contre la cybercriminalité, en tenant compte des raisons et avantages mentionnés au point 4.1 et des résultats de l'inventaire décrit au point 4.2.2.

Il est de coutume que la rédaction d'une stratégie passe par plusieurs étapes d'écriture, de consultation, de retours, de révision et de modification. Plus la rédaction est minutieuse, plus il y a de chances que la version finale de la stratégie fasse l'unanimité auprès des parties prenantes.

Les rédacteurs peuvent se référer au Modèle de stratégie de lutte contre la cybercriminalité (chapitre 5), qui propose une structure possible du document.

4.3 Adoption de la stratégie

Une fois que le processus de formulation de la stratégie est terminé, la version finale de la stratégie de lutte contre la cybercriminalité est prête à être officiellement présentée en vue de son adoption et de sa mise en œuvre.

Ce processus diffère d'un pays à l'autre. Dans certains pays, la stratégie devra préalablement être débattue et approuvée par l'assemblée nationale, le parlement ou un autre forum politique public, ou soumise à l'approbation du chef du gouvernement / de l'État.

4.4 Mise en œuvre de la stratégie

La mise en œuvre d'une stratégie de lutte contre la cybercriminalité ne peut être réussie qu'en adoptant une méthode structurée. Elle diffère d'un pays à l'autre, mais comprend généralement les étapes suivantes :

- Détailler la manière dont les objectifs stratégiques seront atteints (point 4.2.2.4)
- Élaborer un plan de mise en œuvre par mesure concrète
- Affecter des ressources humaines et financières adéquates

Le responsable de projet et les consultants doivent concevoir des mesures concrètes et des plans de mise en œuvre en vue d'atteindre les objectifs stratégiques, et désigner les agents ou unités responsables (« responsables de mesure »). Les responsables de mesure doivent être des représentants des services/unités les plus concernés par la mesure qui leur est attribuée et disposant des meilleures capacités pour la mettre en œuvre.

Ces agents ou unités sont ensuite chargés et responsables de l'exécution du plan qui leur est attribué. Étant donné que les plans de mise en œuvre sont destinés à être exécutés au niveau opérationnel, ils doivent être parfaitement compréhensibles pour les services responsables (responsables de mesure).

Le responsable de projet peut être amené à coordonner l'exécution des différents plans.

Le comité de pilotage peut devoir aider à obtenir les ressources adéquates pour l'exécution des différents plans afin que les efforts consentis jusqu'à présent ne soient pas vains.

Il est recommandé d'inclure des indicateurs (notamment de réussite) dans les plans de mise en œuvre, lesquels permettront de suivre l'avancée de chacune des mesures concrètes.

4.5 Suivi et évaluation de la stratégie

Conformément aux objectifs SMART (point 4.1.5.4) de la stratégie de lutte contre la cybercriminalité, le responsable de projet et les consultants doivent également planifier le suivi et l'évaluation de la stratégie à intervalles réguliers afin de maintenir la dynamique de progrès. L'absence de suivi continu des activités de mise en œuvre peut compromettre les mesures concrètes elles-mêmes, mais aussi le projet dans son ensemble.

Des échanges permanents avec les responsables de mesure et leurs comptes-rendus sur les indicateurs prédéfinis permettront de poursuivre la mise en œuvre de la stratégie de lutte contre la cybercriminalité dans la bonne voie. Le suivi doit se concentrer sur des détails, comme l'avancée des activités de mise en œuvre, la disponibilité des ressources ainsi que les difficultés et risques pouvant entraver l'exécution du plan. Le responsable de projet doit être informé de tout retard dans les meilleurs délais afin que des plans d'atténuation puissent être mis en place. De même, le responsable de projet doit être informé des accomplissements afin qu'ils soient reconnus.

4.6 Ajustement de la stratégie et innovation

À l'instar du processus itératif d'élaboration de la stratégie de lutte contre la cybercriminalité, la version finale de la stratégie doit être révisée régulièrement afin de tenir compte des évolutions technologiques, des vecteurs d'attaque et des besoins du pays.

Exemple : évolution de la stratégie de cybersécurité et de lutte contre la cybercriminalité de la Nouvelle-Zélande

L'exemple de la progression de la stratégie de lutte contre la cybercriminalité de la Nouvelle-Zélande illustre le processus adopté par de nombreux pays pour instaurer un cadre directeur qui s'adapte à l'évolution des tendances économiques et sociétales. Il montre également que la stratégie nationale de lutte contre la cybercriminalité doit être harmonisée avec et s'intégrer dans un cadre plus large de politiques nationales, lesquelles font l'objet de cycles de révision permanents.

La stratégie de cybersécurité de 2011 de la Nouvelle-Zélande présentait la réponse du gouvernement face à l'essor des cybermenaces via la définition d'axes prioritaires et d'initiatives et l'affectation de ressources adéquates.

En 2015, une version actualisée de la stratégie de cybersécurité accompagnée d'un plan d'action est venue remplacer la version de 2011 ; un **Plan national de lutte contre la cybercriminalité**[37] (semblable à une stratégie de lutte contre la cybercriminalité) a également été publié afin d'apporter une réponse adéquate à la cybercriminalité en s'appuyant sur les axes prioritaires suivants :

- Renforcer les capacités de lutte contre la cybercriminalité
- Adapter les cadres politique et législatif à l'ère numérique
- Améliorer la réponse opérationnelle apportée à la cybercriminalité
- Exploiter les relations internationales de la Nouvelle-Zélande dans le cadre de la lutte contre la cybercriminalité

Illustration 5 : Plan national de lutte contre la cybercriminalité de la Nouvelle-Zélande

[37] https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-cybercrime-plan-december-2015.pdf

En 2019, la Nouvelle-Zélande a publié la troisième version de sa stratégie de cybersécurité[38], qui présente de nouveaux axes prioritaires en matière de cybersécurité et de lutte contre la cybercriminalité.

Illustration 6 : Évolution de la stratégie de cybersécurité et de lutte contre la cybercriminalité de la Nouvelle-Zélande

5. La Convention de Budapest

Bien que l'objectif d'une stratégie nationale de lutte contre la cybercriminalité soit de renforcer les capacités d'un pays en la matière, il convient toutefois de l'harmoniser avec les normes et pratiques internationales. Un pays qui élabore ou actualise sa stratégie doit faire en sorte que son cadre juridique et ses objectifs stratégiques satisfassent aux critères d'adhésion à l'accord international sur la cybercriminalité et les éléments de preuve électroniques le plus complet et cohérent qui existe, à savoir la Convention sur la cybercriminalité du Conseil de l'Europe, plus connue sous le nom de Convention de Budapest.

5.1 À propos de la Convention

La Convention est le premier traité international relatif aux infractions commises via Internet et d'autres réseaux informatiques, qui cible plus précisément les infractions contre et via des systèmes et données informatiques, telles que l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données et systèmes, la fraude informatique, le contenu mettant en scène l'exploitation sexuelle d'enfants et d'autres violations de la sécurité des réseaux. Elle prévoit également un éventail de pouvoirs et procédures d'enquête judiciaire ainsi que l'obtention d'éléments de preuve électroniques en lien avec les infractions dont les preuves se trouvent dans un système informatique, notamment via la conservation rapide, la fouille de réseaux informatiques ou l'interception.

Son objectif premier est de poursuivre une politique pénale commune tendant à la protection de la société contre la cybercriminalité, en particulier via l'adoption d'une législation appropriée et la promotion de la coopération internationale.[39] La Convention vise principalement à :

(1) harmoniser les éléments de droit matériel des infractions dans le droit pénal national et les dispositions y afférentes dans le domaine de la cybercriminalité ;

[38] https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf
[39] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

(2) octroyer les pouvoirs de procédure pénale nationale nécessaires à la conduite d'enquêtes et de poursuites au titre de ce type d'infractions ou d'autres infractions commises à l'aide d'un système informatique ou dont les éléments de preuve se présentent sous forme électronique ; et

(3) instaurer un mécanisme rapide et efficace de coopération internationale.[40]

La Convention a été ouverte à la signature en novembre 2001 à Budapest, en Hongrie. En 2003, elle a été complétée par le Protocole relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Un second protocole devrait être prochainement adopté en faveur d'une coopération et d'une diffusion accrues des éléments de preuve électroniques, notamment via une coopération directe avec les fournisseurs de services et une coopération dans les situations d'urgence.

5.2 Avantages de la Convention

Tous les pays peuvent utiliser la Convention de Budapest comme guide, liste de contrôle ou loi type. Toutefois, l'adhésion à ce traité offre des avantages supplémentaires :

- La Convention fournit un cadre juridique pour la coopération internationale en matière de cybercriminalité et d'éléments de preuve électroniques. Le Chapitre III du traité contient des dispositions générales et particulières sur la coopération entre les parties « dans la mesure la plus large possible », non seulement dans le domaine de la cybercriminalité (infractions contre et via des systèmes informatiques), mais également dans le cadre de toute infraction impliquant des éléments de preuve électroniques.
- Les parties sont membres du Comité de la Convention sur la cybercriminalité (T-CY). Les parties partagent des informations et des expériences, évaluent la mise en application de la Convention ou interprètent la Convention via des notes d'orientation.
- Le T-CY peut également rédiger des protocoles additionnels à ce traité. Ainsi, même si une partie n'a pas participé à la négociation du traité originel, elle peut participer à la négociation des futurs instruments et de l'évolution de la Convention de Budapest.
- Les parties à la Convention s'engagent mutuellement à une coopération fiable et efficace. Il semblerait que les entités du secteur privé soient plus enclines à coopérer avec les autorités judiciaires des parties à la Convention, étant donné que celles-ci sont tenues d'instaurer un cadre juridique national en matière de cybercriminalité et d'éléments de preuve électroniques, dont les sauvegardes énoncées à l'article 15.
- Les pays candidats à l'adhésion ou ayant adhéré à la Convention sont généralement prioritaires pour les programmes de renforcement des capacités. Cette assistance technique vise à faciliter la mise en application de la Convention et à accroître la capacité de coopération à l'échelle internationale.

5.3 Adhésion à la Convention

Aux termes de l'article 37 de la Convention, tout État peut devenir partie au traité par « adhésion » s'il est disposé à mettre en application les dispositions énoncées dans la Convention. La procédure d'adhésion est la suivante :

[40] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680occc5b

1. Après avoir rédigé une loi (ou un projet de loi) indiquant que le pays a transposé ou prévoit de transposer les dispositions de la Convention de Budapest dans son droit national, le ministre des Affaires étrangères (ou un représentant habilité) adresse un courrier au Secrétaire général du Conseil de l'Europe pour lui faire part de la volonté de son pays d'adhérer à la Convention de Budapest.

2. Le Conseil de l'Europe consulte alors les parties à la Convention et, une fois que celles-ci parviennent à un accord, l'adhésion du pays est validée.

3. Les autorités du pays achèvent leurs procédures internes pour la ratification de traités internationaux, puis déposent l'instrument d'adhésion auprès du Conseil de l'Europe.[41]

[41] https://rm.coe.int/cyber-buda-benefits-june2020a-en/16809ebe38

6. Modèle de stratégie de lutte contre la cybercriminalité

Ce chapitre propose un modèle dont peuvent s'inspirer les rédacteurs qui en sont aux prémices de l'élaboration de la stratégie de lutte contre la cybercriminalité. Il reprend les points abordés dans les chapitres précédents et fournit des conseils supplémentaires sur la structure et le contenu.

Ce modèle comprend les éléments couramment intégrés dans les stratégies de lutte contre la cybercriminalité, mais nous recommandons aux rédacteurs de tenir compte du contexte et du cadre réglementaire locaux.

La stratégie de lutte contre la cybercriminalité comprend quatre composantes principales :

- Introduction
- Évaluation et analyse de l'environnement cybercriminel actuel
- Ambition
- Axes prioritaires, objectifs stratégiques et mesures concrètes

6.1 Introduction

Cette première partie introduit la stratégie nationale de lutte contre la cybercriminalité. Elle doit permettre aux lecteurs de comprendre la nature de la cybercriminalité dans le pays. Elle peut comprendre des sous-parties comme celles présentées ci-dessous.

6.1.1 Avant-propos

Il peut s'agir d'un message d'une personne soutenant et pilotant la stratégie comme le ministre compétent ou un autre haut responsable politique. Cet élément introductif doit illustrer l'importance de la stratégie et montrer qu'elle bénéficie du soutien de hauts dirigeants qui attendent des résultats. Il convient également de présenter le responsable de projet.

6.1.2 Objet du document

Cette partie explique comment la stratégie sera exploitée et en quoi elle sera utile pour le pays.

6.1.3 Nécessité de la stratégie

Cette partie peut présenter l'évolution de la stratégie de lutte contre la cybercriminalité dans le pays et expliquer le fondement de cette stratégie (cf. point 4.1).

Si elles sont disponibles, il est possible de citer des statistiques, telles que le nombre d'incidents cybercriminels, le nombre d'utilisateurs d'Internet et/ou d'appareils mobiles à l'échelle locale, ou encore les répercussions financières pour le pays et les victimes. Ces chiffres permettront de mettre le contexte cybercriminel actuel en perspective et les statistiques relatives à l'adoption des nouvelles technologies pourront fournir des informations précieuses sur les futurs vecteurs d'attaque potentiels, tels que les objets connectés vulnérables.

Si le pays ne dispose pas de données complètes sur la cybercriminalité, il peut utiliser les chiffres mondiaux comme indicateurs.

6.2 Environnement cybercriminel actuel

6.2.1 Définitions en lien avec la cybercriminalité

Cette partie définit clairement ce que le pays considère comme des infractions dépendant d'Internet et des infractions traditionnelles commises à l'aide d'Internet, ainsi que la notion de cybersécurité (points 2.2 et 2.3). Elle peut également détailler les différents types de cybercriminels (point 3.4) et citer des statistiques pertinentes sur la cybercriminalité.

6.2.2 Statistiques sur la cybercriminalité du pays

Cette partie décompose les statistiques générales du point 5.1.3 selon des indicateurs pertinents, tels que la nature des infractions, la région, la population, etc. Cela permettra d'identifier les cyber-infractions les plus fréquemment commises dans le pays.

Exemples de chiffres et tendances pouvant être cités dans cette partie :

- Le nombre d'infractions dépendant d'Internet par type (ex. nombre d'attaques par rançongiciel au cours d'une période donnée) ;
- Le nombre d'infractions traditionnelles commises à l'aide d'Internet signalées au cours d'une période donnée ;
- Les principales formes de cybercriminalité (défiguration de sites Internet, rançongiciels, hameçonnage, contenu à caractère pédosexuel, harcèlement sur Internet, etc.) ;
- La hausse des diverses formes de cybercriminalité en chiffres et pourcentage sur une période donnée (ex. en glissement annuel).

Le Guide des statistiques judiciaires sur la cybercriminalité et les éléments de preuve électroniques[42] présente les questions importantes en matière de recueil des statistiques de la justice pénale et définit les étapes clés de la collecte et de l'analyse de données ainsi que de la coopération entre plusieurs parties prenantes.

6.2.3 Autorités spécialisées dans la cybercriminalité

Cette partie répertorie l'ensemble des services et autorités chargés d'enquêter sur et de réprimer les cyber-infractions, ainsi que d'engager des poursuites à ce titre. Elle décrit leur rôle dans le système de justice pénale et leur mandat (point 4.2.2.1).

L'objectif est d'exposer clairement la responsabilité de chaque autorité, sa compétence, ses domaines d'enquête, ses initiatives et la nature des cyber-infractions dont elle s'occupe.

6.2.4 Législation actuelle

Cette partie de la stratégie présente la législation relative à la cybercriminalité ayant déjà été adoptée (point 4.2.2.2).

Il peut s'agir :

- de lois relatives à la cybersécurité ;
- de lois relatives à la criminalité informatique ;
- du droit pénal matériel ;

[42] https://www.interpol.int/content/download/15731/file/Guide%20for%20Criminal%20Justice%20Statistics%20on%20Cybercrime%20and%20Electronic%20Evidence.pdf

- du droit procédural (fourniture d'informations élémentaires sur les abonnés, de données relatives au trafic ou au contenu, etc.) ;
- de lois et/ou d'accords de coopération internationale (ex. traités d'entraide judiciaire) ;
- de lois relatives à la protection des données, y compris la réglementation de la conservation des données pour les dépositaires/sous-traitants de données ;
- de toute autre loi octroyant des pouvoirs en matière de prévention, d'enquête ou de poursuites dans le cadre de cyber-infractions.

6.2.5 Synthèse de l'auto-évaluation et de l'analyse

Cette partie présente les résultats du processus d'auto-évaluation et d'analyse décrit au point 4.2.2.3, qui vise à identifier les capacités du pays en matière de lutte contre la cybercriminalité et les lacunes qui doivent être comblées. Cette évaluation étaiera la définition des axes prioritaires, objectifs stratégiques et mesures concrètes de la stratégie (point 5.4).

6.3 Ambition

Cette partie énonce clairement l'ambition du pays en matière de lutte contre la cybercriminalité. Elle se présente généralement sous forme de synthèse des résultats stratégiques escomptés. En voici quelques exemples :

- « L'ambition du NCAP est de garantir un environnement virtuel sûr à Singapour. Nous y parviendrons en menant des actions efficaces de dissuasion, de détection et de perturbation des activités cybercriminelles. » Plan national de lutte contre la cybercriminalité (NCAP) de Singapour[43] ;
- « Les citoyens, les entreprises et les pouvoirs publics peuvent bénéficier des avantages offerts par un environnement virtuel sûr et résilient : nous devons collaborer à l'échelle nationale et internationale afin de comprendre et d'éliminer les risques, de limiter les bénéfices pour les criminels et les terroristes, et de saisir les opportunités d'accroître la sécurité et la résilience du Royaume-Uni. » Stratégie de lutte contre la cybercriminalité du *Home Office* britannique[44] ;
- « La Stratégie de lutte contre la cybercriminalité de la GRC a pour objectif de réduire la menace, les répercussions et la victimisation associées à la cybercriminalité au Canada grâce à des mesures policières. » Stratégie de lutte contre la cybercriminalité de la Gendarmerie royale du Canada (GRC)[45].

L'ambition doit idéalement décrire une approche globale (à l'échelle du gouvernement comme de la société) en matière de lutte contre la cybercriminalité, car la dissuasion, la détection et la perturbation des activités cybercriminelles sont la responsabilité commune des pouvoirs publics, des citoyens, des entreprises et de la société civile. Plus l'ambition est claire, plus il sera facile pour les dirigeants et parties prenantes d'adopter une approche globale et cohérente.

[43] https://www.mha.gov.sg/docs/default-source/press-releases/ncap-document.pdf
[44] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf
[45] https://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf

6.4 Axes prioritaires, objectifs stratégiques et mesures concrètes

Cette partie est la plus volumineuse de la stratégie de lutte contre la cybercriminalité. Elle fait suite à l'auto-évaluation et l'analyse (point 4.2.2.3). En s'appuyant sur ces résultats, elle vise à identifier les axes prioritaires que le pays considère comme impératifs pour lutter efficacement contre la cybercriminalité. Ces axes prioritaires se traduisent ensuite en objectifs stratégiques et en mesures concrètes (point 4.2.2.4), qui sont attribuées aux services concernés (responsables de mesure) et font l'objet d'un suivi (point 4.5).

6.4.1 Axes prioritaires

Comme indiqué ci-avant, les axes prioritaires résultent de l'auto-évaluation et de l'analyse (point 4.2.2.3). Ils doivent être détaillés à l'aide de définitions claires et préciser la raison de leur sélection.

6.4.2 Objectifs stratégiques

Un axe prioritaire peut avoir plusieurs objectifs stratégiques. Ceux-ci exposent les résultats à atteindre selon un calendrier précis.

6.4.3 Mesures concrètes

Les mesures concrètes sont plus détaillées que les objectifs stratégiques : elles sont assorties d'une date butoir et d'indicateurs de réussite, et sont placées sous la responsabilité d'une personne ou d'une entité. Plusieurs mesures concrètes peuvent correspondre à un objectif stratégique.

6.4.4 Exemples d'objectifs stratégiques et de mesures concrètes correspondantes

Vous trouverez ci-après des exemples pour les pays souhaitant définir les objectifs stratégiques de leur stratégie de lutte contre la cybercriminalité. Nous vous invitons également à consulter le point 4.2.2.4, et notamment le Tableau 3.

6.4.4.1 Objectif stratégique N° 1 : Instaurer un cadre juridique plus efficace en matière d'enquête et de poursuites des cyber-infractions

Le cadre juridique de nombreux pays ne criminalise pas suffisamment les cyber-infractions. Ainsi, le nombre de cyber-infractions ne cesse d'augmenter tandis que la législation marque le pas.

Un objectif stratégique pourrait consister à actualiser le cadre juridique et à exploiter les cadres ou instruments internationaux pour surmonter les difficultés actuellement rencontrées en matière d'enquête, de répression et de jugement des cyber-infractions.

Mesures concrètes, délais et services responsables

- Rédiger et promulguer une loi relative à la cybercriminalité dans un délai de *période déterminée* (services responsables proposés : ministère de la Justice, ministère de l'Intérieur ou bureau du procureur général) ;
- Adhérer à la Convention de Budapest sur la cybercriminalité dans un délai de deux ans (service responsable proposé : cellule spéciale conjointe entre le ministère de la Justice et le ministère des Affaires étrangères).

6.4.4.2 Objectif stratégique N° 2 : Renforcer les capacités des autorités judiciaires

Les cyber-infractions sont de plus en plus nombreuses et complexes, ce qui crée des besoins supplémentaires en termes de formation continue pour les autorités judiciaires (ex. police, procureurs et juges) spécialisées dans la cybercriminalité. Dans le même temps, les éléments de preuve numériques jouent un rôle toujours plus important dans diverses affaires pénales. La préservation de l'intégrité des éléments de preuve numériques de leur recueil à leur présentation devant le tribunal est souvent un facteur clé de succès des poursuites.

Étant donné que les appareils numériques et les éléments de preuve électroniques sont présents dans presque tous les types d'infractions, même les agents chargés de l'application de la loi « non spécialisés » doivent avoir une connaissance élémentaire des éléments de preuve numériques et de leur méthode de recueil.

Les procureurs et les juges s'appuient sur le recueil légal d'éléments de preuve précis et fiables en vue de leur présentation et de leur recevabilité devant un tribunal. Les condamnations dépendent souvent du degré de compréhension des éléments de preuve numériques par les procureurs et les juges.

Un objectif stratégique pourrait consister à renforcer les capacités des autorités judiciaires nationales chargées de la prévention, des enquêtes, des poursuites et du jugement des cyber-infractions.

Le renforcement des capacités d'enquête des agents chargés de l'application de la loi leur permettra de lutter plus efficacement contre la cybercriminalité et de faciliter la collaboration avec d'autres organismes publics et des entités privées.

Le renforcement des capacités des procureurs et des juges leur permettra d'interpréter correctement les éléments de preuve électroniques et de les présenter/recevoir devant un tribunal.

Mesures concrètes, délais et services responsables

- Mettre en place et réviser régulièrement un programme de formation sur la cybercriminalité destiné aux services chargés de l'application de la loi dans un délai de six mois (service responsable proposé : ministère de l'Intérieur / de la Sécurité publique ou assimilé) ;
- Dispenser au minimum cinq formations sur les enquêtes en matière de cybercriminalité destinées aux services chargés de l'application de la loi chaque année, à compter de la mise en place du programme de formation (service responsable proposé : ministère de l'Intérieur / de la Sécurité publique ou assimilé) ;
- Organiser et dispenser au minimum une formation sur les principes de base relatifs aux éléments de preuve numériques destinée aux juges et procureurs traitant les cyber-infractions dans un délai de huit mois (services responsables proposés : ministère de la Justice, bureau du procureur général).

6.4.4.3 Objectif stratégique N° 3 : Favoriser les partenariats pour lutter contre la cybercriminalité

Si le personnel spécialisé dans la cybercriminalité et la cybersécurité est chargé d'œuvrer à un environnement virtuel plus sûr, il ne peut pas y parvenir seul. L'aide apportée par d'autres services nationaux, d'autres pays et d'autres secteurs peut être cruciale pour approfondir ses connaissances et renforcer ses capacités.

Collaboration intragouvernementale

Certains services ont tendance à être cloisonnés, et c'est parfois aussi le cas en matière d'échange d'informations entre les services nationaux. Les connaissances, les renseignements et les ressources sont souvent disséminés dans plusieurs services, avec un manque de diffusion ou de coordination des informations, des initiatives, des enquêtes et des capacités entre ces services.

Un objectif stratégique pourrait consister à encourager l'échange d'informations et de ressources entre les services afin d'adopter une approche beaucoup plus efficace en matière de lutte contre la cybercriminalité.

Collaboration intergouvernementale

Les malfaiteurs s'affranchissent des frontières pour communiquer et agir, ce qui leur confère un avantage par rapport aux autorités chargées de les traduire en justice.

Un objectif stratégique pourrait consister à élargir l'utilisation des réseaux internationaux, notamment par les services chargés de l'application de la loi et le ministère public. Ces réseaux permettent généralement d'échanger des informations par le biais de divers mécanismes afin de gagner en efficacité.

Les services nationaux chargés de l'application de la loi disposent de plusieurs mécanismes de coopération, à la fois formels (traités d'entraide judiciaire, par exemple) et informels en vue d'accélérer la transmission d'informations entre les services. Des réseaux officiels disponibles 24 heures sur 24, 7 jours sur 7, tels que le réseau I-24/7 d'INTERPOL, le *24/7 High Tech Crime Network* du G8 et le réseau 24h/24, 7j/7, des contacts des parties à la Convention de Budapest sur la cybercriminalité, ont été développés afin de réceptionner les demandes urgentes d'éléments de preuve numériques et de faciliter la coopération internationale.

Il existe également des mécanismes spécifiques pour les procureurs spécialisés dans la cybercriminalité, tels que le *Global Prosecutors E-Crime Network* (GPEN) de l'*International Association of Prosecutors*.

Partenariats public-privé

La prévention et l'enquête sur des incidents de cybersécurité complexes requièrent des compétences et ressources techniques importantes, qui peuvent être plus facilement accessibles pour les organisations du secteur privé que pour les services chargés de l'application de la loi.

Une collaboration multiniveaux accrue entre les secteurs public et privé permettra d'améliorer considérablement les capacités du pays en matière de lutte contre la cybercriminalité, tandis qu'un public mieux informé limitera le nombre de victimes potentielles.

Un objectif stratégique pourrait consister à former des partenariats public-privé dans différents secteurs en faveur de la prévention et de l'enquête sur les cyber-infractions. Ces partenariats avec des entités comme les fournisseurs de services de télécommunication, les services financiers et les sociétés spécialisées dans la cybersécurité peuvent s'articuler autour de plusieurs axes : sensibilisation, formation technique, ou encore assistance en matière d'analyse et d'enquête via le partage d'informations et de renseignements. Ils peuvent viser à obtenir des informations sur les cybermenaces, les tendances, les vulnérabilités et la gestion d'incidents particuliers.

Un autre objectif stratégique pourrait consister à sensibiliser le grand public aux cybermenaces les plus courantes. Des initiatives public-privé telles que le programme *Get Safe Online*[46] du Royaume-Uni donnent des conseils pratiques au grand public sur la manière de se protéger et de protéger les ordinateurs, les appareils mobiles et les entreprises contre la fraude, l'usurpation d'identité, les virus et de nombreux autres risques présents sur Internet.

Partenariats avec des organisations multinationales

Des partenariats avec les bonnes organisations peuvent avoir un impact direct sur la capacité d'un pays à lutter contre la cybercriminalité, car ils permettent d'échanger des informations et de partager des renseignements susceptibles de faire avancer les enquêtes ou d'être autrement utiles. Ils peuvent également avoir un impact indirect via le travail en réseau et le partage de ressources sous forme de dons de matériel ou de mises à disposition temporaires auprès de certaines organisations partenaires. Les partenaires internationaux et régionaux peuvent par ailleurs apporter des solutions en matière de renforcement des capacités et de partage des bonnes pratiques, dont ce Guide est un exemple.

Un objectif stratégique pourrait consister à former et entretenir des partenariats stratégiques à l'échelle régionale et mondiale.

À l'échelle mondiale, des organisations comme INTERPOL, l'ONUDC, l'UIT, la Banque mondiale et les Centres de partage et d'analyse d'informations (ISAC) sont des partenaires intéressants.

À l'échelle régionale, des partenariats avec des organisations comme l'ASEAN ou ASEANAPOL, Europol, l'Union africaine, l'Organisation des États américains (OEA), l'Organisation de coopération économique (OCE), la Communauté des Caraïbes (CARICOM) et l'*Implementing Agency for Crime and Security* (IMPACS), entre autres, peuvent s'avérer particulièrement bénéfiques.

Mesures concrètes, délais et services responsables

- Créer un « bureau central » de la cybercriminalité, c'est-à-dire un organisme qui centralise le travail des différents acteurs nationaux intervenant dans le cadre des enquêtes et poursuites menées au titre d'incidents cybercriminels. Ce bureau central devrait comprendre un guichet unique pour le signalement des infractions afin d'éviter la duplication des enquêtes. Mise en œuvre dans un délai de 12 mois, pilotée par les ministères compétents ;
- Encourager et optimiser l'utilisation des réseaux disponibles 24 heures sur 24, 7 jours sur 7, avec effet immédiat. Les services responsables sont ceux chargés du fonctionnement du système de justice pénale, par ex. le ministère de l'Intérieur / de la Sécurité publique et le ministère de la Justice ;
- Permettre la conclusion d'accords officiels de partage de renseignements entre des organismes publics et des entités du secteur privé dans un délai de six mois, avec l'objectif d'identifier les cybermenaces qui pèsent sur les secteurs stratégiques (énergie, eau, santé, communication, finance, transport, etc.). Service responsable proposé : unité nationale chargée de la cybercriminalité ;
- Promouvoir une bonne hygiène informatique via des campagnes de sensibilisation comme le *Safer Internet Day*[47], qui a lieu tous les ans en février. Mise en œuvre dans un délai de six mois. Services responsables proposés : service national chargé de la cybersécurité et unité nationale chargée de la cybercriminalité ;

[46] https://www.getsafeonline.org
[47] https://www.saferinternetday.org/

- Explorer et exploiter pleinement les informations et renseignements disponibles auprès ou via des organisations comme INTERPOL (ex. Groupe d'experts mondial d'INTERPOL sur la cybercriminalité (GEMC) et signalements d'activités cybercriminelles (SAC)), avec effet immédiat. Service responsable : unité nationale chargée de la cybercriminalité ou ministère compétent.

6.4.5 Annexes

6.4.5.1 Glossaire

Il est recommandé d'intégrer à la stratégie de lutte contre la cybercriminalité un glossaire définissant les termes-clés, les abréviations et les acronymes.

6.4.5.2 Références

Liens vers les références pouvant fournir des informations complémentaires.

Annexe A : Stratégies et règlements nationaux en matière de cybersécurité et de lutte contre la cybercriminalité

La présente annexe fournit une liste des ressources et références accessibles au public dont les pays peuvent s'inspirer pour formuler leur propre stratégie de lutte contre la cybercriminalité. Certains pays ont choisi de ne pas publier leur stratégie de lutte contre la cybercriminalité, ce qu'il est possible de faire lorsque la diffusion publique présente un risque.

La plupart du temps, la stratégie de lutte contre la cybercriminalité vient compléter la stratégie de cybersécurité. Dans certains cas, la stratégie de lutte contre la cybercriminalité fait partie intégrante de la stratégie de cybersécurité.

Australie

- Stratégie de cybersécurité (2020) https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf

Canada

- Stratégie nationale de cybersécurité (2018) https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf
- Stratégie de lutte contre la cybercriminalité de la Gendarmerie royale du Canada (2014) http://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf

Europe / Union européenne

- Convention de Budapest et normes y afférentes (2001) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561
- Agence de l'Union européenne pour la cybersécurité (ENISA) - *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies* (2016) https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport

Nouvelle-Zélande

- Plan national de lutte contre la cybercriminalité (2015) https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-cybercrime-plan-december-2015.pdf
- Stratégie de cybersécurité (2019) https://dpmc.govt.nz/sites/default/files/2019-07/Cyber%20Security%20Strategy.pdf

Singapour

- Stratégie de cybersécurité de Singapour (2016) https://www.csa.gov.sg/-/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

Royaume-Uni

- Stratégie nationale de cybersécurité 2016-2021 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

- Stratégie de lutte contre la cybercriminalité (2010)
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

États-Unis d'Amérique (2018)

- Stratégie nationale de cybersécurité des États-Unis d'Amérique
  https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Union internationale des télécommunications (UIT)

- Guide pour l'élaboration d'une stratégie nationale de cybersécurité (2018)
  https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

INTERPOL

À PROPOS D'INTERPOL

INTERPOL est l'organisation internationale de police la plus importante au monde. Notre rôle est d'assister les services chargés de l'application de la loi de nos 194 pays membres dans la lutte contre toute forme de criminalité transnationale. Nous nous employons à aider les polices du monde entier à relever les défis – de plus en plus nombreux – de la lutte contre la criminalité au 21ème siècle en leur apportant un appui technique et opérationnel grâce à une infrastructure de pointe. Nos services comprennent des formations ciblées, un soutien spécialisé aux enquêtes, des bases de données spécialisées et un système de communication policière sécurisé.

NOTRE VISION : « RELIER LES POLICES POUR UN MONDE PLUS SÛR »

Notre vision est celle d'un monde dans lequel chaque professionnel des services chargés de l'application de la loi pourra, par la voie d'INTERPOL, transmettre, partager et consulter en toute sécurité des informations de police vitales, à tout moment et en tout lieu où il en aura besoin, afin d'assurer la sécurité des personnes sur toute la surface du globe. Nous apportons et travaillons à offrir continuellement des solutions innovantes et de pointe aux problèmes qui se posent à l'échelle mondiale en matière de police et de sécurité.