GUIDE POUR L´ÉLABORATION D´UNE STRATÉGIE NATIONALE DE CYBERSÉCURITÉ

ENGAGEMENT STRATÉGIQUE POUR LA CYBERSÉCURITÉ

ITU

CCDCOE

The Commonwealth Cybercrime Initiative

CTO

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Deloitte.

Global Cyber Security Capacity Centre

GCSP
Geneva Centre for Security Policy

Microsoft

Certains droits réservés

Droits & autorisation

Remerciements

Ce Guide a été élaboré par douze partenaires d'organisations intergouvernementales et internationales issues du secteur privé, des milieux universitaires et de la société civile, dont: le Secrétariat du Commonwealth (Comsec), l'Organisation des télécommunications du Commonwealth (OTC), Deloitte, le Centre de Genève pour la politique de sécurité (GCSP), le Centre mondial des capacités de cybersécurité (GCSCC) de l'Université d'Oxford, l'Union internationale des télécommunications (UIT), Microsoft, le Centre d'excellence de l'OTAN pour la cyberdéfense en coopération (CE-CDC OTAN), l'Institut Potomac d'études politiques, RAND Europe, la Banque mondiale et la Conférence des Nations Unies sur le commerce et le développement (CNUCED).

L'équipe comptait les membres suivants: Katalaina Sapolu (Comsec), Shadrach Haruna (Comsec), Martin Koyabe (OTC), Fargani Tambeayuk (OTC), Andrea Rigoni (Deloitte), Carolin Weisser (GCSCC), Marco Obiso (UIT), Kaja Ciglic (Microsoft), Kadri Kaska (CE-CDC OTAN), Francesca Spidalieri et Melissa Hathaway (Institut Potomac d'études politiques), Erik Silfversten (RAND Europe), David Satola et Sandra Sergeant (Banque mondiale) et Cecile Barayre (CNUCED).

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a apporté une contribution significative à ce Guide.

Nous saluons également les contributions des personnes ci-après: Grace Acayo, Rosheen Awotar-Mauree, Ben Baseley-Walker, Paul Cornish, Luc Dandurand, Michael Goldsmith, Kemal Huseinovic, Andraz Andy Kastelic, Maxim Kushtuev, Lena Lattion, Gustav Lindstrom, Damien Maddalena, Emily Munro, Lara Pace, Sarah Puello Alfonso, Valeria Risuglia, Taylor Roberts, Monica M. Ruiz, Irene Rubio, Ann Valjataga et Julienne Wright.

Avant-propos

J'ai le plaisir de vous présenter – au nom des partenaires concernés – le Guide sur les stratégies nationales en matière de cybersécurité, visant à fournir un ensemble agrégé et harmonisé de principes et de bonnes pratiques pour l'élaboration, l'établissement et la mise en oeuvre de stratégies nationales en matière de cybersécurité.

Sous la houlette de l'UIT, douze partenaires des secteurs public et privé, des milieux universitaires et de la société civile ont accepté de partager leur expérience, leurs connaissances et leur expertise pour produire le présent Guide, qui rassemble le savoir-faire existant des organisations participantes et fournit des références de publications complémentaires, pour faciliter l'accès aux ressources disponibles.

Au cours des deux dernières décennies, des milliards de personnes dans le monde ont bénéficié de la croissance exponentielle et de l'adoption rapide des technologies de l'information et de la communication ainsi que des opportunités économiques et sociales qui en découlent. Nous assistons à une révolution numérique qui transforme profondément nos sociétés.

La cybersécurité est un facteur fondamental dans la réalisation du développement socioéconomique. Pourtant, seuls soixante-seize pays[1] dans le monde possèdent publiquement une stratégie nationale en matière cybersécurité. Il est donc impératif d'intensifier les efforts dans ce domaine. Ce Guide – comme son tire le suggère – a pour vocation de susciter une réflexion stratégique et d'aider les dirigeants nationaux et les décideurs politiques à élaborer, à établir et à mettre en oeuvre des stratégies nationales en matière de cybersécurité.

Je suis convaincu que ce Guide sur les stratégies nationales de cybersécurité constituera un outil utile pour toutes les parties prenantes ayant des responsabilités en matière de cybersécurité. Je tiens personnellement à exprimer ma gratitude aux partenaires pour leur soutien constant et précieux et leur engagement à faire de ce projet un grand succès témoignant ainsi de la mise en place d'une collaboration multipartite réussie.

Brahima Sanou
Directeur, Bureau de développement des télécommunications de l'UIT

[1] Selon l'Indice de cybersécurité dans le monde (GCI) 2017.

Table des matières

Préface

Ce Guide sur les stratégies nationales de cybersécurité brosse un panorama aussi exhaustif que possible des stratégies efficaces en matière de cybersécurité. Il est le fruit d'une initiative multiparties prenantes, menée dans l'équité et la collaboration, et tire parti des connaissances, de l'expérience et de l'expertise de nombreuses organisations dans le domaine des stratégies et politiques nationales relatives à la cybersécurité. Plus précisément, ce Guide a été élaboré par douze partenaires des secteurs public et privé, ainsi que par les milieux universitaires et la société civile.

Les partenaires se sont rendu compte de la nécessité de renforcer la coopération et la coordination au sein de la communauté internationale en ce qui concerne le renforcement des capacités de cybersécurité. Des efforts ont donc été déployés pour soutenir les dirigeants et les décideurs nationaux dans le développement de réponses défensives aux cyber-menaces, sous la forme d'une stratégie nationale de cybersécurité, et dans leurs réflexions stratégiques en matière de cybersécurité, de cyberpréparation, d'intervention et de résilience de même que concernant l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC).

Le présent Guide sur les stratégies nationales de cybersécurité a été élaboré selon une approche itérative, visant à parvenir à un accord par la recherche d'un consensus. Il se fonde sur les ressources existantes et vise à faciliter son utilisation par les parties prenantes nationales. A chaque fois que cela est possible, les sources et outils pertinents utilisés pour élaborer chaque ensemble de recommandations sont énumérés dans la Section Documents de référence, pour permettre une utilisation plus large.

La cybersécurité est un élément fondamental qui sous-tend la réalisation des objectifs socio-économiques des économies modernes. Il faut espérer que ce Guide sur les stratégies nationales de cybersécurité servira d'outil de référence pour toutes les parties prenantes, y compris les décideurs nationaux, les législateurs et les régulateurs ayant des responsabilités en matière de cybersécurité. Son champ d'application peut néanmoins être élargi, dans la mesure où les concepts introduits peuvent être appliqués aux niveaux régional ou municipal et adaptés pour l'industrie.

1 Aperçu général du document

1.1 Objet

Le présent document a pour objet d'aider les dirigeants et les décideurs nationaux à élaborer une stratégie nationale de cybersécurité et à développer une réflexion stratégique en matière de cybersécurité, de cyberpréparation et de résilience.

Ce Guide vise à fournir un cadre utile, souple et convivial pour définir le contexte de la vision socio-économique et de la situation de sécurité actuelle d'un pays et pour aider les décideurs politiques à élaborer une stratégie qui tienne compte de la situation spécifique du pays ainsi que de ses valeurs socioculturelles et qui encourage le développement de sociétés sûres, résilientes, axées sur les TIC et connectées.

Il constitue une ressource unique en son genre, car il fournit un cadre approuvé par des organisations possédant une expérience démontrée et diversifiée dans ce domaine et s'appuie sur leurs travaux antérieurs dans ce domaine. De ce fait, il brosse un panorama le plus complet possible des stratégies efficaces en matière de cybersécurité.

1.2 Portée

La cybersécurité représente un défi complexe qui englobe plusieurs aspects différents, liés à la gouvernance, à la politique, à l'exploitation, à la technique et au juridique.

Ce Guide tente d'aborder, d'organiser et de hiérarchiser nombre de ces domaines, en fonction de modèles, de cadres et d'autres références bien établis qui existent déjà. Il cible la protection des aspects civils du cyberespace et, en tant que tel, souligne les principes généraux et les bonnes pratiques à prendre en compte lors de l'élaboration, du déploiement et de la gestion d'une stratégie nationale de cybersécurité.

A cette fin, il établit une distinction claire entre la «procédure», qui sera adoptée par les pays durant le cycle de vie d'une stratégie nationale de cybersécurité (lancement, inventaire et analyse, production, mise en oeuvre, examens), et le «contenu», à savoir le texte actuel à figurer dans un document de stratégie nationale de cybersécurité. Le Guide ne couvre pas certains cas spécifiques tels que le développement de cybercapacités défensives ou offensives par les forces

de défense miliaire ou les services de renseignement d'un pays, quand bien même nombre de pays auraient développé de telles capacités.

Afin de fournir de bonnes pratiques sur ce qui devrait être inclus dans une stratégie nationale de cybersécurité, ainsi que sur la manière de l'élaborer, de la mettre en oeuvre et de la réviser, le présent Guide traite de ces deux aspects à la fois.

Le Guide fournit également une vue d'ensemble des principales composantes que les pays devront prendre en compte pour se préparer en termes de cybersécurité, en soulignant les aspects critiques que les gouvernements sont appelés à prendre en considération lorsqu'ils établissent leur stratégie nationale et leur plan de mise en oeuvre.

Enfin, le Guide offre aux décideurs un aperçu global et de haut niveau des approches et applications existantes et fournit une référence à des ressources supplémentaires et complémentaires visant à informer des efforts spécifiquement déployés au niveau national en matière de cybersécurité.

1.3 Structure générale et utilisation du Guide

Le présent Guide a été structuré principalement comme une ressource, pour aider les intervenants du secteur public à préparer, rédiger et gérer leur stratégie nationale de cybersécurité.

De ce fait, son contenu est organisé de façon à pouvoir suivre la procédure et les différentes phases de développement d'une stratégie:

- Section 2 – Introduction: présente le contenu du guide avec les définitions correspondantes;
- Section 3 – Cycle de vie du développement de la stratégie: détaille les étapes du développement d'une stratégie et de sa gestion pendant tout son cycle de vie;
- Section 4 – Principes généraux d'une stratégie: souligne les considérations transversales et fondamentales à prendre en compte lors de l'élaboration d'une stratégie;
- Section 5 – Domaines d'intervention et bonnes pratiques: identifie les éléments clés et les sujets à prendre en compte lors de l'élaboration d'une stratégie; et
- Section 6 – Documents de référence complémentaires: fournit des indications supplémentaires sur la littérature pertinente que les parties prenantes peuvent examiner dans le cadre du processus de rédaction.

Notons que la Section 3 traite du processus et des aspects liés à l'élaboration d'une stratégie nationale de cybersécurité (tels que la préparation, l'élaboration, la mise en oeuvre et la durabilité sur le long terme), tandis que les Sections 4 et 5 sont davantage axées sur le contenu de la stratégie en mettant en avant les concepts et les éléments que le document doit contenir.

1.4 Destinataires

Le présent guide est avant tout destiné aux décideurs politiques responsables de l'élaboration d'une stratégie nationale en matière de cybersécurité. Il cible en second lieu toutes les autres parties prenantes des secteurs public et privé impliquées dans le développement et la mise en oeuvre d'une stratégie, par exemple les fonctionnaires compétents, les autorités de réglementation, les forces de police, les fournisseurs de TIC, les opérateurs d'infrastructures essentielles, la société civile, les universités et instituts de recherche. Ce Guide pourrait également être utile aux différents acteurs de la communauté internationale du développement, qui fournissent une assistance en matière de cybersécurité.

2 Introduction

Au cours des deux dernières décennies, des milliards de personnes dans le monde ont bénéficié de la croissance exponentielle et de l'adoption rapide des technologies de l'information et de la communication, ainsi que des opportunités économiques et sociales qui en découlent.

Depuis sa création, l'Internet est passé d'une plate-forme d'échange d'informations à ce qui constitue aujourd'hui le dorsal des entreprises modernes, des services et infrastructures essentiels, des réseaux sociaux et de l'économie mondiale dans son ensemble. En conséquence, les dirigeants nationaux ont commencé à lancer des stratégies numériques et à financer des projets qui augmentent la connectivité Internet et qui tirent parti des avantages découlant de l'utilisation des TIC pour stimuler la croissance économique, accroître la productivité et l'efficacité, améliorer la prestation et la capacité de services, fournir un accès aux entreprises et à l'information, permettre l'apprentissage en ligne, améliorer les compétences de la main-d'oeuvre et promouvoir la bonne gouvernance. Les pays ne peuvent pas ignorer les opportunités associées à leur implication dans l'économie de l'Internet.

Alors que nos sociétés s'appuient de plus en plus sur l'infrastructure numérique, la technologie reste intrinsèquement vulnérable. La confidentialité, l'intégrité et la disponibilité de l'infrastructure informatique sont mises à l'épreuve par les cybermenaces qui évoluent à un rythme soutenu, notamment la fraude électronique, le vol de données de propriété intellectuelle et d'identité, la perturbation du service, ainsi que les dommages ou la destruction de biens. Le pouvoir de transformation des TIC et de l'Internet, en tant que catalyseurs de la croissance économique et du développement social, est arrivé à un point critique où la confiance des citoyens et des pays à l'égard de l'utilisation des TIC se trouve érodée par la cyber-insécurité.

Pour exploiter pleinement le potentiel de la technologie, les Etats doivent aligner leurs visions économiques nationales sur leurs priorités en matière de sécurité nationale. Si les risques de sécurité associés à la prolifération d'infrastructures TIC et d'applications Internet ne sont pas adéquatement réduits par des stratégies nationales globales de cybersécurité et des plans de résilience, les pays ne pourront pas réaliser la croissance économique et les objectifs de sécurité nationale qu'ils recherchent.

En réponse à cette situation, les pays développent des capacités offensives et défensives leur permettant de se défendre contre les activités illicites et illégales dans le cyberespace et de prévenir les incidents pour éviter tout préjudice. Ce document examinera spécifiquement les réponses défensives, en particulier sous la forme de stratégies nationales de cybersécurité.

Le développement et la mise en oeuvre d'une stratégie nationale de cybersécurité permet à un pays de renforcer la sécurité de son infrastructure numérique et in fine aide à la réalisation de ses aspirations socio-économiques plus larges. Les dirigeants nationaux doivent se montrer stratégiques face aux opportunités et aux risques que fait émerger l'environnement numérique pour leurs pays; ils doivent également définir clairement l'avenir numérique qu'ils entendent créer.

2.1 Qu'est-ce que la cybersécurité?

Plusieurs définitions du terme «cybersécurité» ont été établies aux niveaux national et international. Aux fins du présent document, on entend par «cybersécurité» l'ensemble des outils, politiques, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger la disponibilité, l'intégration et la confidentialité des actifs dans les infrastructures connectées du gouvernement, des organisations privées et des utilisateurs; ces actifs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication et les données dans le cyberenvironnement[1].

2.2 Avantages d'une stratégie nationale de cybersécurité et processus d'élaboration de la stratégie

Les stratégies nationales de cybersécurité peuvent revêtir diverses formes et comporter différents niveaux de détails, selon les objectifs spécifiques du pays et le niveau de préparation en matière de cybersécurité. Il n'existe donc pas de définition établie et communément admise de ce que recouvre la notion de stratégie nationale de cybersécurité.

S'appuyant sur les recherches existantes dans ce domaine, le présent document encourage les parties prenantes à envisager une stratégie nationale de cybersécurité comme étant:

- une expression de la vision, des objectifs de haut niveau, des principes et des priorités qui guident un pays dans la lutte contre la cybersécurité;
- une vue d'ensemble des parties prenantes chargées d'améliorer la cybersécurité du pays, de leurs rôles et responsabilités respectifs; et
- une description des étapes, programmes et initiatives qu'un pays s'emploiera à suivre pour protéger sa cyber-infrastructure nationale et, par là même, accroître sa sécurité et sa résilience.

[1] Définition adaptée de https://www.bcmpedia.org/wiki/Cyber_Security.

Le fait de définir une vision, des objectifs et des priorités permet aux gouvernements d'envisager la cybersécurité de manière globale comme faisant partie intégrante de leur écosystème numérique national, plutôt que de se concentrer sur un secteur particulier, un objectif ou une réponse à un risque spécifique - ils peuvent dès lors jouer la carte de la stratégie. Les priorités en matière de stratégies nationales de cybersécurité varient d'un pays à l'autre. Ainsi, un pays pourra cibler les risques critiques liés aux infrastructures, tandis que d'autres choisiront de protéger la propriété intellectuelle, de promouvoir la confiance dans l'environnement en ligne ou de sensibiliser le grand public à la cybersécurité voire traiteront plusieurs thématiques simultanément.

Il est nécessaire d'identifier et de hiérarchiser a posteriori les investissements et les ressources pour gérer avec succès les risques dans un domaine aussi vaste que la cybersécurité.

Une stratégie nationale de cybersécurité offre également la possibilité d'aligner les priorités en matière de cybersécurité sur d'autres objectifs liés aux TIC. La cybersécurité est essentielle à la réalisation des objectifs socio-économiques des économies modernes et la stratégie doit refléter la manière dont ces objectifs sont soutenus. Une solution consiste à se référer aux politiques existantes visant à mettre en oeuvre les agendas numériques ou programmes de développement des pays ou à évaluer comment la cybersécurité peut être intégrée à ces agendas ou programmes.

Enfin, le processus d'élaboration de la stratégie nationale de cybersécurité devrait traduire la vision du gouvernement dans des politiques cohérentes et réalisables qui l'aideront à atteindre ses objectifs. Cela comprend non seulement les étapes, programmes et initiatives à mettre en place, mais également les ressources allouées à ces efforts et la manière dont ces ressources doivent être utilisées. De même, le processus devrait identifier les paramètres à utiliser pour s'assurer que les résultats souhaités soient atteints dans les délais et budgets impartis.

3 Cycle de vie d'une stratégie nationale de cybersécurité

La présente Section fournit une vue d'ensemble des différentes phases de développement d'une stratégie nationale de cybersécurité, comprenant notamment:

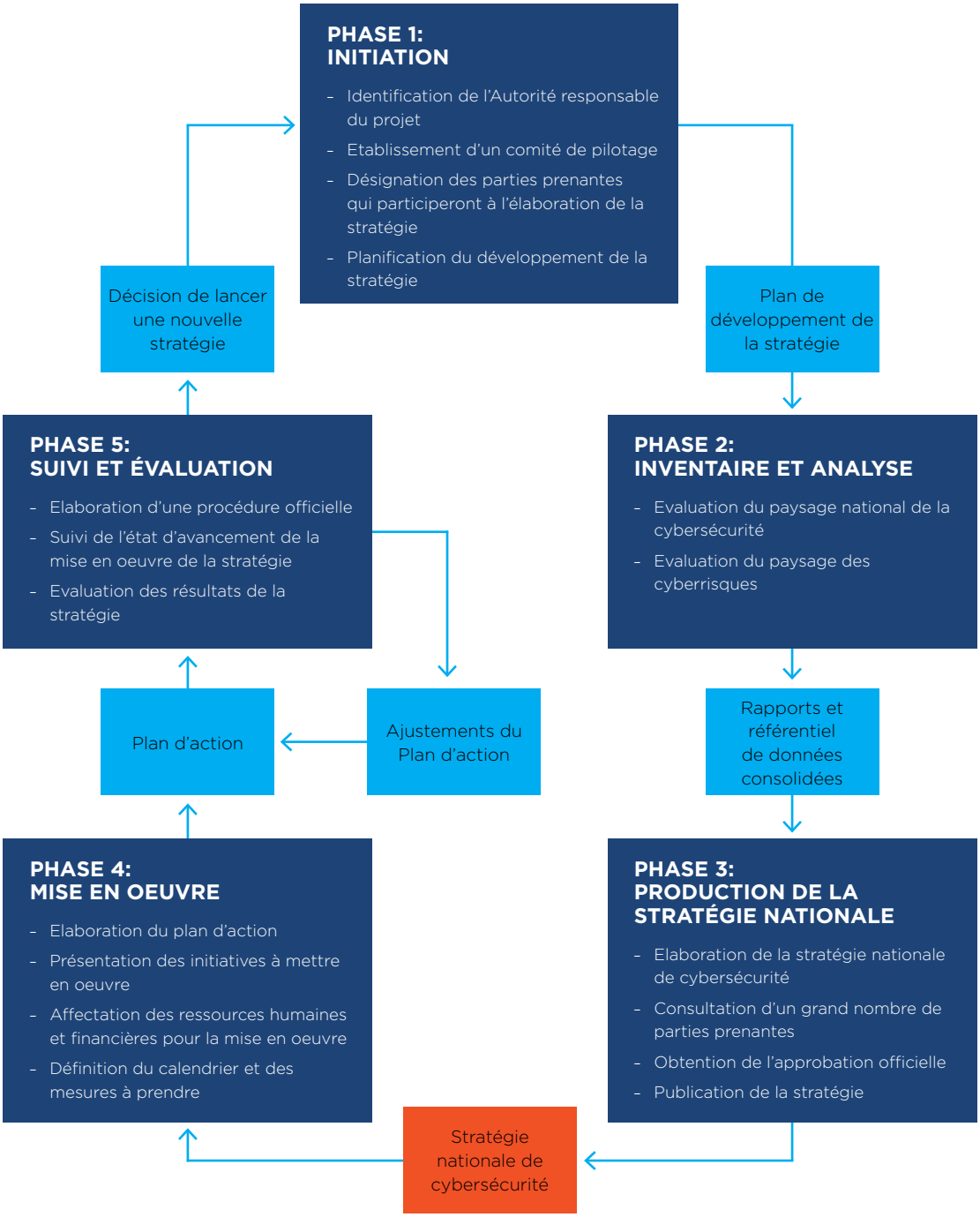
- Phase I – Lancement
- Phase II – Inventaire et analyse
- Phase III – Production
- Phase IV – Mise en oeuvre
- Phase V – Suivi et évaluation

Cette Section présente également les entités clés qui devraient participer à l'élaboration de la stratégie ainsi que d'autres parties prenantes concernées susceptibles de contribuer au processus.

Enfin, cette Section a pour objectif de permettre aux lecteurs de mieux comprendre les mesures mises en place par un pays aux fins de l'élaboration d'une stratégie nationale de même que les mécanismes possibles de mise en oeuvre selon les besoins et exigences spécifiques du pays, en intégrant les principes généraux (décrits à la Section 4) et les bonnes pratiques (décrites à la Section 5).

Ce cycle de vie, tel qu'illustré à la Figure 1, guide la réflexion stratégique des utilisateurs du présent document en ce qui concerne la cybersécurité au niveau national.

***Figure 1** – Cycle de vie d'une stratégie nationale de cybersécurité*



3.1 Phase I: Lancement

Conformément aux Sections 4 et 5 du présent document, la phase de lancement d'une stratégie nationale de cybersécurité pose les fondations d'un développement efficace. Cette phase porte normalement sur les processus, les délais et l'identification des principales parties prenantes appelées à jouer un rôle dans l'élaboration de la stratégie. Elle débouche sur la réalisation d'un plan de développement de la stratégie. Lorsque la procédure de gouvernance du pays le prévoit, le plan peut requérir l'approbation de l'organe exécutif du pays.

3.1.1 Identification de l'Autorité responsable du projet

Le processus d'élaboration de la stratégie devrait être coordonné par une seule et même autorité compétente, conformément au principe qui consiste à définir clairement l'encadrement, les rôles et l'attribution des ressources (Section 4.8). L'organe exécutif a pour mission de nommer une entité publique préexistante ou nouvellement créée, telle qu'un ministère, une agence ou un département, pour piloter l'élaboration de la stratégie. Cette entité, désignée dans le présent document sous le nom d'Autorité responsable du projet, doit à son tour nommer une personne responsable et redevable du processus d'élaboration de la stratégie.

L'Autorité responsable du projet doit rester neutre tout au long du processus d'élaboration. A cette fin, il est recommandé que cette entité soit différente de celle(s) responsable(s) de la mise en oeuvre de la stratégie. Ce mécanisme ou d'autres procédures devraient être adoptés pour surmonter tout préjugé inhérent et éviter la concurrence intragouvernementale pour les ressources.

3.1.2 Etablissement d'un comité de pilotage

L'organe exécutif est également tenu de constituer un comité de pilotage chargé de collaborer avec l'Autorité responsable du projet au développement de la stratégie. Il doit être habilité à fournir des conseils et à jouer un rôle dans l'assurance de la qualité. Enfin, il doit garantir la transparence et le caractère inclusif de la procédure, selon le principe qui consiste à définir clairement l'encadrement, les rôles et l'attribution des ressources (Section 4.8). Le rôle, la structure et la composition du comité de pilotage doivent être clairement définis dès le départ.

Le comité de pilotage sera constitué en conséquence, sachant qu'il pourra être amené à examiner des documents confidentiels. Il est également important que sa composition reflète les diverses responsabilités conférées à cet organe, par exemple au travers de l'ancienneté des nominations.

3.1.3 Désignation des parties prenantes qui participeront à l'élaboration de la stratégie

Lors de cette étape, l'Autorité responsable du projet doit désigner une première série de parties prenantes qui participeront à l'élaboration de la stratégie. Elle vérifiera également les rôles des différentes parties prenantes et passera en

revue les modalités de leur collaboration pour gérer les attentes tout au long du processus.

Sur la période concernée, l'Autorité responsable du projet pourra être amenée à contacter d'autres parties prenantes pour s'assurer que toutes les connaissances et compétences pertinentes sont utilisées. Cela prendrait en compte le principe relatif à une approche inclusive (Section 4.3), qui souligne l'importance de la coopération avec un éventail de parties prenantes au sein du gouvernement, du secteur privé et de la société civile. Par exemple, l'Autorité responsable du projet pourrait envisager d'inclure les entreprises TIC, les opérateurs d'infrastructures essentielles, les experts du monde universitaire et les organisations non gouvernementales oeuvrant, entre autres, à l'amélioration de la sensibilisation et de l'état de préparation en matière de cybersécurité.

Ce mécanisme de coopération pourrait prendre la forme d'un comité consultatif qui contribuerait à la composition du comité de pilotage et qui serait également consulté sur les différentes phases.

3.1.4 Planification du développement de la stratégie

3La dernière étape de la phase de lancement consiste en la rédaction d'un plan de développement de la stratégie nationale en matière de cybersécurité par l'Autorité responsable du projet. Une fois rédigé, ce plan sera soumis, s'il y a lieu, au comité de pilotage et à l'organe exécutif pour approbation, conformément aux procédures nationales de gouvernance.

Lors de sa rédaction, l'Autorité responsable du projet devra également déterminer si la stratégie nationale de cybersécurité prendra la forme d'une législation ou d'une politique, sachant que le choix retenu pourra influer sur les procédures officielles à suivre de même que sur l'échéancier à adopter.

Le plan de développement de la stratégie doit identifier les principales étapes et activités, les parties prenantes clés, les échéanciers et les ressources nécessaires. Il doit spécifier comment et quand les parties prenantes concernées devront participer au processus de développement pour apporter leur contribution et leurs commentaires.

Il doit également préciser quelles sont les ressources humaines et financières nécessaires et où les trouver. Par exemple, une expertise peut être sollicitée auprès des organisations intergouvernementales, du secteur privé, des universités ou des organismes de développement. De même, les besoins de financement peuvent être satisfaits par la réaffectation de sources de financement dédiées dans les budgets existants ou par de nouveaux financements disponibles auprès de tierces parties (par exemple, des organisations internationales).

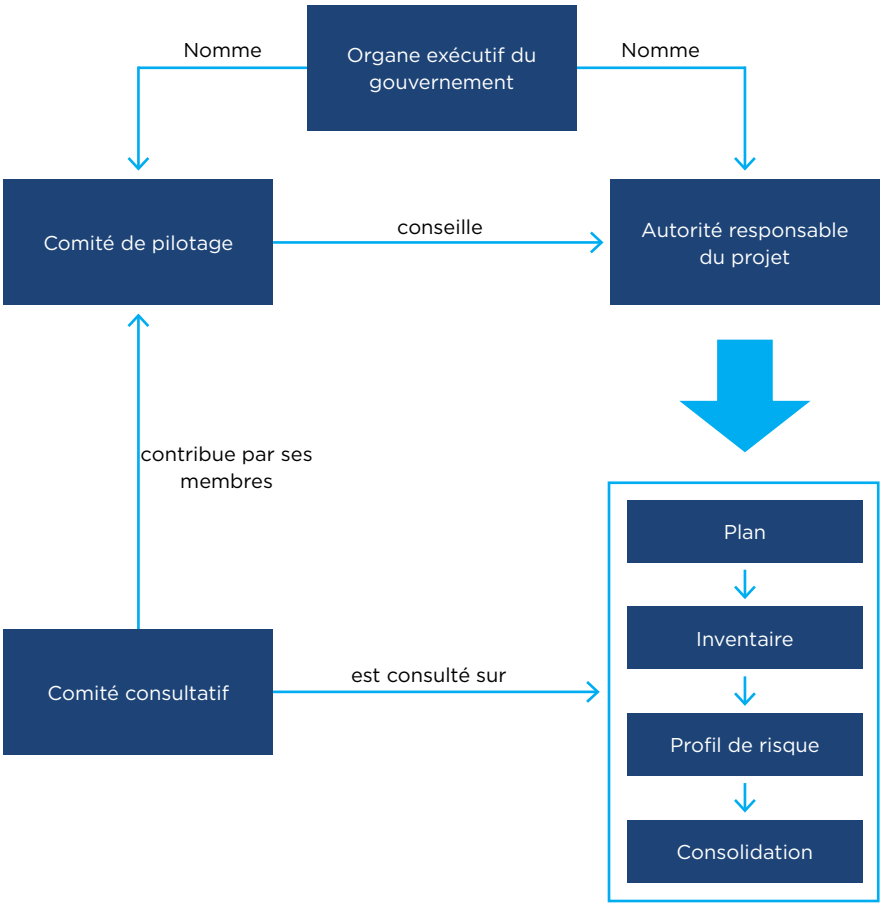
Une attention particulière sera portée à la sûreté du financement à long terme sur toute la durée du cycle de vie de la stratégie nationale de cybersécurité, y compris sur les phases de développement, de mise en oeuvre et de perfectionnement. Pour plus de détails sur l'affectation des ressources aux fins de la mise en oeuvre,

voir «Affectation des ressources humaines et financières pour la mise en oeuvre» (Section 3.4.3) et pour plus de détails sur le financement à long terme, voir «Affecter le budget et les ressources spécifiques» (Section 5.1.5).

La Figure 2 montre les interactions possibles et la répartition des rôles entre les différentes parties prenantes et les différents comités.

De plus amples informations sont fournies à la page 55.

***Figure 2** – Parties prenantes*



3.2 Phase II: Inventaire et analyse

Le but de cette phase est de collecter des données pour évaluer le paysage national de la cybersécurité ainsi que le paysage actuel et futur du cyberrisque, afin de guider l'élaboration et le développement de la stratégie nationale de cybersécurité. L'exercice devrait être suivi par la rédaction d'un rapport donnant un aperçu de la posture stratégique nationale de cybersécurité et de l'environnement en matière de risques, qui sera présenté au comité de pilotage.

Avant d'entamer la production du texte de la stratégie, l'Autorité responsable du projet doit analyser et évaluer avec soin les informations recueillies au cours de la phase d'inventaire pour s'assurer que les déficits de capacité en matière de cybersécurité soient identifiés et que les options pour y remédier soient présentées. L'analyse devrait déboucher sur la réalisation d'une évaluation afin de montrer dans quelle mesure les dispositifs politiques, réglementaires et opérationnels existants satisfont aux objectifs énoncés relatifs à la stratégie et de mettre en lumière les domaines où ce n'est pas le cas.

Elle devrait être également utilisée pour identifier des problèmes clés spécifiques, tels que les lacunes en matière d'éducation et de formation.

Enfin, l'analyse devrait aboutir à une évaluation de tous les résultats pertinents et escomptés de la stratégie ainsi que des résultats et effets possibles des moyens choisis.

De plus amples informations sont fournies à la page 55.

3.2.1 Evaluation du paysage national de la cybersécurité

La stratégie nationale de cybersécurité, pour être efficace, doit refléter la posture du pays en matière de cybersécurité. A cette fin, il convient d'analyser les forces et les faiblesses existantes du pays en la matière et de consulter les matériels et documents pertinents en collaboration avec les parties prenantes concernées, au sein des gouvernements, du secteur privé et de la société civile. Cette étape devra tenir compte du principe de l'approche globale et des priorités ciblées (voir la Section 4.2).

L'Autorité responsable du projet doit par conséquent identifier les actifs et les services essentiels au bon fonctionnement de la société et de l'économie et répertorier les lois, règlements, politiques, capacités et programmes existants liés à la cybersécurité. L'Autorité responsable du projet doit également identifier les mécanismes de réglementation «douce» en vigueur tels que les partenariats public-privé et prendre la mesure des capacités qui ont été développées pour faire face aux problèmes de cybersécurité, à l'instar des équipes nationales d'intervention en cas d'incident informatique (CIRT). Qui plus est, les rôles et responsabilités des agences publiques existantes dotées d'un mandat en matière de cybersécurité, tels que les régulateurs ou les agences de protection des données, doivent être identifiés et répertoriés.

En outre, les données susceptibles de renseigner sur la posture de cybersécurité du pays doivent être collectées. Peuvent être concernés à ce titre les informations sur les programmes de cybersécurité existants au niveau national, les initiatives internationales, les projets du secteur privé, les TIC, la cyber-éducation et les programmes de développement des compétences, les cyber-initiatives de la R&D, les données sur la pénétration de l'Internet et les taux d'infection, l'adoption des TIC, les développements technologiques et les réflexions sur les futures tendances et menaces en matière de TIC et de cybersécurité.

Les informations pertinentes fournies par le secteur privé, les instituts de recherche et d'autres groupes de parties prenantes devraient également être incluses dans cette analyse. Il est aussi indispensable pour les pays en développement de prévoir des initiatives de collaboration avec des partenaires de développement pour coordonner l'assistance technique et les investissements.

Enfin, l'Autorité responsable du projet doit examiner les informations analogues aux niveaux régional et international et analyser les stratégies et initiatives propres au secteur.

3.2.2 Evaluation du paysage du cyberrisques

S'appuyant sur les informations collectées lors de l'étape précédente, l'Autorité responsable du projet doit évaluer le risque encouru par le pays du fait de la dépendance vis-à-vis du numérique. Ce peut être fait via l'identification des actifs numériques nationaux – publics et privés – de leurs interdépendances, vulnérabilités et menaces et via l'estimation de la probabilité et de l'impact potentiel d'un cyberincident.

Ces efforts tiennent compte du principe de gestion des risques et de résilience (Section 4.6), reconnaissant le caractère essentiel de la gestion des risques pour tirer pleinement parti des avantages de l'environnement numérique pour le développement socio-économique. Pour finir, l'évaluation des risques initiale pourrait constituer le fondement de futures estimations de risques plus spécifiques (de plus amples informations sur le principe de gestion des risques et de résilience et sur les modalités de conduite des évaluations de risques sont fournies à la Section 5.2).

3.3 Phase III: Production de la stratégie nationale de cybersécurité

Cette phase consiste à élaborer le texte de la stratégie en faisant participer les intervenants clés du secteur public, du secteur privé et de la société civile à travers une série de consultations publiques et de groupes de travail. Ce groupe élargi de parties prenantes, coordonné par l'Autorité responsable du projet, sera chargé

de définir la vision globale et la portée de la stratégie, en fixant des objectifs de haut niveau, en faisant l'inventaire de la situation actuelle (détaillé dans la Phase II), en hiérarchisant les objectifs en termes d'impact sur la société, les citoyens et l'économie, et en garantissant les ressources financières nécessaires. Cette phase intègre également la prise en compte des principes transversaux (Section 4) et des éléments de bonne pratique (Section 5), détaillés dans ce Guide

3.3.1 Elaboration de la stratégie nationale de cybersécurité

A l'issue de la phase d'inventaire et d'analyse, l'Autorité responsable du projet se lance dans l'élaboration de la stratégie, en collaboration avec le comité de pilotage. Des groupes de travail dédiés peuvent être créés pour travailler sur des sujets spécifiques ou rédiger différentes sections de la stratégie, conformément aux processus établis lors de la phase de lancement et les adapter au besoin.

La stratégie doit fournir l'orientation générale en matière de cybersécurité pour le pays, exprimer une vision et une portée claires, fixer les objectifs à atteindre dans un délai précis et prioriser ceux-ci en termes d'impact sur la société, l'économie et les infrastructures. Elle doit également identifier les actions possibles, encourager les efforts de mise en oeuvre et piloter l'allocation des ressources nécessaires pour soutenir toutes ces activités. Enfin, la stratégie peut inclure certains résultats obtenus lors de la phase d'inventaire et d'analyse.

De même que pour l'étape consacrée à la planification du développement de la stratégie, il s'agit de formuler ici un cadre de gouvernance clair (Section 5.1), qui définit les rôles et les responsabilités des principales parties prenantes. Il est nécessaire, à ce stade, de nommer une entité responsable de la gestion et de l'évaluation de la stratégie et une entité responsable de la gestion et de la mise en oeuvre au niveau global, à l'instar de l'autorité centrale ou du conseil national de cybersécurité.

La stratégie doit en outre définir ou confirmer le mandat des différentes entités responsables de l'élaboration et du développement des politiques et réglementations de cybersécurité dans le pays. Elle doit aussi définir les responsabilités et les tâches des entités chargées de collecter les informations sur les menaces et les vulnérabilités, de réagir aux cyber-incidents (p. ex. équipes nationales CIRT), de renforcer les activités de préparation et de gérer les crises. Enfin, la stratégie doit veiller à expliquer clairement la façon dont toutes ces entités interagissent les unes avec les autres et avec l'autorité centrale.

3.3.2 Consultation d'un grand nombre de parties prenantes

Comme nous l'avons mentionné ci-avant, il est essentiel d'impliquer des parties prenantes pour le succès de la stratégie. Afin de s'assurer que la stratégie finale repose bien sur une vision commune, le projet de document devrait être diffusé auprès d'un vaste groupe de parties prenantes qui ne se limite pas aux personnes impliquées dans le processus d'élaboration de la stratégie. Cela peut se faire par

le biais de divers engagements, notamment de consultations en ligne, d'ateliers de validation et de groupes de travail supplémentaires. Les commentaires et feedbacks résultant de ce processus devraient être utilisés pour finaliser la stratégie.

3.3.3 Obtention de l'approbation officielle

Lors de la dernière étape du développement de la stratégie, l'Autorité responsable du projet devra s'assurer que la stratégie est officiellement adoptée par l'organe exécutif. La procédure d'adoption officielle varie selon les pays et dépend de la façon dont la stratégie est définie dans le cadre législatif. Celle-ci peut, par exemple, avoir été adoptée au moyen d'une procédure parlementaire ou d'un décret gouvernemental.

Il est par ailleurs essentiel que la stratégie ne soit pas développée seulement avec l'approbation des plus hautes instances gouvernementales, et que cet engagement se poursuive également pendant la phase de mise en oeuvre. Les responsables concernés devraient être tenus responsables de leurs actes et être soutenus à la fois par leur capital politique et par leurs ressources.

3.3.4 Publication de la stratégie

La stratégie est un document public qui devrait être aisément disponible. Cette grande disponibilité garantit que les priorités et objectifs du gouvernement en matière de cybersécurité sont connus du grand public et appuie tous les efforts visant à sensibiliser davantage à la cybersécurité. Si la stratégie s'accompagne d'un plan d'action, ce dernier mentionnera d'autres possibilités de renforcer l'engagement et la coopération avec la société civile et le secteur privé.

De plus amples informations sont fournies à la page 55.

3.4 Phase IV: Mise en oeuvre

La phase de mise en oeuvre est l'élément le plus important du cycle de vie global de la stratégie nationale de cybersécurité. La mise en place d'une approche structurée de la mise en oeuvre, appuyée par des ressources humaines et financières adéquates, est essentielle au succès de la stratégie et doit être considérée comme faisant partie de son développement. La phase de mise en oeuvre repose souvent sur un plan d'action, qui guide les différentes activités envisagées.

3.4.1 Développement du plan d'action

Comme pour l'élaboration de la stratégie, la phase de mise en oeuvre ne peut être confiée à une seule autorité. Elle nécessite l'engagement et la coordination d'un grand nombre de parties prenantes au gouvernement ainsi que le soutien de la société civile et du secteur privé. Le plan d'action, élaboré selon le principe de la définition claire de l'encadrement, des rôles et de l'attribution des ressources (Section 4.8), peut soutenir la mise en oeuvre efficace de la stratégie.

Le développement du plan d'action est presque aussi important que le plan lui-même. La procédure, orchestrée par l'Autorité responsable du projet, devrait permettre de réunir les parties prenantes concernées pour les amener à s'entendre sur les objectifs et les résultats ainsi que pour coordonner et mettre en commun les ressources.

3.4.2 Présentation des initiatives à mettre en oeuvre

La stratégie nationale de cybersécurité présente les objectifs du gouvernement et les résultats attendus dans les différents domaines d'action identifiés. Dans le plan d'action, l'Autorité responsable du projet ciblera les initiatives spécifiques pour chacun de ces domaines qui contribueront à la réalisation des objectifs, en coordination avec les parties prenantes concernées. Citons, à titre d'exemple, l'organisation d'exercices de cybersécurité, l'établissement de références de base pour la sécurité des infrastructures essentielle ou la mise en place d'un cadre de rapport des incidents.

Le calendrier et les efforts nécessaires à la mise en oeuvre de ces initiatives doivent être hiérarchisés en fonction de leur criticité pour veiller à ce que les ressources limitées soient mobilisées de manière appropriée. A cette fin, il pourra être utile de consulter les résultats de la Phase II (Inventaire et analyse), notamment en ce qui concerne l'»Evaluation du paysage national de la cybersécurité» (Section 3.2.2).

3.4.3 Affectation des ressources humaines et financières pour la mise en oeuvre

Une fois les initiatives prioritaires identifiées, l'Autorité responsable du projet doit définir des entités gouvernementales spécifiques comme propriétaire de chacune de ces initiatives. Ces entités gouvernementales seront à leur tour responsables et redevables de la mise en oeuvre de chaque initiative spécifique qui leur sera confiée et devront coordonner leurs efforts avec ceux des autres parties prenantes concernées dans le cadre de la procédure de mise en oeuvre.

Afin de s'assurer que ces entités puissent fournir les résultats attendus, l'Autorité responsable du projet doit évaluer si ces dernières ont ou non reçu un mandat approprié – légal ou autre – pour la mise en oeuvre. L'Autorité responsable du projet doit également collaborer avec les propriétaires des initiatives spécifiques

pour évaluer les ressources nécessaires à la réalisation des tâches. Cette évaluation doit aborder la question des ressources humaines, de l'expertise et du financement. L'Autorité responsable du projet doit donc collaborer avec les propriétaires pour les aider à identifier et à sécuriser les ressources requises en conformité avec les structures administratives et financière du pays.

3.4.4 Définition du calendrier et des mesures à prendre

Le dernier élément essentiel du plan d'action consiste en la mise en place de mesures spécifiques et d'indicateurs clés de performance pour évaluer chacune des actions entreprises, par exemple si le pays a mené une campagne de sensibilisation sur l'importance du partage d'informations, organisé et exécuté un exercice de cybersécurité avec le secteur des infrastructures essentielles ou promulgué une loi sur les exigences de base en matière de sécurité. Des échéances spécifiques pour la mise en oeuvre seront également définies.

Les mesures spécifiques et les indicateurs clés de performance seront élaborés par l'Autorité responsable du projet en collaboration avec les propriétaires respectifs. Ces derniers devraient être encouragés à définir et à maintenir un ensemble plus détaillé de mesures pour faciliter l'évaluation de l'efficacité des actions menées pendant et après l'achèvement.

De plus amples informations sont fournies à la page 55.

3.5 Phase V: Suivi et évaluation

Lors de cette phase, une autorité compétente sera chargée d'élaborer une procédure officielle de suivi et d'évaluation de la stratégie. En matière de suivi, le gouvernement veillera à ce que la stratégie soit mise en oeuvre selon le plan d'action. En matière d'évaluation, le gouvernement et son autorité compétente jugeront de la pertinence de la stratégie en fonction de l'évolution des risques et de l'adéquation de cette dernière avec les objectifs du gouvernement et détermineront les ajustements nécessaires.

3.5.1 Elaboration d'une procédure officielle

Afin de garantir un suivi et une évaluation efficaces de la mise en oeuvre de la stratégie, le gouvernement devra désigner une entité indépendante responsable du suivi et de l'évaluation des progrès et de l'efficacité de la mise en oeuvre. Cette entité devrait idéalement participer à l'adoption de mesures de suivi et d'évaluation pour la mise en oeuvre de la stratégie ainsi que du plan d'action et des initiatives associés, laquelle devrait intervenir pendant les phases de production et de lancement.

Les mécanismes de gouvernance mis en place par les pays devraient inclure le suivi et la mesure de la performance de même que de l'exécution réussie du plan de mise en oeuvre de la stratégie. L'évaluation continue du plan de mise en oeuvre (à savoir l'analyse de ce qui fonctionne et de ce qui ne fonctionne pas) permet d'orienter la stratégie. Les mécanismes de bonne gouvernance relatifs à la mise en oeuvre de la stratégie devraient aussi clairement définir la redevabilité et la responsabilité en vue d'une exécution réussie. L'établissement de paramètres de mesure ou d'indicateurs fondamentaux de performance (IFP) pour les objectifs à court terme, moyen terme et long terme contribue à renforcer les mécanismes de gouvernance et de gestion. Ces paramètres de mesure ou indicateurs fondamentaux de performance doivent être:

- ***Spécifiques*** *– cibler un domaine particulier à des fins d'amélioration.*
- ***Mesurables*** *– quantifier ou a minima définir un indicateur de progrès.*
- ***Atteignables*** *– spécifier les résultats qui pourront être atteints d'un point de vue réaliste, compte tenu des ressources disponibles.*
- ***Réalistes*** *– préciser qui sera responsable.*
- ***Temporels*** *– indiquer quand le ou les résultats seront atteints.*

L'établissement de mesures de base facilitera le suivi des actions et mettra en évidence les potentiels d'amélioration. Enfin, l'affectation des budgets devrait être à la mesure des niveaux d'ambition et de complexité de la cible définie.

3.5.2 Suivi de l'état d'avancement de la mise en oeuvre de la stratégie

L'entité chargée de suivre l'état d'avancement de la mise en oeuvre de la stratégie doit s'acquitter de cette tâche conformément à un calendrier convenu tout au long du cycle de vie de la stratégie. A l'issue du suivi, on consignera, dans un rapport ou autre, tout écart par rapport au calendrier établi de même que les raisons des éventuels retards (changement de priorités, insuffisance de la main d'oeuvre ou des ressources, etc.). Cette action est réalisée en sus des mises à jour régulières effectuées par les propriétaires des différents volets de la mise en oeuvre de la stratégie, à destination de l'Autorité responsable du projet.

Cette approche garantit que les parties prenantes concernées sont tenues responsables des engagements pris; elle garantit également la détection précoce des défis posés en matière de mise en oeuvre. Au travers de ces éléments et sur la base des enseignements tirés de la mise en oeuvre, le gouvernement peut rectifier la situation ou ajuster ses plans en conséquence.

3.5.3 Evaluation des résultats de la stratégie

En plus d'évaluer l'état d'avancement par rapport aux indicateurs convenus, il est aussi important d'évaluer périodiquement les résultats et de les comparer avec les objectifs définis. La démarche est essentielle pour comprendre si les objectifs sont effectivement en passe d'être atteints ou si d'autres mesures doivent être envisagées. Dans le cadre de ce processus, il convient de réévaluer périodiquement l'exposition aux risques au sens large, pour évaluer si des changements externes affectent les résultats de la stratégie. Le processus a effectivement pour effet de légèrement modifier le profil d'évaluation des risques du pays.

L'évaluation et les recommandations associées devraient être compilées dans un rapport à l'intention de l'Autorité responsable du projet, lequel comprendra des moyens de mettre à jour le plan d'action tout en veillant à ce que la stratégie soit actualisée et adaptée à l'évolution de la politique et de l'environnement en matière de risques.

Pour finir, les rapports produits pendant tout le cycle de vie de la stratégie devraient également former la base pour procéder à l'examen d'ensemble de la stratégie nationale de cybersécurité, conformément au calendrier établi pendant la phase de lancement. Cet examen général ne doit pas uniquement tenir compte des progrès réalisés et de l'évolution du contexte extérieur, mais doit également réévaluer les priorités et objectifs propres du gouvernement.

De plus amples informations sont fournies à la page 55.

4 Principes généraux

Cette section présente neuf principes transversaux qui, pris ensemble, peuvent contribuer au développement d'une stratégie nationale de cybersécurité à la fois prospective et globale.

Ces principes sont applicables à tous les domaines d'activité clés identifiés dans le présent document. Ils devraient être pris en compte dans toutes étapes du processus de développement de la stratégie, depuis l'élaboration du document de stratégie nationale jusqu'à sa mise en oeuvre.

L'ordre de présentation de ces principes répond plus à une logique narrative qu'à une priorisation par ordre d'importance.

4.1 Vision

La stratégie devrait définir une vision claire au niveau de l'ensemble des gouvernements et de l'ensemble de la société.

Une stratégie a plus de chances de réussir si elle propose une vision qui aide toutes les parties prenantes à mieux comprendre ce qui est en jeu, les raisons pour lesquelles la stratégie s'impose (contexte), ce qui doit être accompli (objectifs), l'objet de la stratégie et les personnes impactées (portée).

Plus la vision est claire, plus il sera facile pour les dirigeants et les principales parties prenantes d'avoir approche plus complète et plus cohérente. Une vision claire facilite également la coordination, la coopération et la mise en oeuvre de la stratégie entre les parties prenantes concernées. Elle devrait être formulée à un niveau suffisamment élevé et tenir compte de la nature dynamique de l'environnement numérique.

Les objectifs et le calendrier de mise en oeuvre de la stratégie devraient être compatibles avec cette vision.

De plus amples informations sont fournies à la page 56.

4.2 Approche globale et priorités ciblées

La stratégie devrait résulter d'une compréhension et d'une analyse globale de l'environnement numérique dans son ensemble, tout en étant adaptée à la situation spécifique de chaque pays et priorisée.

La cybersécurité n'est pas seulement un défi technique, elle est aussi une thématique complexe avec de multiples facettes, dont certains aspects

dépassent le cadre de la prospérité économique et sociale dans des secteurs tels que l'application de la loi, la sécurité nationale et internationale, les relations internationales, les négociations commerciales, le développement durable, etc.

Il est important de comprendre que tous les aspects de la cybersécurité, et la manière dont s aspects sont liés, se complètent potentiellement ou se font concurrence. Sur cette base, et compte tenu de la situation spécifique du pays, des priorités peuvent être définies conformément aux objectifs et au calendrier de mise en oeuvre de la stratégie. Ces priorités permettront de définir des objectifs et un calendrier spécifiques et d'affecter les ressources nécessaires.

Chaque stratégie nationale de cybersécurité comporte des priorités propres au pays concerné. Certains thèmes de cybersécurité peuvent être abordés dans un même document ou dans des documents distincts (par exemple, les aspects numériques de sécurité et de défense nationales peuvent être traités dans le cadre de la stratégie nationale de sécurité ou de défense).

De plus amples informations sont fournies à la page 56.

4.3 Approche inclusive

La stratégie devrait être élaborée avec la participation active de toutes les parties prenantes concernées et tenir compte de leurs besoins et responsabilités.

L'environnement numérique est aujourd'hui une composante essentielle pour le gouvernement, les entreprises et les particuliers. Ces différents acteurs sont confrontés à des risques en matière de cybersécurité et partagent un niveau de responsabilité dans leur gestion, en fonction de leur rôle. Même si cela peut sembler difficile, il est essentiel d'identifier et d'impliquer les parties prenantes à l'élaboration et à la mise en oeuvre réussie d'une stratégie nationale de cybersécurité. Cela aidera à comprendre les besoins des parties prenantes ainsi que leurs connaissances et compétences et facilitera la coopération en vue d'atteindre les objectifs de la stratégie.

La stratégie devrait être un document public visant à renforcer l'inclusion.

De plus amples informations sont fournies aux pages 56 et 57.

4.4 Prospérité économique et sociale

La stratégie devrait renforcer la prospérité économique et sociale et optimiser la contribution des TIC au développement durable et à l'inclusion sociale.

L'environnement numérique peut accélérer la croissance économique et le progrès social, faire progresser les valeurs sociétales fondamentales, améliorer la prestation

et la capacité de services publics, faciliter le commerce international et promouvoir la bonne gouvernance.

La dépendance croissante au numérique, qui suit l'évolution des besoins des sociétés, renforce l'importance de la cybersécurité. Cependant, la cybersécurité n'est pas un objectif en soi; la stratégie devrait être adaptée aux objectifs socio-économiques plus larges du pays et contribuer à instaurer la confiance nécessaire pour faciliter la réalisation de ces objectifs et protéger le pays des cybermenaces.

De plus amples informations sont fournies à la page 57.

4.5 Droits humains fondamentaux

La stratégie devrait respecter les valeurs fondamentales et s'y conformer.

La stratégie devrait reconnaître le fait que les personnes ont des droits hors ligne qui doivent aussi être protégés en ligne. Elle devrait respecter les droits fondamentaux universellement reconnus et notamment, sans toutefois s'y limiter, ceux qui figurent dans la Déclaration universelle des droits de l'homme et dans le Pacte international relatifs aux droits civils et politiques des Nations Unies ainsi que dans les systèmes juridiques multilatéraux ou régionaux concernés.

Une attention particulière devrait être accordée à la liberté d'expression, à la confidentialité des informations et à la protection des données à caractère personnel. En particulier, la stratégie devrait éviter de favoriser la pratique arbitraire, injustifiée ou autrement illégale de la surveillance, de l'interception des communications ou du traitement de données à caractère personnel.

En trouvant le juste équilibre entre les besoins de l'Etat et ceux des individus, la stratégie devrait veiller à ce que, le cas échéant, la surveillance, l'interception des communications et la collecte des données soient réalisées dans le cadre d'une enquête ou d'une procédure judiciaire spécifique, avec l'autorisation de l'autorité nationale compétente et sur la base d'un cadre juridique public, précis, complet et non discriminatoire, permettant un contrôle efficace, des garanties de procédure et des recours.

De plus amples informations sont fournies aux pages 57 et 58.

4.6 Gestion des risques et résilience

La stratégie devrait permettre une gestion efficace des risques de cybersécurité et renforcer la résilience des activités économiques et sociales.

L'environnement numérique offre aux parties prenantes des opportunités économiques et sociales, mais il les expose également au risque de cybersécurité.

Lorsque des organisations utilisent les TIC pour promouvoir l'innovation, gagner en productivité et améliorer la compétitivité ou lorsque les gouvernements déploient leurs services en ligne, des incidents de cybersécurité peuvent survenir et risquer de donner lieu à des incidences financières, de porter atteinte à la réputation, d'entraîner une non-continuité des opérations, de miner les innovations, etc. A l'instar des autres types de risques, le risque de cybersécurité ne peut pas être entièrement supprimé, mais il peut être géré et minimisé.

Pour relever ce défi, la stratégie devrait encourager les entités à hiérarchiser leurs investissements en matière de cybersécurité et à gérer les risques de manière proactive. Selon la propension au risque des entités, un équilibre doit être maintenu entre les mesures de sécurité et les bénéfices potentiels, lequel équilibre tiendra compte de la nature dynamique de l'environnement numérique. La stratégie devrait également reconnaître la nécessité d'un processus continu de gestion du risque et faciliter une approche cohérente entre les entités indépendantes.

Mettre l'accent sur la gestion des risques permet de sensibiliser les parties prenantes aux incidents de sécurité potentiels et de garantir la résilience des activités économiques et sociétales dans le pays. Dans cet esprit, la stratégie devrait enfin encourager l'adoption de mesures visant à assurer la continuité des opérations, incluant la gestion des incidents et des crises et les plans de rétablissement.

De plus amples informations sont fournies à la page 58.

4.7 Ensemble approprié d'instruments politiques

La stratégie devrait utiliser les instruments politiques les plus adéquats pour la réalisation de chacun de ses objectifs, compte tenu des circonstances spécifiques propres à chaque pays.

Les objectifs du gouvernement en matière de cybersécurité ne seront atteints que si un changement de comportement se produit parmi toutes les parties prenantes impliquées. Les gouvernements disposent bien souvent de leviers et instruments politiques différents pour atteindre ce résultat, tels que la législation, la réglementation, la normalisation, les programmes et mécanismes d'incitation et de partage d'informations, les programmes d'éducation, le partage des bonnes pratiques, l'instauration de normes de comportement attendues et la création de communautés de confiance. Chacun possède des forces et faiblesses qui lui sont propres, présente un coût différencié et produit des résultats différents.

Le fait de sélectionner l'instrument de politique le plus approprié pour chaque objectif individuel, en équilibrant l'utilisation des différents outils, permet d'obtenir les meilleurs résultats.

De plus amples informations sont fournies à la page 59.

4.8 Définition claire de l'encadrement, des rôles et de l'attribution des ressources

La stratégie devrait être définie à l'échelon le plus élevé de l'administration, lequel serait responsable de l'attribution des rôles et des responsabilités et de l'affectation des ressources humaines et financières en quantité suffisante.

La cybersécurité devrait être encouragée et soutenue à l'échelon le plus élevé de l'administration. Il convient par ailleurs, pour garantir la responsabilisation et les progrès, d'identifier des coordonnateurs pour chaque axe de travail de même que, pour toutes les parties impliquées, de comprendre clairement leurs rôles et responsabilités respectifs.

La stratégie devrait également allouer les ressources humaines, financières et matérielles nécessaires à sa mise en oeuvre. Ce principe doit guider à la fois le processus de développement de la stratégie et l'élaboration du plan d'action y relatif.

De plus amples informations sont fournies à la page 59.

4.9 Environnement de confiance

La stratégie devrait contribuer à mettre en place un environnement numérique en lequel les citoyens et les entreprises puissent avoir confiance.

Il est essentiel de créer la confiance dans l'écosystème numérique national, d'assurer la protection des droits et intérêts des utilisateurs et la sécurité des données et systèmes, afin de réaliser le plein potentiel des opportunités sociales, politiques et économiques offertes par les TIC. La stratégie doit, au niveau national, encourager les politiques, procédures et actions visant à sécuriser les services essentiels (y compris la gouvernance électronique, le commerce électronique et les transactions financières numériques) basés sur les TIC et utilisés par les citoyens. Les mesures prises en ce sens ancreront le principe de confiance au sein de la population générale, mais aussi au sein des organisations publiques et privées qui offriront des services TIC aux citoyens.

De plus amples informations sont fournies à la page 59.

5 Bonnes pratiques de la stratégie nationale de cybersécurité

La cybersécurité affecte de nombreux domaines du développement socio-économique et est influencée par plusieurs facteurs au niveau national.

Aussi cette Section présente-t-elle un ensemble d'éléments de bonnes pratiques visant à rendre la stratégie plus globale et efficace, tout en permettant une adaptation au contexte national.

Ces éléments de bonne pratique sont regroupés en des domaines d'intervention distincts – qui sont les thèmes généraux de la stratégie nationale de cybersécurité. Les domaines d'intervention et les éléments sont tous deux présentés ici comme des exemples de bonne pratique, mais ces derniers tout particulièrement devront être envisagés dans un contexte national, car certains ne seront pas pertinents au regard de la situation spécifique d'un pays. Les pays devront identifier et suivre les éléments constitutifs de bonnes pratiques visant à appuyer leurs propres objectifs et priorités en conformité avec la vision définie dans leur stratégie (Section 4). L'ordre de présentation des éléments individuels ou domaines d'intervention ci-dessous ne devrait pas être en lien avec le niveau d'importance ou de priorité accordé.

5.1 Domaine d'intervention 1 – Gouvernance

Ce domaine d'intervention présente des éléments de bonne pratique qui pourraient être inclus dans le texte de la stratégie au chapitre de la structure de gouvernance pour la cybersécurité nationale. La stratégie devrait énoncer clairement les objectifs et ambitions du gouvernement en matière de cybersécurité et définir les rôles et responsabilités nécessaires pour assurer sa mise en oeuvre.

A cette fin, la stratégie devrait identifier et habiliter l'autorité compétente responsable de sa mise en oeuvre, mettre en place un mécanisme d'identification et d'inclusion des entités gouvernementales concernées ou responsables de la mise en oeuvre de la stratégie; s'engager à inclure des objectifs spécifiques, mesurables, réalisables, basés sur les résultats et sur le temps dans le plan de mise en oeuvre de la stratégie, et reconnaître la nécessité d'engager des ressources (politiques, financières, humaines, en temps, etc.) pour atteindre les résultats souhaités.

5.1.1 Garantir un niveau de soutien maximum

La stratégie devrait recevoir l'approbation officielle des plus hautes instances du gouvernement, ce qui, premièrement, augmente la probabilité que les ressources soit affectées en quantités suffisantes que les efforts de coordination soient couronnés de succès et, deuxièmement, montre à l'écosystème national plus vaste combien la cybersécurité est importante pour le pays.

5.1.2 Etablir une autorité compétente chargée de la cybersécurité

La stratégie devrait désigner une autorité nationale dédiée en charge de la cybersécurité – un chef de file (qu'il s'agisse d'une personne physique ou morale) haut placé et fortement ancré dans les plus hautes sphères gouvernementales – pour indiquer une direction, coordonner les actions et suivre la mise en oeuvre de la stratégie.

Cette autorité nationale en charge de la cybersécurité devrait également agir comme entité de gestion pour définir et clarifier les rôles, les responsabilités, les processus, les droits de décision et les travaux requis pour assurer la mise en oeuvre efficace de la stratégie. Il s'agit d'identifier les parties prenantes qui superviseront la mise en oeuvre de la stratégie et de fixer des objectifs de performance pour les différents départements ministériels ou gouvernementaux, institutions ou individus chargés de traiter des aspects spécifiques de la stratégie et de son plan d'action. Cette approche peut nécessiter des structures politiques et juridiques supplémentaires pour le bon accomplissement des diverses missions à réaliser.

Etant donné que la cybersécurité touche de nombreux domaines différents, il est important de veiller à ce que l'autorité nationale compétente puisse impliquer et piloter les parties prenantes concernées.

5.1.3 Garantir une coopération intragouvernementale

La stratégie devrait instaurer un mécanisme visant à identifier et à inclure les entités gouvernementales concernées ou chargées de sa mise en oeuvre. Ces entités gouvernementales doivent notamment faire preuve d'implication, de coordination et de coopération au sein du gouvernement pour que les ressources et mécanismes gouvernementaux (à savoir les réglementations) puissent produire les résultats attendus définis dans la stratégie.

La communication et la coordination doivent être efficaces de façon à ce que tous les ministères et agences gouvernementales connaissent les prérogatives, missions et tâches de leurs homologues. L'engagement, en revanche, consiste à soutenir des politiques cohérentes sur la durée, pour garantir que les promesses de la stratégie soient tenues. Un exemple de coordination serait la tenue des réunions périodiques impliquant toutes les parties prenantes concernées dans les plans d'action qui doivent faire l'objet d'une révision conjointe. Un exemple de coopération serait la mise sur pied d'un Groupe spécial pour traiter d'une question particulière. Concernant l'engagement, on pourrait évoquer la cohérence des programmes de politique intérieure et extérieure du pays de sorte qu'un ministère ne vienne pas saper pas la crédibilité d'un autre en représentant différentes positions sur le même domaine de politique.

5.1.4 Garantir une coopération intersectorielle

La stratégie devrait refléter la compréhension des dépendances entre le gouvernement, le secteur privé et les autres parties prenantes nationales (et vice-versa) pour assurer la cybersécurité. A cette fin, elle devrait expliquer comment le gouvernement implique ces parties prenantes et comment il définit leurs rôles et responsabilités. Par exemple, la stratégie devrait identifier un réseau de points de contact nationaux faisant autorité pour les industries critiques, indispensables au fonctionnement et à la restauration des services et des infrastructures essentielles.

5.1.5 Affecter le budget et les ressources spécifiques

La stratégie devrait fournir des précisions sur l'affectation des ressources dédiées et appropriées pour sa mise en oeuvre, sa maintenance et sa révision. Un financement suffisant, cohérent et continu constitue le fondement d'une posture nationale efficace en matière de cybersécurité. Les ressources doivent être définies en termes d'argent (budget dédié), de personnes, de matériel, ainsi que de relations et de partenariats, d'engagement politique continu et de leadership nécessaires à la bonne exécution. L'affectation des objectifs et des tâches au sein de la stratégie ne devrait pas être considérée comme une initiative ponctuelle.

Les ressources peuvent être affectées par tâche ou objectif, ou par une entité gouvernementale. Le gouvernement peut également envisager d'instaurer un budget central pour la cybersécurité, qui serait géré par un mécanisme central de gouvernance de la cybersécurité. Qu'il s'agisse de réunir des fonds disparates, d'intégrer ou de mettre en oeuvre un budget intragouvernemental unifié, le programme global doit être géré et suivi par étapes afin de garantir la réussite de la mise en oeuvre de la stratégie.

5.1.6 Elaborer un plan de mise en oeuvre

La stratégie devrait inclure ou mentionner un plan de mise en oeuvre expliquant plus en détail la manière dont les objectifs stratégiques seront atteints. Ce plan de mise en oeuvre, pour être efficace, nommera l'entité responsable chargée de chaque tâche et objectif, les ressources nécessaires à sa mise en oeuvre dans la durée (à court, moyen et long terme), les processus qui seront utilisés et les résultats qui peuvent être atteints (Section 3.4 relative à la mise en oeuvre).

De plus amples informations sont fournies à la page 61.

5.2 Domaine d'intervention 2 – Gestion des risques de cybersécurité au niveau national

Ce domaine d'intervention met en place de bonnes pratiques pour aborder la cybersécurité au travers de la gestion des risques. Comme énoncé dans le principe de gestion des risques et de résilience (Section 4.2), une approche de gestion des risques s'impose, car les cyberrisques ne peuvent pas tous être éliminés. Un pays qui possède une bonne compréhension des risques auxquels il se trouve exposé pourra gérer ses risques de façon plus efficace. En termes d'évaluation des risques, l'approche devra notamment cibler les interdépendances et également envisager les risques liés aux dépendances transfrontières. Cette approche tiendra compte de l'ensemble du cycle de vie, depuis le développement ou approvisionnement jusqu'à l'exploitation et au remplacement.

Compte tenu de la nature extrêmement dynamique et imprévisible des menaces à la cybersécurité, il est par ailleurs important de préciser que toute approche de ce type devra faire l'objet d'une évaluation régulière. La stratégie devrait dans ce cadre prévoir un suivi et une évaluation des activités de gestion des risques afin d'assurer une amélioration continue.

5.2.1 Définir une approche de gestion des risques

La stratégie devrait définir une approche de gestion des risques cohérente qui devrait être suivie par toutes les entités gouvernementales et tous les opérateurs d'infrastructures essentielles référencés au niveau local. Cette approche devrait permettre d'identifier les principaux actifs et services essentiels au bon fonctionnement de la société et de l'économie, de même que les menaces et les risques associés.

L'approche devrait conduire à l'élaboration d'un registre national des risques, qui serait stocké et communiqué en toute sécurité et qui permettrait au gouvernement d'exercer une surveillance sur les risques et les lignes de conduite adoptées pour gérer ces risques. L'approche devrait également développer une méthode de priorisation basée sur un calcul de la probabilité de réalisation des risques et de leur impact. Elle devrait enfin préciser les responsabilités des entités clés de chaque secteur en ce qui concerne l'évaluation, l'acceptation et le traitement des risques de cybersécurité au niveau national.

5.2.2 Définir une méthodologie commune de gestion des risques en matière de cybersécurité

La stratégie devrait définir une méthodologie commune de gestion des risques en matière de cybersécurité, ce qui garantira l'efficacité et la cohérence au sein des organisations et facilitera l'échange d'informations sur les risques entre des systèmes interdépendants. On préférera une méthodologie fondée sur des normes internationales dans la mesure où elle pourrait réduire les coûts et générer une meilleure interaction avec le secteur privé.

La méthodologie devrait fournir des indications sur l'attribution des rôles et responsabilités en ce qui concerne divers aspects de la gestion des risques, tels que l'évaluation des menaces, la valorisation des actifs, la mise en oeuvre et le maintien de mesures d'atténuation et l'acceptation du risque résiduel. La méthodologie devrait inclure un programme de certification pour aider à évaluer et éventuellement améliorer la conformité.

Il est important de noter qu'en ce qui concerne l'achat et le développement d'infrastructures ou de services, la méthodologie de gestion des risques doit également renseigner sur la minimisation des risques grâce à une architecture et une conception sécurisées, sachant que la sécurité se trouve renforcée lorsqu'elle fait partie intégrante du processus de conception du produit, du processus ou du service (sécurité dès la conception).

5.2.3 Développer des profils de risque par secteur en matière de cybersécurité

La stratégie devrait préconiser l'utilisation de profils de risque sectoriels pour la cybersécurité. Un profil de risque sectoriel est une analyse quantitative des types de menaces rencontrés. Il a pour objet de fournir une compréhension moins subjective du risque en attribuant des valeurs numériques aux différents types de menaces et au danger représenté. La stratégie devrait encourager le développement de profils de risque pour ces secteurs que les pays considèrent comme essentiels pour la société et l'économie.

L'utilisation de profils de risque sectoriels fournit une base pour des évaluations de risques plus spécifiques pour des organisations individuelles, introduit une cohérence au sein et à travers tous les secteurs et réduit les ressources nécessaires pour les évaluations de risques organisationnelles. Ils devraient être mis à jour sur une base régulière pour rester d'actualité.

5.2.4 Etablir des politiques de cybersécurité

La stratégie devrait encourager l'établissement de politiques de cybersécurité pour les principales entités nationales, notamment les agences gouvernementales et les opérateurs d'infrastructures essentielles. Ces politiques, adoptées en vertu du principe selon lequel il convient d'utiliser un ensemble approprié d'instruments politiques (Section 4.7), couvriraient les exigences en matière de bonne gouvernance, d'exploitation et de technique, instruiraient les parties prenantes sur leurs rôles et responsabilités et proposeraient ou imposeraient des approches spécifiques sur ces questions.

Il pourrait s'agir, par exemple, de politiques qui traitent de la cybersécurité dans les achats ou le développement, définissent des programmes de partage d'informations, coordonnent les informations sur les vulnérabilités, établissent des normes minimales de prise en charge, fixent des références en matière de sécurité, instaurent des programmes de certification de la conformité et imposent le signalement des cyber-incidents.

La coordination des actions au niveau national permettrait d'améliorer l'efficacité et l'efficience de la gestion de la cybersécurité, via l'harmonisation des pratiques et le renforcement de la coordination et de l'interopérabilité.

De plus amples informations sont fournies à la page 61.

5.3 Domaine d'intervention 3 – Préparation et résilience

Ce domaine d'intervention présente un survol des bonnes pratiques qui soutiennent la mise en place et la durabilité de capacités nationales efficaces pour prévenir, détecter, atténuer et combattre les incidents majeurs de cybersécurité et pour améliorer la cyberrésilience globale du pays.

5.3.1 Mettre en place des capacités de réaction face aux cyber-incidents

La stratégie devrait appeler à la mise en place, au niveau national, de capacités de réaction appropriées pour faire face aux incidents opérationnels de cybersécurité. Ces capacités peuvent consister à créer des équipes d'intervention en cas d'incident informatique (CIRT), des équipes d'intervention en cas d'incident de sécurité informatique (CSIRT) et des équipes d'intervention en cas d'urgence informatique (CERT), dotées d'une responsabilité nationale.

Bien que la forme organisationnelle spécifique d'un CIRT/CSIRT/CERT puisse varier (entité nationale, gouvernementale, sectorielle ou autre) et que tous les pays n'ont pas les mêmes besoins et ressources, ces équipes spécialisées et dédiées doivent fournir un ensemble de fonctions à la fois proactives et réactives ainsi que des

services préventifs et éducatifs. Ainsi, ces entités peuvent accroître la capacité d'un pays à réagir et à se relever rapidement face aux cyberattaques et à renforcer sa résilience face aux cybermenaces, réduisant par là même l'incidence globale possible des cyberattaques d'importance nationale sur les activités économiques et opérationnelles. La stratégie devrait par ailleurs identifier et développer des mécanismes de coopération et des procédures de communication entre les équipes nationales et sectorielles d'intervention en cas d'incident (si elles existent dans le pays), ainsi qu'avec les homologues internationaux.

5.3.2 Elaborer des plans d'urgence pour la gestion des crises de cybersécurité

La stratégie devrait encourager le développement, au niveau national, d'un plan d'urgence pour la gestion des crises en matière de cybersécurité. Ce plan devrait faire partie intégrante ou être aligné sur le plan d'urgence national global. Un plan spécifique pour les infrastructures de l'information essentielles devrait également être envisagé.

Ce plan d'urgence national en matière de cybersécurité devrait tenir compte des conclusions des évaluations de risques nationales et des éventuelles dépendances intersectorielles pouvant affecter la continuité des opérations au niveau des infrastructures essentielles ainsi que des mécanismes de récupération en cas de sinistre. Enfin, il devrait fournir un aperçu des mécanismes nationaux d'intervention en cas d'incidents et montrer comment les incidents de cybersécurité sont classés, selon leurs incidences sur les services et actifs essentiels.

5.3.3 Promouvoir le partage d'informations

La stratégie devrait préconiser la mise en place de mécanismes d'échange d'informations afin de permettre l'échange de renseignements décisionnels et de renseignements sur les menaces entre et au sein des secteurs public et privé.

Les programmes officiels et informels de partage d'informations peuvent contribuer à promouvoir une communication plus efficace ainsi que des communications cohérentes, précises et appropriées lors des activités de réponse aux incidents et de rétablissement, à faciliter le partage rapide des informations sur les menaces et le renseignement entre les parties concernées et les autres intervenants, à mieux comprendre comment et quels secteurs ont été ciblés, à diffuser des informations sur les méthodes pouvant être utilisées pour protéger et limiter les dommages sur les actifs concernés et, enfin, à réduire les vulnérabilités et l'exposition aux risques associés.

La stratégie devrait identifier une ou plusieurs structures institutionnelles (comme les autorités compétentes), chargées de transmettre des informations précises et recevables au sein de la communauté nationale de cybersécurité, y compris les secteurs public et privé.

Le partage d'informations devrait être un processus à double sens. Si les gouvernements se montrent disposés à partager les informations qu'ils détiennent, leurs actions devront démontrer aux entités du secteur privé que le gouvernement se positionne bel et bien comme un partenaire dans le partage d'informations sur les menaces et contribuer à faire en sorte que les intervenants soient mieux préparés et outillés pour faire face aux principales menaces.

5.3.4 Réaliser des exercices de cybersécurité

La stratégie devrait encourager l'organisation et la coordination des exercices nationaux et internationaux de cybersécurité et d'intervention en cas d'incident. Ces derniers peuvent prendre différentes formes (simulations, exercices en temps réel, etc.) et cibler les décideurs ou le personnel technique.

Les exercices de cybersécurité et autres mécanismes de planification en cas de crise peuvent aider les pays à développer une capacité institutionnelle chargée de répondre efficacement aux incidents, à tester les procédures de gestion de crise et les mécanismes de communication, à vérifier la capacité opérationnelle des Certs/Csirts/Cirts à répondre à la pression et à comprendre toutes les dépendances intersectorielles.

De même, les exercices internationaux de cybersécurité peuvent contribuer à renforcer la capacité d'intervention face aux cyber-incidents entre les pays, à comprendre les dépendances intersectorielles, à accroître la confiance entre les pays et à améliorer les niveaux globaux de résilience et de préparation au niveau international.

De plus amples informations sont fournies à la page 63.

5.4 Domaine d'intervention 4 – Services d'infrastructures critiques et services essentiels

Ce domaine d'intervention passe en revue les bonnes pratiques concernant la protection des infrastructures essentielles et en particulier des infrastructures de l'information essentielles. S'il n'existe pas de définition universellement admise pour ces deux termes et si les gouvernements doivent se poser la question de savoir quels entités et services inclure sur la base de leur propre évaluation nationale des risques, le présent Guide donne cependant la définition suivante:

- *Les infrastructures essentielles* désignent les actifs essentiels au fonctionnement et à la sécurité d'une société et d'une économie dans un pays donné.
- *Les infrastructures de l'information* essentielles sont, quant à elles, des systèmes informatiques et systèmes basés sur les TIC qui assurent les fonctions clés des infrastructures essentielles d'un pays.

Par extension, on parle de «services essentiels» pour désigner les services qui sont nécessaires au maintien des fonctions sociétales ou économiques critiques.

Dans les deux cas de figure, ces services couvrent notamment: l'énergie (électricité, pétrole et gaz), les transports (aérien, ferroviaire, maritime et routier), la finance et la banque (établissements de crédit, plates-formes de négociation et contreparties centrales), les soins de santé (organisations de soins de santé, y compris hôpitaux et cliniques privées), le réseau d'approvisionnement et de distribution en eau potable, le numérique et les télécommunications (services de téléphonie fixe et mobile et fourniture d'une infrastructure Internet, tels que des points d'échange Internet (Ixps) et un service de nom de domaine, entre autres).

5.4.1 Mettre en place une approche de gestion des risques pour protéger les infrastructures et services essentiels

La stratégie devrait aborder la protection des infrastructures essentielles et des infrastructures de l'information essentielles du point de vue de la gestion des risques, conformément au principe de gestion des risques et de résilience (énoncé à la Section 4.6). Une évaluation détaillée des risques devrait permettre d'identifier les infrastructures essentielles et infrastructures de l'information essentielles de même que les services essentiels, dont la perturbation pourrait avoir de graves conséquences sur la santé, la sûreté, la sécurité ou le bien-être économique des citoyens ou sur le fonctionnement efficace du gouvernement ou de l'économie.

Une approche fondée sur les risques devrait par ailleurs être adoptée aux fins de l'identification et de la hiérarchisation de la mise en oeuvre des programmes et politiques conçus pour protéger les infrastructures essentielles et infrastructures de l'information essentielles. Une approche de gestion des risques reposant sur des normes internationales pourrait aussi être envisagée pour faciliter les relations avec le secteur privé.

5.4.2 Adopter un modèle de gouvernance avec des responsabilités claires

A un niveau plus élevé, la stratégie devrait décrire la structure de gouvernance ainsi que les rôles et responsabilités des différentes parties prenantes de la protection des infrastructures essentielles et infrastructures de l'information essentielles. Comme stipulé dans le Principe de la définition claire de l'encadrement, des rôles et de l'attribution des ressources (Section 4.8), les programmes de protection des infrastructures essentielles à la fois efficaces et efficients donnent une définition claire des rôles et des responsabilités et mettent en place un mécanisme de coordination pour la gestion des problèmes en cours. Bien souvent, les infrastructures essentielles et infrastructures de l'information essentielles ne sont pas détenues ni contrôlées par le gouvernement et les efforts de protection en la matière excèdent généralement les capacités et le mandat d'une seule agence gouvernementale.

La désignation d'un responsable général de la coordination pour la (cyber)sécurité des infrastructures essentielles et infrastructures de l'information essentielles (par exemple, une commission interinstitutions) peut, dans ce cas, grandement contribuer aux efforts de protection des infrastructures essentielles.

Le modèle de gouvernance pour la protection des infrastructures essentielles et infrastructures de l'information essentielles devrait inclure l'identification des entités gouvernementales chargées de secteurs verticaux spécifiques, les responsabilités et la responsabilisation des opérateurs d'infrastructures essentielles et d'infrastructures de l'information essentielles ainsi que les canaux de communication et les mécanismes de coopération entre les agences publiques et privées pour garantir l'exploitation et la récupération des services et infrastructures essentiels.

5.4.3 Définir des références de base minimum en matière de cybersécurité

La stratégie devrait mentionner les cadres législatifs et réglementaires existants ou proposer le développement de nouveaux cadres fixant entre autres des références

de base minimum en matière de cybersécurité pour les opérateurs d'infrastructures essentielles et d'infrastructures de l'information essentielles. Lors de l'établissement de ces références de base, il est conseillé de s'appuyer sur les normes reconnues internationalement et sur les bonnes pratiques pour obtenir de meilleurs résultats en termes de sécurité et une plus grande efficacité.

Les références de sécurité devraient être axées sur les résultats – c'est-à-dire définir les objectifs des organisations (par exemple, «contrôler l'accès logique aux ressources essentielles») plutôt que les modalités de mise en oeuvre de la sécurité (par exemple, «utiliser une authentification à deux facteurs») – ce qui permet au gouvernement et à l'industrie de bénéficier d'améliorations constantes en matière de sécurité. Une approche basée sur les résultats autorise également une plus grande marge de manoeuvre en ce qui concerne les orientations et la mise en place dans les secteurs, donnant ainsi plus de souplesse aux entreprises pour adapter à intervalles périodiques leurs propres orientations à l'évolution de la menace et aux progrès de la technologie.

5.4.4 Utiliser un large panel de leviers marketing

La stratégie devrait prendre en compte un large panel de politiques visant à garantir que toutes les organisations et personnes sont réellement incitées à assumer leurs responsabilités en matière de cybersécurité, eu égard aux risques auxquels elles sont exposées et conformément au principe de l'approche globale et des priorités ciblées (Section 4.2).

L'identification des écarts entre ce que les marchés peuvent ou devraient faire et les contraintes générées par l'exposition aux risques s'avère être une étape essentielle pour déterminer comment et quand utiliser les mesures d'incitation et de dissuasion disponibles pour améliorer la sécurité. Pour encourager l'adoption des normes et pratiques de cybersécurité concernant les infrastructures essentielles et les infrastructures de l'information essentielles, la stratégie devrait par ailleurs mentionner que le gouvernement envisagera de mettre à sa disposition une série d'options politiques et de leviers marketing.

5.4.5 Instaurer des partenariats public-privé

La stratégie devrait encourager la création de partenariats officiels entre le secteur public et le secteur privé afin d'accroître la sécurité des infrastructures essentielles et des infrastructures de l'information essentielles. Les partenariats public-privé sont la pierre angulaire d'une protection efficace des infrastructures essentielles et de la gestion des risques de sécurité sur le court et long terme. Ils sont essentiels pour renforcer la confiance au sein et entre l'industrie et le gouvernement.

Pour que ces partenariats puissent durer dans le temps, cependant, toutes les parties prenantes concernées doivent avoir une compréhension claire des objectifs du partenariat et des avantages mutuels liés à la collaboration en termes de sécurité. Exemples de domaines concernés: l'atteinte d'un accord sur les références de base communes en termes de cybersécurité, la mise en place de structures efficaces de coordination, de processus et protocoles de partage d'informations, l'établissement de rapports de confiance, l'identification et l'échange d'idées, d'approches et de bonnes pratiques pour améliorer la sécurité et la coordination internationale.

De plus amples informations sont fournies à la page 64.

5.5 Domaine d'intervention 5 – Renforcement des capacités et sensibilisation

Des considérations technologiques et politiques peuvent dominer les discussions sur la cybersécurité et occulter l'élément humain fondamental en son centre. Ce domaine d'intervention recense les enjeux liés au renforcement des capacités de cybersécurité et à la sensibilisation parmi les entités gouvernementales, les citoyens, les entreprises et autres organisations – qui sont essentiels pour soutenir l'économie numérique d'un pays.

Les bonnes pratiques examinées dans cette section incluent la mise en place de cursus dédiés à la cybersécurité et de programmes de sensibilisation, la généralisation de plans de formation et de programmes de développement de la main-d'oeuvre, l'adoption de systèmes de certification internationaux et la promotion de pôles d'innovation et de recherche et développement (R&D).

5.5.1 Développer des cursus dédiés à la cybersécurité

La stratégie devrait faciliter le développement de cursus scolaires dans le but d'accélérer le développement des compétences et la sensibilisation à la cybersécurité dans le cadre du système d'éducation officiel. Il pourrait s'agir d'élaborer des programmes de cybersécurité dédiés dans les écoles primaires et secondaires, d'intégrer des modules de cybersécurité dans tous les programmes d'informatique et de TI de l'enseignement supérieur et de créer des diplômes de cybersécurité de même que des apprentissages officiels.

Les cursus scolaires ainsi créés peuvent par ailleurs encourager une prise de conscience et susciter un intérêt plus grand pour les opportunités de carrière dans la cybersécurité. Pour poursuivre les efforts dans ce domaine, le gouvernement devrait également envisager le développement de diverses mesures incitatives telles que les bourses d'études pour les programmes d'éducation privés et les subventions pour les apprentissages appropriés.

5.5.2 Encourager le développement des compétences et la formation de la main-d'oeuvre

La stratégie devrait s'intéresser au développement de programmes de formation professionnelle et de développement des compétences en cybersécurité pour les experts et non experts dans les secteurs public et privé. Il peut s'agit de fournir des formations, des stages ou des apprentissages au niveau exécutif ou opérationnel de même que des certifications (nationales et internationales) de professionnels de la sécurité, en se fondant sur les besoins cernés par l'industrie et le gouvernement. La formation technique devrait être complétée par des initiatives axées sur la gestion des risques.

La stratégie devrait également encourager des initiatives visant à développer des parcours de carrière dédiés à la cybersécurité, en particulier pour le secteur public, ainsi que des incitations à augmenter le nombre de professionnels qualifiés dans la cybersécurité. Un partenariat avec les universités, le secteur privé et la société civile devrait être mis en place. Enfin, pour combler l'écart hommes-femmes concernant l'emploi d'experts en cybersécurité, il conviendrait d'adopter une approche plus équilibrée entre les sexes pour motiver, encourager et promouvoir un plus grand

engagement de la part des femmes et ce, dans tous les efforts de développement des compétences et de formation, pour assurer l'inclusivité à l'avenir.

5.5.3 Mettre en place un programme coordonné de sensibilisation à la cybersécurité

La stratégie devrait attribuer la responsabilité de coordonner les campagnes et activités nationales de sensibilisation dans le domaine de la cybersécurité à une autorité compétente, de façon à garantir l'utilisation rationnelle des ressources et à établir le cadre des responsabilités. Cette autorité devrait collaborer avec les parties prenantes concernées pour développer et mettre en oeuvre des programmes de sensibilisation à la cybersécurité, axés sur la diffusion d'informations relatives aux risques et menaces liés à la cybersécurité, ainsi que pour partager les bonnes pratiques permettant de les combattre.

Un tel programme coordonné pourrait comprendre, entre autres, des campagnes de sensibilisation du grand public, des enfants et des usagers du numérique, des programmes d'éducation axés sur le consommateur et des initiatives de sensibilisation, à l'intention des cadres des secteurs public et privé.

5.5.4 Encourager l'innovation et la R&D en matière de cybersécurité

La stratégie devrait promouvoir un contexte stimulant la recherche fondamentale et appliquée en matière de cybersécurité dans tous les secteurs et auprès de divers groupes de parties prenantes. Il pourrait s'agir, par exemple, de veiller à ce que les efforts de recherche au niveau national soutiennent les objectifs de la stratégie nationale de cybersécurité, de développer des programmes de R&D axés sur la cybersécurité dans les organismes de recherche publics, de diffuser efficacement les nouvelles découvertes, les technologies de base de même que les techniques, processus et outils. Les pays devraient par ailleurs, toujours dans le cadre de la stratégie, chercher à nouer des liens avec la communauté de recherche internationale dans les domaines scientifiques liés à la cybersécurité, tels que l'informatique, l'ingénierie électrique, les mathématiques appliquées et la cryptographie, mais également dans des domaines non techniques tels que les sciences politiques et sociales, les études de commerce et de gestion ou encore la psychologie, pour ne citer qu'eux.

La stratégie devrait examiner les mécanismes d'incitation offerts tels que subventions, achats, dégrèvements fiscaux, concours et autres initiatives encourageant le développement de solutions, produits et services innovants en matière de cybersécurité.

De plus amples informations sont fournies à les pages 64 et 65.

5.6 Domaine d'intervention 6 – Législation et réglementation

Ce domaine d'intervention concerne l'élaboration d'un cadre juridique et réglementaire visant à protéger la société contre la cybercriminalité et à promouvoir un cyberenvironnement fiable et sécurisé, selon le principe relatif à une approche inclusive et à un environnement de confiance (Sections 4.3 et 4.9 respectivement). Un tel cadre peut prévoir, entre autres, l'adoption d'une législation

qui définit la notion de cyberactivité illégale, la reconnaissance juridique des droits individuels et des libertés civiles, l'établissement d'un mécanisme de conformité, le renforcement de la capacité à faire appliquer le cadre, l'institutionnalisation des entités essentielles et la coopération internationale pour lutter contre la cybercriminalité.

5.6.1 Elaboration d'une législation de lutte contre la cybercriminalité

La stratégie devrait promouvoir le développement d'un cadre juridique national qui définit clairement ce qu'est une cyberactivité interdite et qui vise la réduction de la criminalité en ligne. Le plus souvent, cette capacité prend la forme d'une législation sur la cybercriminalité, qui peut résulter de la promulgation de lois spécifiques nouvelles ou existantes (par exemple, le Code pénal, les lois régissant les secteurs bancaires, les télécommunications et autres secteurs).

La stratégie devrait également encourager la création d'un processus de suivi de la mise en oeuvre et d'examen de la législation et des mécanismes de gouvernance, identifier les lacunes et les chevauchements de compétences de même que clarifier et hiérarchiser les secteurs qui nécessitent une modernisation (par exemple, les lois existantes, telles que les anciennes lois sur les télécommunications).

5.6.2 Reconnaître et protéger les droits individuels et les libertés

La stratégie devrait protéger les droits essentiels à une procédure régulière (dans le cas d'investigations criminelles et de poursuites judiciaires) ainsi que les droits à la protection des données, y compris la protection du respect du caractère privé des données personnelles (via la mise en place, le cas échéant, d'un cadre de protection des données et de la vie privée) et de la liberté d'expression, conformément aux principes fondamentaux des droits de l'homme (Section 4.5).

5.6.3 Créer des mécanismes de conformité

La stratégie devrait promouvoir la mise en place de mécanismes nationaux de conformité (de mise en oeuvre et d'incitation). Ces mécanismes devraient être mis en place pour combattre, prévenir et atténuer les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes et infrastructures TIC, qui menacent les données informatiques, conformément au cadre juridique susmentionné. Ils devraient notamment couvrir les particularités de l'investigation numérique, l'interception licite des communications et l'utilisation des preuves électroniques.

5.6.4 Encourager le renforcement des capacités à des fins d'application de la loi

La stratégie devrait encourager le développement de capacités dans le domaine de l'application des lois cybernétiques, incluant la formation et l'éducation des nombreuses parties prenantes impliquées dans la lutte contre la cybercriminalité (juges, procureurs, avocats, responsables de l'application de la loi, experts en criminalistique et autres enquêteurs). Les forces de l'ordre devraient recevoir une formation spécialisée pour interpréter et appliquer les lois nationales en matière de cybercriminalité (traduire la loi en spécifications techniques et vice versa), pour détecter, dissuader, enquêter et poursuivre efficacement les infractions relevant de la cybercriminalité; et pour collaborer efficacement avec le secteur et les services

internationaux chargés de l'application de la loi (tels qu'INTERPOL, Europol) pour lutter contre la cybercriminalité et renforcer la cybersécurité. Cet élément devrait tenir compte du domaine d'intervention 5 – Renforcement des capacités et sensibilisation (Section 5.5).

5.6.5 Mettre en place des processus intersectoriels

La stratégie devrait identifier et reconnaître les mandats des organismes nationaux ayant pour mission première de garantir la conformité avec la législation sur la cybercriminalité, qu'il s'agisse des entités responsables de la protection des infrastructures essentielles ou des entités chargées de s'assurer que toutes les exigences internationales en matière de cybercriminalité sont bien prises en compte (par exemple, veiller à ce que la législation nationale soit en conformité avec les obligations découlant des traités internationaux), au-delà des frontières judiciaires (par exemple, coopération transfrontières) (voir également les Sections 5.1.3 et 5.1.4; et la Section 5.6.6).

Dans certains systèmes juridiques, il peut être nécessaire de légiférer pour la mise en place d'institutions impliquées dans la cybersécurité, telles que les Certs/Cirts/Csirts nationales, ou pour clarifier le pouvoir d'une agence unique de coordonner la cyber-politique dans un pays.

5.6.6 Soutenir la coopération internationale pour lutter contre la cybercriminalité

La stratégie devrait manifester un engagement à protéger la société contre la cybercriminalité à l'échelle mondiale, en ratifiant – dans la mesure du possible et conformément au programme national global – des accords internationaux sur la cybercriminalité ou des accords équivalents en matière de lutte contre la cybercriminalité et en promouvant des mécanismes de coordination visant à combattre la cybercriminalité au niveau international. Peuvent être concernés, à titre d'exemple, l'alignement des lois nationales sur les obligations conventionnelles internationales et sur les accords bilatéraux, par exemple en mettant en place une entraide judiciaire, la réalisation d'enquêtes judiciaires et de poursuites transfrontalières, le traitement d'éléments de preuve numérique et l'extradition. Cet élément devrait tenir compte du domaine d'intervention 7 sur la coopération internationale (Section 5.7).

De plus amples informations sont fournies à la page 66.

5.7 Domaine d'intervention 7 – Coopération internationale

Ce domaine d'intervention met l'accent sur les éléments que devrait couvrir la stratégie en termes d'engagements de cybersécurité en dehors du pays, aux niveaux régional et international. La cybersécurité joue un rôle de plus en plus grand dans de nombreux domaines des relations internationales, notamment dans le secteur des droits de l'homme, du développement économique, des échanges, du commerce, de la maîtrise des armements, de la sécurité, de la stabilité, de la paix et du règlement des conflits.

La stratégie devrait par conséquent reconnaître que la cybersécurité ne connaît pas de frontières et souligner la nécessité de coopérer non seulement avec les parties prenantes nationales, mais également internationales. Les engagements

internationaux avec les parties prenantes publiques et privées sont essentiels pour faciliter un dialogue constructif, développer des mécanismes de confiance et de coopération, trouver des solutions mutuellement acceptables aux défis communs et créer une culture mondiale de la cybersécurité.

Selon le principe de l'approche globale et des priorités ciblées (Section 4.2), il convient d'encourager la coopération aux niveaux régional et international, en harmonie avec les dispositions politiques, sociales, culturelles et économiques du pays, ainsi qu'avec ses priorités en matière de politique étrangère.

5.7.1 Reconnaître l'importance de la cybersécurité comme une priorité de politique étrangère

La stratégie devrait exprimer un engagement en faveur de la coopération internationale au service de la cybersécurité et reconnaître que les questions relevant de la cybercriminalité font partie intégrante de la politique étrangère du pays. A cette fin, il est important d'encourager le développement et l'utilisation des compétences et des connaissances sur les questions de cybercriminalité (cyberdiplomatie) en complément des méthodes et procédures traditionnelles de la diplomatie. La stratégie pourrait également inclure la création de structures organisationnelles spécifiques de même que la mise en place de bureaux ou de personnels qualifiés dont les travaux porteraient sur l'engagement diplomatique sur les questions de cybercriminalité.

Plus spécifiquement, la stratégie devrait clairement stipuler les domaines d'intervention et objectifs à long terme du gouvernement en matière de coopération internationale, y compris les parties prenantes impliquées (aux niveaux public, privé, régional, international). Peuvent être concernés, par exemple, le soutien en faveur de l'établissement de normes internationales de cybersécurité et de mesures d'instauration de la confiance, l'engagement à renforcer les capacités en matière de cybersécurité, la participation dans le développement de normes internationales de cybersécurité et le regroupement des instruments internationaux et régionaux existants.

Une meilleure harmonisation entre les différents acteurs gouvernementaux (par exemple, les chefs d'Etat et de cabinet, le ministère des Affaires étrangères, le ministère des TIC, le ministère de l'Industrie et du Commerce, le ministère de la Justice ou le ministère de la Défense) sera parfois nécessaire pour que la position politique exprimée par un acteur domestique à la table des négociations sur la scène internationale de la cybersécurité soit correctement coordonnée et en accord avec les autres organismes gouvernementaux.

5.7.2 Prendre part aux débats internationaux

La stratégie devrait lister les forums internationaux spécifiques et les mécanismes de coopération auxquels le pays souhaite adhérer pour nouer concrètement des contacts diplomatiques au sujet des questions relevant de la cybercriminalité. Il peut s'agir d'organisations régionales ou internationales, de discussions intergouvernementales, d'alliances des secteurs public et/ou privé ainsi que de mécanismes traditionnels de coopération et de collaboration établis, traitant des questions de cybersécurité.

A mesure que le pays prend des engagements de ce type, le gouvernement sera amené à développer des compétences et connaissances additionnelles axées sur les questions de cybercriminalité et à accroître sa capacité globale en termes

de cybersécurité. Il est donc important de hiérarchiser efficacement ces efforts et d'allouer les ressources adéquates (humaines et financières) pour garantir l'obtention de résultats concrets.

5.7.3 Promouvoir des formes de coopération officielles et informelles dans le cyberespace

La stratégie devrait indiquer les mécanismes de coopération opérationnelle internationale auxquels le pays souhaite adhérer. Le pays peut souhaiter s'engager dans des efforts internationaux officiels et informels visant à faire progresser la coopération, par exemple, en matière d'élaboration de politiques et de législation, d'application de la loi, de réaction aux incidents, de partage d'informations et de menaces. La participation à de telles initiatives pourrait améliorer la coopération et l'échange d'informations entre les autorités compétentes sur les menaces et les vulnérabilités potentielles.

5.7.4 Aligner les efforts de cybersécurité aux niveaux national et international

La stratégie devrait tenir compte des initiatives régionales et internationales existantes en matière de cybersécurité et favoriser leur harmonisation et leur alignement. Le pays pourrait ainsi tirer parti des bonnes pratiques existantes et contribuer à la cohésion et à la convergence des approches en matière de cybersécurité.

Pour ce faire, la stratégie devrait démontrer l'engagement du pays à assurer la cohérence entre sa politique intérieure et sa politique extérieure, en harmonisant son cadre juridique national et ses politiques avec ses engagements à l'international et en alignant ses approches de la cybersécurité au niveau national avec ses efforts à l'international.

Parmi les exemples notables d'efforts internationaux pouvant être pris en compte dans le cadre de la stratégie, nous pouvons citer, sans toutefois s'y limiter: les travaux du Groupe d'experts gouvernementaux des Nations Unies chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (UN GGE), de l'Organisation pour la sécurité et la coopération en Europe (OSCE) sur les mesures de transparence et de confiance et normes internationales applicables au cyberespace, les travaux du High-Tech Crime Subgroup du G7, la Convention de Budapest sur la cybercriminalité du Conseil de l'Europe, la convention de l'Union Africaine sur la cyber sécurité, l'accord entre les gouvernements des Etats membres de l'Organisation de coopération de Shanghai sur la coopération pour garantir la sécurité de l'information au niveau international, la Convention arabe sur la lutte contre les infractions portant sur les technologies de l'information, la directive de la CEDEAO sur la cybercriminalité et le soutien du Centre d'excellence de l'OTAN pour la cyberdéfense en coopération (CE-CDC OTAN) aux Manuels de Tallinn 1.0 et 2.0.

De plus amples informations sont fournies à la page 66.

6 Documents de référence

Pour la réalisation du présent Guide, il a été procédé à un inventaire des guides existants et des bonnes pratiques identifiées.

Ce travail nous a permis de repérer les matériaux d'ores et déjà disponibles pour soutenir les pays dans l'élaboration de leur stratégie nationale de cybersécurité. La liste ci-dessous fournit un catalogue complet des documents susmentionnés (avec les liens Internet).

CCI (2017), *Harare Scheme on Mutual Legal Assistance in Criminal Matters*

Carnegie Mellon (2003), *Handbook for Computer Security Incident Response*

Commonwealth (2018), *Commonwealth Cyber Declaration*

OTC (2015)*, Commonwealth Approach for Developing National Cyber Security Strategies*

Conseil de l'Europe (2001), *Convention de Budapest sur la cybercriminalité*

Conseil de l'Union européenne (2017), *boîte à outils cyberdiplomatique*

ENISA (2014), *An Evaluation Framework For National Cyber Security Strategies*

ENISA (2011), *CERT Operational Gaps and Overlaps*

ENISA (2011), *Good Practice Guide for Incident Management*

ENISA (2015), *Methodologies for the Identification of Critical Information Infrastructure Assets and Services*

ENISA (2016), *National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies*

ENISA (2012), *National Cyber Security Strategies: Practical Guide on Development and Execution*

ENISA (2012), *National Cyber Security Strategy, Setting the Course for National Efforts to Strengthen Security in Cyberspace*

ENISA (2016), *National Cyber Security Strategies: Training Tool*

ENISA (2016), *Stocktaking, Analysis and Recommendations on the Protection of CIIs*

ENISA (2016), *Strategies for Incident Response and Cyber Crisis Cooperation*

Global Cyber Security Capacity Centre, University of Oxford (2016), *Cybersecurity Capacity Maturity Model for Nations*

UIT (2017), *Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité*

UIT (2017), *Indice de cybersécurité dans le monde*

UIT (2011), *Guide sur les stratégies nationales en matière de sécurité*

UIT (2010), *COMPRENDRE LA CYBERCRIMINALITE: phénomènes, enjeux et réponse juridique*

UIT (2009), *Guide de cybersécurité pour les pays en développement*

Microsoft (2013), *Developing a National Strategy for Cybersecurity*

Microsoft (2014), *Critical Infrastructure Protection: Concepts and Continuum*

Microsoft (2014), *Critical Connections: Protecting Infrastructures*

Microsoft (2014), *Hierarchy of Cybersecurity Needs*

Microsoft (2018), *Building an effective national cybersecurity agency*

Microsoft (2015), *Information Sharing Framework for Cybersecurity*

Microsoft (2017), *Risk Management for Cybersecurity: Security Baselines*

OTAN CCD COE (2012), *National Cyber Security Framework Manual*

OTAN CCD COE (2013), *National Cyber Security Strategy Guidelines*

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*

OAS (2015), *Best Practice for Establishing a National CSIRT*

OAS (2004), *Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture*

OAS (2015), *Cyber Security Awareness Campaign Toolkit*

OAS (2015), Report Cybersecurity and Critical Infrastructure in the Americas

OCDE (2015), *Document d'accompagnement de la Recommandation sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale*

OCDE (2012), *Cybersecurity Policy Making at a Turning Point*

OCDE (2015), *Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale*

OCDE (2013), *Recommandation du Conseil sur les Principes directeurs gouvernant la protection de la vie privée et le flux transfrontière des données de caractère personnel (Privacy Guidelines)*

OCDE (2008), *Recommandation du Conseil sur la protection des infrastructures d'information critiques*

OCDE (2007), *Report on the Development of Policies for the Protection of Critical Information Infrastructures*

Institut Potomac d'études politiques (2015), *Cyber Readiness Index 2.0 – A Plan for Cyber Readiness:A Baseline and An Index*

Nations Unies (2015), *Objectifs de développement durable*

Nations Unies (1976), *Pacte international relatif aux droits économiques, sociaux et culturels, Pacte international relatif aux droits civils et politiques et Protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques*

Nations Unies (2014), *Le droit à la vie privée à l'ère du numérique, Res A/RES/68/167*

Nations Unies (1948)*, Déclaration universelle des droits de l'homme*

CNUCED (2014), *A Framework for Information and Communications Technology*

CNUCED, *Developing E-Commerce Legislation*

CNUCED (2016), *Study on Data Protection Regulations and International*

UNHR (1976), *International Covenant on Civil and Political Rights*

Banque mondiale et al (2017), *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*

Tous les détails sur les références aux principes individuels et aux bonnes pratiques peuvent être trouvés ici.

Cycle de vie d'une stratégie nationale de cybersécurité

Sous-thème	Référence
Lancement	ENISA (2016), National Cyber Security Strategies: Training Tool OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3
Inventaire et analyse	ENISA (2016), National Cyber Security Strategies: Training Tool OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 2.1, 2.2, 3.2.1, 3.3.1 OTAN CCD COE (2012): National Cyber Security Framework Manual, sections: 3.4, 4
Production de la stratégie nationale	ENISA (2016), National Cyber Security Strategies: Training Tool
Mise en oeuvre	ENISA (2016), National Cyber Security Strategies: Training Tool
Suivi et évaluation	ENISA (2016), National Cyber Security Strategies: Training Tool OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, section: 3.9 OTAN CCD COE (2012): National Cyber Security Framework Manual, section: 2.4

Principes généraux

Sous-thème	Référence
Vision	Microsoft (2013), Developing a National Cybersecurity Strategy, p.4
	OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3.1
	OCDE (2015), Recommandation sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale
	Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.1-3
Approche globale et priorités ciblées	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, p.14
	Microsoft (2013), Developing a National Cybersecurity Strategy, p.5
Approche inclusive	CCI (2013), Checklist p2
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies 4.5 and 4.6.6
	ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services, chapter 3
	ENISA (2016), An Evaluation Framework for National Cyber Security Strategies 3.2
	ENISA (2016), National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace, p.9
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, p.14
	UIT (2011), Guide sur les stratégies nationales en matière de cybersécurité, chapitre 5.3
	OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.1.3
	OTAN CCD COE (2012): National Cyber Security Framework Manual, sections: 3.4, 3.5, 4.3
	OAS (2015), Cyber Security Awareness Campaign Toolkit, p.20

Sous-thème	Référence
Approche inclusive (suite)	OAS (2015), Report on Cybersecurity and Critical Infrastructure in the Americas, p.2
	OCDE (2015), Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale, p.14-15
	OCDE (2013), Recommendation du Conseil sur les Principes directeurs gouvernant la protection de la vie privée et le flux transfrontière des données de caractère personnel (Privacy Guidelines); Supplementary Explanatory Memoran-dum to the Revised OECD Privacy Guidelines, p.31
	Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.3-6
	CNUCED (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development
	CNUCED (2014), A Framework for Information and Communications Technology Policy Reviews
Prospérité économique et sociale	Microsoft (2014), Hierarchy of Cybersecurity Needs, chapitre 1
	OTAN CCD COE (2012): National Cyber Security Framework Manual, sections: 1.5.1, 2.2.1
	Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.1-3
Droits humains fondamentaux	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, Principle 4
	ENISA (2014), An Evaluation Framework for Cyber Security Strategies, 3.1.1 Objectives
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, p.39
	UIT (2011), Guide sur les stratégies nationales en matière de cybersécurité, chapitre 7.4
	Microsoft (2013), Developing a National Cybersecurity Strategy, p.5
	OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 1.3.1, 1.3.3
	OTAN CCD COE (2012): National Cyber Security Framework Manual, sections: 1.5.4, 1.5.5, 5.2.6

Sous-thème	Référence
Droits humains fondamentaux (suite)	OCDE (2015), Document d'accompagnement de la Recommandation sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale, principle 9 et principle 3
	CNUCED (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development
	Nations Unies (1948), Déclaration universelle des droits de l'homme
	Nations Unies (1976), Pacte international relatif aux droits économiques, sociaux et culturels, Pacte international relatif aux droits civils et politiques et Protocole facultatif se rapportant au Pacte international relatif aux droits civils et politiques
	Nations Unies (2014), Le droit à la vie privée à l'ère du numérique
Gestion des risques et résilience	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.15
	Microsoft (2013), Developing a National Cybersecurity Strategy, p.6
	Microsoft (2017), Risk Management for Cybersecurity: Security Baselines
	OCDE (2015), Recommendation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale et Document d'accompagnement
Ensemble approprié d'instruments politiques	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies
	OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, section: 3.1
	OTAN CCD COE (2012): National Cyber Security Framework Manual, section: 1.4

Sous-thème	Référence
Définition claire de l'encadrement, des rôles et de l'attribution des ressources	ENISA (2016), NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies OTAN CCD COE (2012): National Cyber Security Framework Manual, section: 4 Microsoft (2018):Building an effective national cybersecurity agency Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, sections: 1-7
Environnement de confiance	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 2.2, p.25 OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3.1 Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0, sections: 4, 6

Bonnes pratiques de la stratégie nationale de cybersécurité

Sous-thème	Référence
Domaine d'intervention 1 – Gouvernance	CCI (2013), Checklist.
	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.1, 4.4.4, 4.4.5, 4.4.8, 4.4.9, 4.4.20, 4.4.21, 4.4.34, 4.5
	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.1, 3.2, 3.4, 3.5, 3.17
	ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, sections: 2.2.1, 3.1.1, 3.1.2, 3.1.3
	ENISA (2016), National Cyber Security Strategies: Setting the course for National Efforts to Strengthen Security in Cyberspace, sections: 4, 6
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, 1.5, 1.6, p.14-15
	UIT (2011): Guide sur les stratégies nationales en matière de cybersécurité, sections: 5.2.1, 5.3, 7.2, 7.3, 11.1, 11.2, 20, 20.2
	Microsoft (2013), Developing a National Cybersecurity Strategy, sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline
	Microsoft (2018) Building an effective national cybersecurity agency
	OTAN CCD COE (2013), National Cyber Security Strategy Guidelines, sections: 1.1, 3.3, 3.8
	OTAN CCD COE (2012), National Cyber Security Framework Manual, sections: 1.4.2, 2.1.1 2.1.3, 2.2, 2.3, 2.4, 3.1, 3.5, 4, 5.3.1
	OCDE (2012), Cybersecurity Policy Making at a Turning Point, Annex IV
	OCDE (2013), Recommandation du Conseil sur les Principes directeurs gouvernant la protection de la vie privée et le flux transfrontière des données de caractère personnel (Privacy Guidelines)
	OCDE (2015), Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale, 2-A, Document d'accompagnement

Sous-thème	Référence
Domaine d'intervention 1 – Gouvernance (suite)	OCDE (2015), Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale, 2-A, Document d'accompagnement OCDE (2008), Recommandation du Conseil sur la protection des infrastructures d'information critiques Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0, section 1
Domaine d'intervention 2 – Gestion des risques de cybersécurité au niveau national	ENISA (2016), National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.3 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.14 UIT (2011), Guide sur les stratégies nationales en matière de cybersécurité, section 10.1.2 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2013), Developing a National Cybersecurity Strategy, chapter on Building a Risk Approach OTAN CCD COE (2013), National Cyber Security Strategy Guidelines, section: 3.5 OTAN CCD COE (2012): National Cyber Security Framework Manual, sections: 2.1.2, 5.3.2 NIST (2015), Framework for Improving Critical Infrastructure Cybersecurity OAS (2018), Managing National Cyber Risk OCDE (2008), Recommandation du Conseil sur la protection des infrastructures d'information critiques OCDE (2015), Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0, section: 1
Domaine d'intervention 3 – Préparation et résilience	Carnegie Mellon (2003), Handbook for Computer Security Incident Response Teams (CSIRTs) CCI (2013), Checklist CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, section: 4.4.3, 4.4.20, 4.4.21, 4.4.22, 4.4.27, 4.4.31

Sous-thème	Référence
Domaine d'intervention 3 – Préparation et résilience (suite)	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.6, 3.7, 3.10, 3.14, 4.1, 4.5, 4.8
	ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, p
	ENISA (2011), CERT Operational Gaps and Overlaps, p.
	ENISA (2011), Good Practice Guide for Incident Management, p.
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.2, p.14
	UIT (2011), Guide sur les stratégies nationales en matière de cybersécurité: 11.3, 17.3
	Microsoft (2017), Risk Management for Cybersecurity: Security Baselines
	Microsoft (2015), Information Sharing Framework for Cybersecurity
	Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Building Incident Response Capabilities
	OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, Section: 3.5
	OTAN CCD COE (2012): National Cyber Security Framework Manual, sections: 3.2, 4.2.2
	OAS (2016), Best Practice for Establishing a National CSIRT, p.35
	OAS (2004), Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, pp.3-4
	OCDE (2015), Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale, section: 2-B
	Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0, sections: 2, 4
Domaine d'intervention 4 – Services d'infrastructures critiques et services essentiels	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.12, 4.4.13, 4.4.20, 4.4.25, 4.4.26, 4.4.28, 4.4.32
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, 1.4, p.14; Dimension 5.2, p.49

Sous-thème	Référence
Domaine d'intervention 4 – Services d'infrastructures critiques et services essentiels (suite)	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.6 ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, section: 4.2 UIT (2011), Guide sur les stratégies nationales en matière de cybersécurité, sections: 5.1.1, 5.3.3, 11.4 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2014), Critical Infrastructure Protection: Concepts and Continuum, all sections Microsoft (2014), Critical Connections: Protecting Infrastructures, all sections OTAN CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 3.4, 3.5 OTAN CCD COE (2012), National Cyber Security Framework Manual, section: 4.5.4 OAS (2015), Report Cybersecurity and Critical Infrastructure in the Americas OECD (2015), Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale OCDE (2008), Recommandation du Conseil sur la protection des infrastructures d'information critiques: Partie I, Partie II Institut Potomac d'études politiques (2015): Cyber Readiness Index 2.0, sections: 2, 4
Domaine d'intervention 5 – Renforcement des capacités et sensibilisation	CCI (2013), Checklist; CCI (2005, 2017), Commonwealth Network of Contact Persons Framework; CCI (2011), Harare Scheme on Mutual Legal Assistance in Criminal Matters; CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.11, 4.4.17, 4.4.20, 4.4.34, 4.4.12, 4.4.14, 4.4.16, 4.4.23 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.12, 3.8, 3.11, 3.13, 4.3, 4.6, 4.7, 4.14

Sous-thème	Référence
Domaine d'intervention 5 – Renforcement des capacités et sensibilisation (suite)	ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, section: 2.1 ENISA (2011), CERT Operational Gaps and Overlaps, p.6, 16, 19, 21, 27, 29, 31, 32, 50, 57 ENISA (2010), Good Practice Guide for Incident Management, p.19, 23, 26, 32, 46, 56, 58, 64, 69 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.5, p.15; Dimension 2.1, 2.2., 2.3, p.25; Dimension 3-1, 3-2, 3-3, p. 32; Dimension 5.6, p.49 UIT (2011), Guide sur les stratégies nationales en matière de cybersécurité, sections: 5.3.7, 5.3.8, 12.4, 12.1, 12.3, 18 Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Driving Research and Technology Investment, Public Awareness, Workforce Training and Education; OTAN CCD COE (2013, National Cyber Security Strategy Guidelines, section: 3.5 OTAN CCD COE (2012), National Cyber Security Strategy Framework Manual, sections: 4.5.5, 4.6.3; OAS (2015), Cyber Security Awareness Campaign Toolkit, all sections; OCDE (2015), Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale, section: 2-B Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0, sections: 2, 5 CNUCED (2015), Programme on E-Commerce and Law Reform
Domaine d'intervention 6 – Législation et réglementation	CCI (2013), Checklist CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4.9, 4.4.18, 4.4.19, 4.4.20 Conseil de l'Europe (2001), Convention de Budapest sur la cybercriminalité, article 15 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.15, 3.184.9, 4.12

Sous-thème	Référence
Domaine d'intervention 6 – Législation et réglementation (suite)	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, 4.2, 4.3, p.39-40; Dimension 5.7, p.50 UNHR (1976), International Covenant on Civil and Political Rights, article 19 UIT (2011), Guide sur les stratégies nationales en matière de cybersécurité, sections: 5.3.4, 5.3.5, 9, 11.5, 12.2, 15 UIT (2010), Kit pratique UIT pour la législation sur la cybercriminalité OTAN CCD COE (2013), National Cyber Security Strategy Guidelines, section: 3.2 OTAN CCD COE (2012), National Cyber Security Strategy Framework Manual, section: 5 OAS: Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0, section: 3 ONU (2015), Objectifs de développement durable, article 16.3 CNUCED, Global Cyberlaw Tracker Banque mondiale et al., Combatting Cybercrime: Tools and Capacity Building for Emerging Economies
Domaine d'intervention 7 – Coopération internationale	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.20, 4.4.21 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.16 and 4.10 ENISA (2016), Guidebook on National Cyber Security Strategies, section: 3.16 Global Cyber Security Capacity Centre, University of Oxford(2016), Cybersecurity Capacity Maturity Model for Nations(CMM), Dimension 4.3, p.40 UIT (2011), Guide sur les stratégies nationales en matière de cybersécurité, sections:5.3.9, 10.2.2, 13, 19 Microsoft (2013), Developing a National Strategy for Cybersecurity, section on structuring international engagement OTAN CCD COE (2013), National Cyber Security Strategy Guidelines, sections: 1.3, 3.2.1, 3.3.2

Sous-thème	Référence
Domaine d'intervention 7 – Coopération internationale (suite)	OTAN CCD COE (2012), National Cyber Security Strategy Framework Manual, sections: 4.7, 5.4.2, 5.4.3 OCDE (2008), Recommandation du Conseil sur la protection des infrastructures d'information critiques, chapitres: 4, 5 OCDE (2015), Recommandation du Conseil sur la gestion du risque de sécurité numérique pour la prospérité économique et sociale, p. 13, 48, 58 Institut Potomac d'études politiques (2015), Cyber Readiness Index 2.0, sections: 4, 6

7 Acronymes

Acronyme	Définition
CCI	Commonwealth Cybercrime Initiative
CERT	Equipe d'intervention en cas d'urgence informatique
CBM	Mesures de renforcement de la confiance
CII	Infrastructure de l'information essentielle
OTC	Organisation des télécommunications du Commonwealth
ENISA	Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information
TIC	Technologies de l'information et de la communication
UIT	Union internationale des télécommunications
OTAN CCD COE	Centre d'excellence de coopération pour la cyberdéfense de l'OTAN
NIST	National Institute of Standards and Technology
OAS	Organisation des Etats américains
OCDE	Organisation de coopération et de développement économiques
ONU	Organisation des Nations Unies
CNUCED	Conférence des Nations Unies sur le commerce et le développement

ISBN: 978-92-61-27792-5