KM2 : STRATÉGIE, POLITIQUE ET RÉGLEMENTATION EN MATIÈRE DE CYBERSÉCURITÉ

OBJECTIF DU MODULE DE CONNAISSANCES

Bienvenue dans le module de connaissances sur la stratégie, la politique et la réglementation en matière de cybersécurité. Ce module fournit un guide pour l'élaboration de stratégies nationales en matière de cybersécurité, qui permettra de soutenir les objectifs nationaux. Dans ce module, vous découvrirez également deux des principaux leviers pour la mise en œuvre des stratégies : la législation et la réglementation. Le module repose sur des études de cas et sur les meilleures pratiques du domaine.

À la fin de ce module, vous serez en mesure de répondre aux questions suivantes et de trouver des ressources supplémentaires les concernant :

- Un pays a-t-il besoin d'une stratégie nationale de cybersécurité, et quel doit en être le contenu ?
- Quelles sont les sources d'information et de soutien en mesure de faciliter l'élaboration d'une stratégie nationale ?
- Quels sont les leviers dont un gouvernement dispose pour garantir la mise en œuvre de la stratégie ?
- Quel est le rôle de la législation et de la réglementation, et comment sont-elles élaborées ?
- Quelles sont les sources d'information et de soutien en mesure de faciliter l'élaboration de la législation et de la réglementation ?
- Comment certains pays africains ont-ils abordé l'élaboration de stratégies et quels sont les enseignements à tirer de ces approches ?
- Comment suivre et évaluer la mise en œuvre des stratégies ?
- Quand entamer un autre cycle de vie de la stratégie ?

INTRODUCTION

La dépendance accrue envers la technologie numérique à l'échelle mondiale apporte son lot de risques et de menaces. Une stratégie de cybersécurité est un document de haut niveau conçu pour gérer les risques et les problèmes liés à l'utilisation des technologies numériques. L'élaboration d'une stratégie nationale de cybersécurité présente l'avantage d'offrir un degré de certitude en matière de gouvernance de la cybersécurité, ce qui aura pour effet d'accroître la confiance des utilisateurs des technologies numériques et de fournir les outils, les politiques et les lignes directrices nécessaires pour la gestion des risques.

Une fois la stratégie élaborée, la responsabilité de coordonner sa mise en œuvre incombe au gouvernement. La mise en œuvre réussie des stratégies dépend de la façon dont les gouvernements emploient les différents leviers à leur disposition et de la perception concernant la meilleure façon d'utiliser ces leviers pour parvenir aux résultats souhaités. Ces leviers et la manière dont les gouvernements peuvent les utiliser sont généralement décrits dans la stratégie.

La législation et les réglementations sont deux des leviers les plus efficaces que les gouvernements et leurs agences peuvent adopter pour mettre en œuvre des stratégies fonctionnelles. Ces leviers permettent de créer des institutions, d'établir des relations et d'attribuer les responsabilités nécessaires à la mise en œuvre réussie des stratégies. L'objectif et la manière de développer l'utilisation des législations et des réglementations peuvent varier d'un pays à l'autre, en fonction des priorités et des autres cadres juridiques existants. Ce module fournira un guide sur la façon d'aborder les options dont dispose un gouvernement et d'envisager comment développer la législation ou la réglementation en vue d'atteindre les objectifs de sa stratégie.

QU'EST-CE QU'UNE STRATÉGIE NATIONALE DE CYBERSÉCURITÉ ?

L'Agence de l'Union européenne pour la cybersécurité (ENISA) définit une stratégie nationale de cybersécurité comme « un plan d'actions visant à améliorer la sécurité et la résilience des infrastructures et services nationaux ». Il s'agit d'une approche descendante de haut niveau en matière de cybersécurité, qui établit une série de priorités et d'objectifs nationaux à atteindre dans un délai précis. Elle peut également être décrite comme une méthode ou un plan minutieux de protection des actifs informationnels et non informationnels par l'intermédiaire de l'infrastructure TIC, pour atteindre des objectifs nationaux particuliers, généralement sur une longue période (Azmi et al.).

Habituellement, les stratégies nationales de cybersécurité sont des plans nationaux de haut niveau, orientés vers les parties prenantes, que les gouvernements utilisent pour décrire des questions telles que :

- La vision, les objectifs de haut niveau, les principes et les priorités qui guideront le pays dans la prise en charge de la cybersécurité ;
- Un aperçu des parties prenantes chargées d'améliorer la cybersécurité à l'échelle du pays, ainsi que de leurs rôles et responsabilités respectifs ; et

- Les mesures, les programmes et les initiatives que le pays mettra en œuvre pour protéger sa cyberinfrastructure nationale et, dans le même temps, accroître sa sécurité et sa résilience.

[Source : *Guide pour l'élaboration d'une stratégie nationale de cybersécurité* - (Union internationale des télécommunications (UIT) et al. 2018, 13)]

L'élaboration de la SNC ne se limite pas strictement à la seule cybersécurité. Elle peut également être un outil de développement économique. Il existe différentes phases et activités qui pourraient s'inscrire dans le développement et la mise en œuvre d'une stratégie nationale de cybersécurité. Ces activités et ces résultats sont généralement désignés comme le cycle de vie de la stratégie. Nous aborderons ce point dans la suite du document. Le Guide de l'Union internationale des télécommunications (UIT) pour l'élaboration d'une stratégie nationale de cybersécurité définit neuf principes directeurs qui devraient aider les responsables et les parties prenantes tout au long du cycle de vie de la stratégie. Ces principes ne sont pas limités à une phase du cycle et ils doivent être considérés comme un tout, car ils s'appliquent à tous les domaines d'intervention clés de la SNC. Ces principes sont décrits dans le diagramme ci-dessous.

Figure 1. Schéma des principes directeurs du processus de SNC.

Point de réflexion
Connaissez-vous une stratégie nationale de votre pays dans un domaine ou un sujet donné ? Dans l'affirmative, veuillez en examiner la structure.

STRATÉGIES DE CYBERSÉCURITÉ EN AFRIQUE

De manière générale, les pays africains n'ont que peu progressé dans l'élaboration et la mise en œuvre d'une stratégie nationale de cybersécurité. Des informations récentes indiquent que

seuls 17 des 54 pays d'Afrique ont achevé une stratégie nationale de cybersécurité, soit moins de la moitié de la moyenne mondiale, comme le montre la carte ci-dessous.

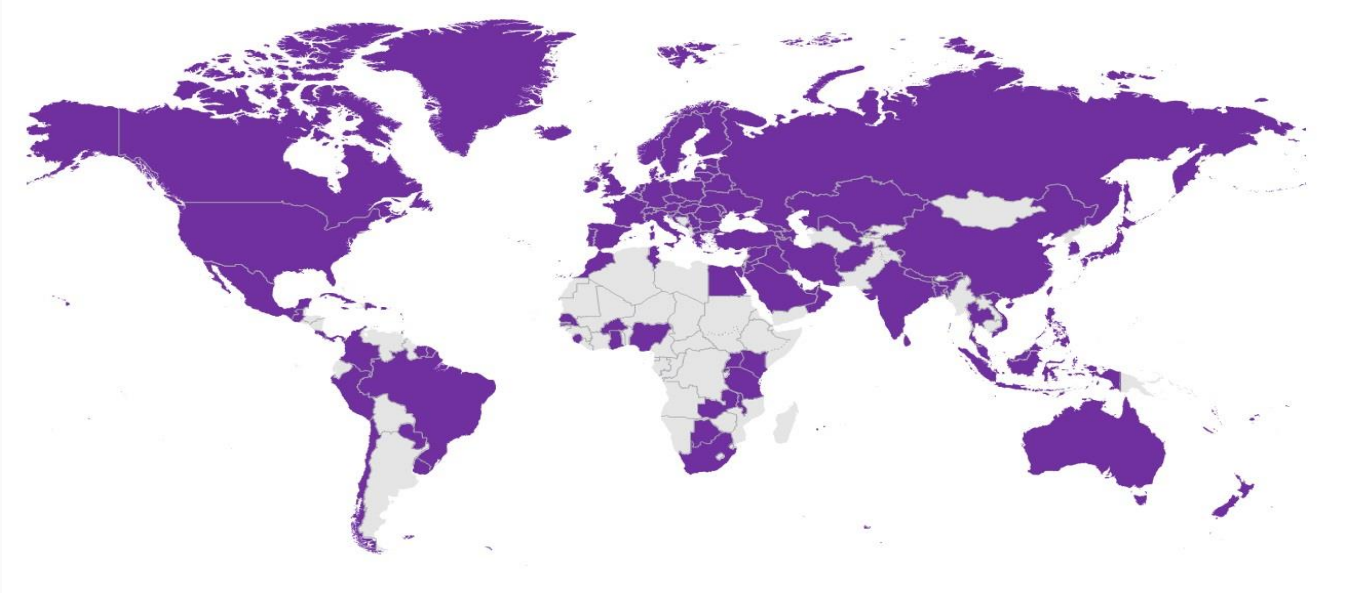


Fig. 2 Représentation des pays dotés d'une SNC
Source : Référentiel des stratégies nationales de cybersécurité *de l'UIT*

Les pays d'Afrique dotés de stratégies de cybersécurité en sont arrivés à différents niveaux d'élaboration et de mise en œuvre. Le tableau ci-dessous indique l'état d'avancement de ces stratégies.

Stratégies nationales de cybersécurité en Afrique						
Pays	Évaluation des menaces	Plan d'action	Calendrier	Attribution des responsabilités	Allocation des ressources	Dernière mise à jour
Bénin	✓	✓		✓		2020
Burkina Faso		✓				2019
Égypte	✓	✓	✓			2018
Eswatini	✓	✓	✓	✓	✓	2020
Gambie		✓		✓		2016
Ghana		✓	✓	✓		2020
Kenya	✓	✓	✓	✓	✓	2014
Malawi		✓	✓	✓	✓	2017
Maurice		✓	✓	✓		2014
Maroc		✓	✓	✓	✓	2013
Nigeria	✓	✓	✓	✓		2021
Rwanda		✓	✓	✓	✓	2015
Sénégal	✓	✓	✓	✓	✓	2017
Sierra Leone	✓	✓	✓		✓	2017
Afrique du Sud		✓		✓		2012
Tanzanie		✓		✓		2016
Ouganda		✓				2014
TOTAL	7	17	11	13	7	

Fig. 3. Stratégies de cybersécurité en Afrique

Source : Centre d'études stratégiques de l'Afrique, article « Leçons d'Afrique en matière de cyber-stratégie »

Malheureusement, l'existence d'un document intitulé « stratégie nationale de cybersécurité » n'est pas suffisante pour aborder les questions de cybersécurité à l'échelle nationale. La question pertinente concerne sa mise en œuvre et son impact sur le pays. L'article intitulé « Leçons d'Afrique en matière de cyber-stratégie » (Ajijola et Allen) identifie les stratégies de trois pays qu'il considère comme répondant aux critères minimaux essentiels en Afrique : l'Eswatini, le Kenya et le Sénégal. Ces critères incluent notamment :

- Une évaluation des menaces qui identifie la portée et l'ampleur des cybermenaces d'un pays
- Un plan d'action qui contient des objectifs et des activités concrets destinés à faire face aux menaces
- Un calendrier
- Une répartition des responsabilités entre les principales parties prenantes
- Des dispositions claires en matière d'affectation des ressources

La stratégie de cybersécurité de l'Eswatini définit clairement la portée de la stratégie, qui couvrira tous les secteurs du pays et fournira à toutes les parties prenantes concernées des lignes directrices sur leurs rôles et responsabilités attendus. Le contexte stratégique a permis d'identifier les menaces et les vulnérabilités, tandis que l'examen des capacités a contribué à déterminer l'état actuel de la cybersécurité dans le pays.

La stratégie a également décrit son alignement sur l'objectif national du pays et définit ses propres objectifs, à savoir : améliorer la sécurité et la résilience ; renforcer la gouvernance de la cybersécurité, de même que les cadres politiques, réglementaires et législatifs ; renforcer les capacités et l'expertise de l'Eswatini en matière de cybersécurité ; favoriser une société de l'information sûre et sécurisée pour l'Eswatini ; et renforcer la coopération, la collaboration et les partenariats en matière de cybersécurité. La stratégie attribue également des rôles et des responsabilités pour la mise en œuvre, y compris un cadre de suivi et d'évaluation.

Le même modèle est adopté pour le Kenya et le Sénégal. L'un des facteurs stratégiques pour la réussite de l'élaboration et de la mise en œuvre d'une stratégie nationale de cybersécurité est le besoin d'inclusion, qui permettrait de fournir les ressources nécessaires à son élaboration et à sa mise en œuvre.

Point de réflexion
Selon vous, pour quelles raisons la plupart des pays africains n'ont-ils pas encore élaboré une stratégie nationale de cybersécurité ?

AVANTAGES ET UTILISATIONS D'UNE STRATÉGIE DE CYBERSÉCURITÉ

L'élaboration d'une stratégie de cybersécurité présente plusieurs avantages pour un pays. Le principal avantage est qu'un pays doté d'une stratégie devrait obtenir de meilleurs résultats en matière de cybersécurité qu'un pays sans stratégie. Offrant des mesures et des plans pour répondre aux menaces liées à l'utilisation des technologies numériques, la stratégie de cybersécurité constitue une mesure de confiance qui soutient l'utilisation des technologies numériques pour parvenir au développement économique. Elle fournit également un cadre

pour la coopération internationale en abordant les questions mondiales relatives à la cybersécurité.

Une stratégie de cybersécurité présente d'autres avantages, dans la mesure où elle peut faciliter les opérations suivantes :

- Déterminer comment la cybersécurité peut soutenir les objectifs nationaux de plus haut niveau, tels que la croissance économique, la défense, l'éducation, la sécurité des citoyens, etc.
- Hiérarchiser les efforts et les investissements en matière de cybersécurité.
- Créer une feuille de route ou un plan d'action pour passer de l'état actuel à l'état de préparation et aux capacités de cybersécurité souhaitées par le pays.
- Garantir que l'approche nationale de la cybersécurité reflète les valeurs nationales.
- Améliorer la communication et la coopération entre tous les ministères et agences concernés par la cybersécurité.
- Clarifier ou modifier les responsabilités de ces ministères et agences.
- Prescrire la création de nouvelles institutions ou agences.
- Fixer des objectifs pour les ministères et les agences, avec un processus de rapport pour que les ministres et les fonctionnaires puissent suivre les progrès et identifier rapidement les problèmes.
- Améliorer la coopération entre les ministères et les organisations clés extérieures au gouvernement, dans le secteur privé et la société civile, qui sont nécessaires pour mettre en œuvre la SNCS et améliorer la cybersécurité nationale.
- Encourager le soutien à l'effort national de cybersécurité en impliquant les entreprises, la société civile et même les citoyens dans le processus de décision concernant les priorités de la stratégie et la façon d'atteindre ses objectifs.

Les catégories d'utilisation des SNCS peuvent être divisées en trois grands secteurs (Azmi et al.). Le premier secteur majeur est celui de la sécurité nationale. Dans ce cadre, les stratégies sont principalement utilisées comme des outils destinés à réduire les cybermenaces contre les infrastructures nationales critiques, en renforçant la résilience nationale au niveau des CNI et en protégeant les secrets d'État. Dans certains cas, elles peuvent également servir d'outil pour promouvoir la sécurité et la prospérité économiques. Deuxièmement, la stratégie pourrait servir un objectif jurisprudentiel, car elle pourrait être une exigence d'autres documents politiques ou d'une loi. Elle pourrait également être un mandat de l'agence gouvernementale requise par la loi. Ainsi, la création de la SNCS répond aux exigences de la loi ou d'autres politiques. Troisièmement, elle peut être utilisée pour répondre à des besoins politiques. Elle peut parfois s'imposer par la volonté politique de créer une SNC. À l'ère moderne de la diplomatie numérique, la SNC pourrait servir d'outil diplomatique pour mobiliser des ressources en vue de poursuivre le développement et de promouvoir l'image d'un pays.

Étude de cas : Ghana

- 2008 création de l'Agence nationale des technologies de l'information
- 2015 publication de la SNCS. La stratégie prévoit la création de quatre nouvelles institutions : le Conseil national de cybersécurité, le Centre national de cybersécurité, la CSIRT nationale et le Groupe de travail sur la politique nationale de cybersécurité.
- 2018 création du Centre national de cybersécurité
- Adoption de la loi sur la cybersécurité de 2020 (loi 1038) destinée à réglementer les activités de cybersécurité au Ghana

PHASES DE L'ÉLABORATION ET DE LA MISE EN ŒUVRE D'UNE STRATÉGIE NATIONALE

L'élaboration et la mise en œuvre d'une politique et d'une stratégie nationales de cybersécurité comportent plusieurs phases et activités. C'est ce que nous appelons le cycle de vie de la politique et de la stratégie. Le guide de la SNC recommande le modèle suivant pour les étapes du cycle de vie d'une politique et d'une stratégie :

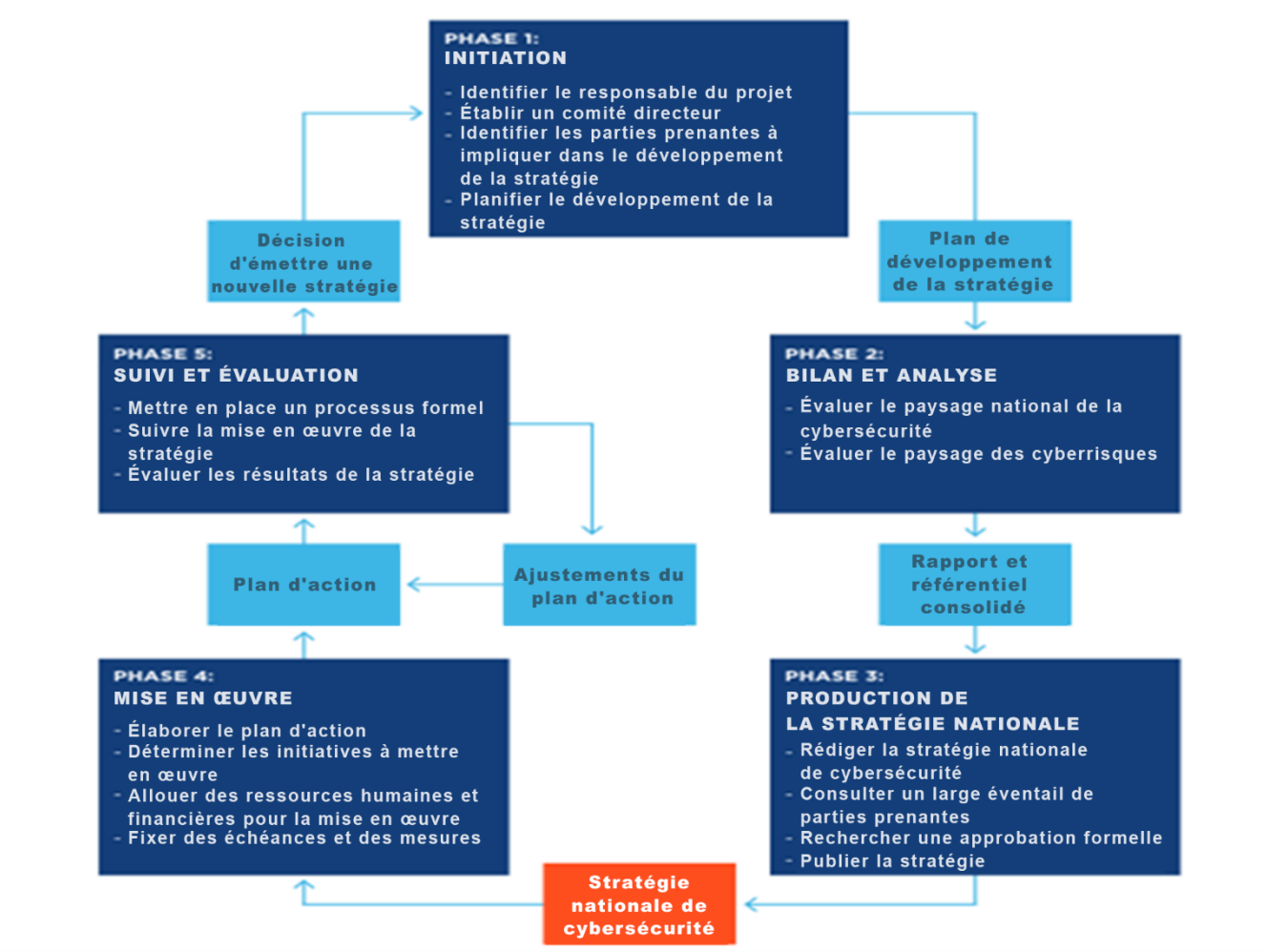
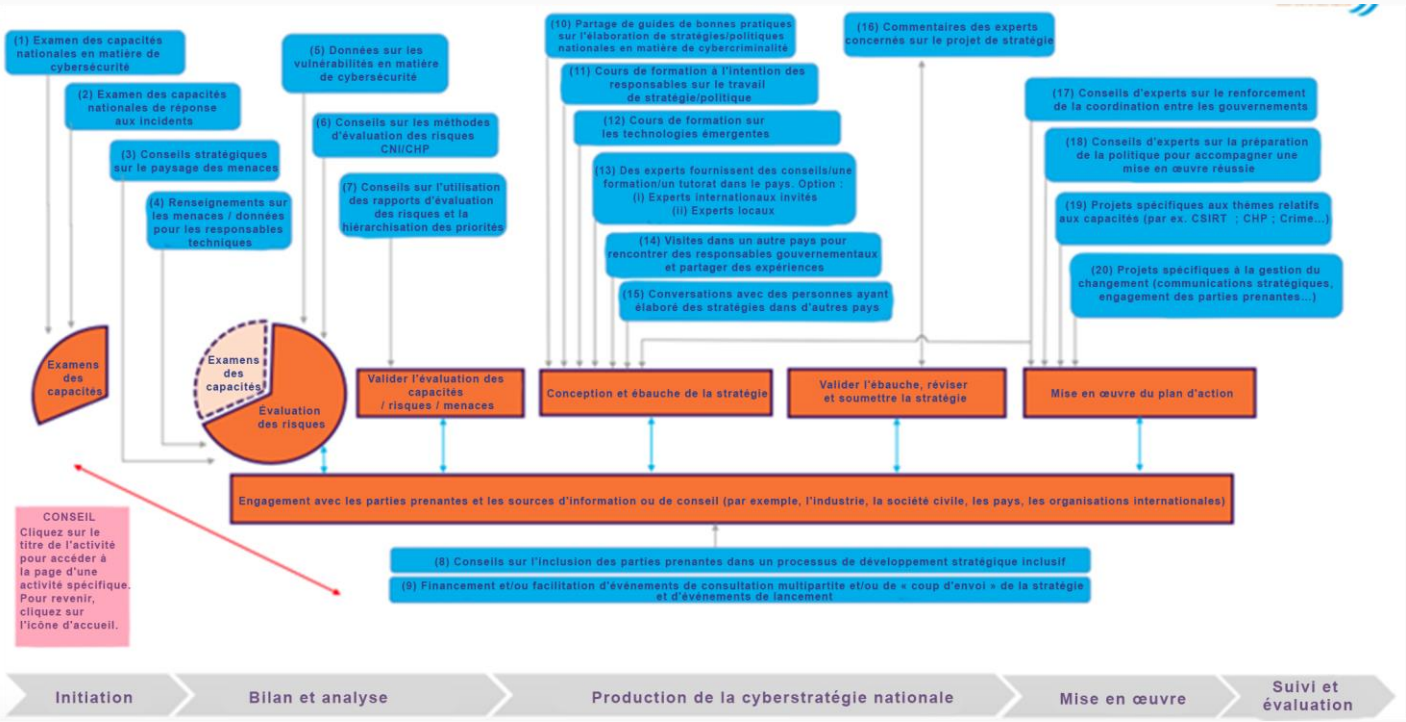


Figure 4. Représentation de l'ensemble du processus et du cycle de vie d'une SNC.

Lorsqu'un pays envisage de développer une SNC, il peut bénéficier de diverses opportunités d'assistance internationale tout au long du cycle de vie de la stratégie. Le GFCE a illustré les différents types d'assistance auxquels un pays peut faire appel dans son *Catalogue des options de projet pour le cycle de la stratégie nationale de cybersécurité (SNC)* Ce catalogue offre des exemples de 20 activités qui pourraient s'inscrire dans un projet soutenant le cycle de la SNC d'un pays. Nous recommandons d'utiliser le catalogue comme un document de référence afin de comprendre le soutien disponible pour les pays, offrant des exemples fournis par des études de cas.



Avant ou pendant l'**initiation** d'une stratégie nationale, un pays peut bénéficier d'examens des capacités/compétences couvrant la situation nationale globale et/ou se concentrant sur des capacités spécifiques telles que la réponse nationale aux incidents.

Une fois que le processus de développement de la stratégie a été initié (souvent par l'orientation politique d'un ministre), la phase d'**inventaire et d'analyse** commence. L'un des principaux facteurs qu'un pays doit explorer dans cette phase relève des cyberrisques auxquels il est confronté, ainsi que des menaces et des vulnérabilités qui contribuent à ces risques. Il est possible de solliciter l'assistance de partenaires internationaux pour bien comprendre ces risques. Les projets peuvent notamment fournir des conseils sur le paysage stratégique des risques, les données de renseignement sur les menaces, les données sur les vulnérabilités nationales en matière de cybersécurité ou les méthodologies d'évaluation du cyberrisque pour les infrastructures nationales essentielles. Ce bilan peut rassembler bon nombre de données et d'évaluations. Les pays peuvent donc demander de l'aide pour regrouper toutes ces informations, les hiérarchiser et les utiliser pour en tirer des enseignements qui serviront à rédiger la stratégie.

Si ce n'est déjà fait, la phase de bilan et d'analyse est le moment idéal pour que les gouvernements entreprennent ou renforcent leur communication et leur collaboration avec les parties prenantes externes de la SNCS. Ces parties prenantes comprennent généralement le secteur privé, les universités, les groupes de réflexion, les ONG, les médias et, enfin, le public du pays. L'assistance internationale peut offrir des conseils sur la manière d'impliquer ces parties prenantes dans le cycle de vie de la stratégie et mener les événements avec les parties prenantes pour discuter de la stratégie.

Après avoir recueilli et analysé les informations, et commencé à consulter les parties prenantes, un pays peut passer à la phase de **production de la stratégie nationale**. Afin de bénéficier de l'aide internationale au moment d'entamer cette phase, l'un des moyens les plus rapides consiste à lire les guides de bonnes pratiques et d'enseignements concernant l'élaboration de la stratégie/politique nationale. Le *Guide pour l'élaboration d'une stratégie nationale de cybersécurité* est une source qui a déjà été mentionnée, mais il en existe d'autres

comme les *Stratégies nationales de cybersécurité : réflexions et enseignements tirés des Amériques et d'autres régions* de l'Organisation des États américains. Le portail Cybil propose un référentiel de ces guides.

Outre la lecture de guides de bonnes pratiques, il peut également être utile de discuter avec les responsables d'autres pays qui ont eux-mêmes élaboré des stratégies nationales. Cette démarche présente un avantage supplémentaire dans la mesure où elle peut créer ou renforcer entre les pays des réseaux de travail qui peuvent se révéler utiles lors de la mise en œuvre de la stratégie. Ces conversations peuvent avoir lieu à distance, mais elles peuvent aussi être menées en personne lors de visites dans d'autres pays.

Diverses options permettent un apprentissage et un partage des connaissances plus poussés sur le développement de la stratégie, qui vont au-delà des conversations et des visites. L'une de ces options consiste à envoyer des responsables suivre des cours de formation portant sur la stratégie et la politique de cybersécurité ou sur des questions clés de la stratégie, telles que les technologies émergentes. Une autre solution consiste à faire appel à des experts internationaux ou locaux pour fournir des conseils indépendants et un soutien à l'élaboration de la stratégie. Si ce n'est pas une bonne pratique de demander à ces experts de rédiger la stratégie, il est courant de solliciter l'assistance d'experts extérieurs au gouvernement. Ces experts peuvent également contribuer à renforcer la coordination et la collaboration au sein du gouvernement pour élaborer la stratégie, par exemple en animant des ateliers interministériels.

Une fois que les responsables ont préparé un projet de stratégie, ou des chapitres de cette stratégie, ils peuvent inviter des experts indépendants à leur faire part de leurs commentaires en toute confidentialité. Après avoir pris en compte les commentaires des experts et les consultations des parties prenantes, les responsables modifieront le projet afin qu'il soit prêt à être examiné par les ministres, puis approuvé et adopté.

Une bonne pratique veut qu'une SNCS soit accompagnée d'un plan d'action qui guidera sa mise en œuvre. Un plan d'action présente de façon détaillée les actions requises par la stratégie, les responsables, le moment où elles seront exécutées et les indicateurs qui seront utilisés pour vérifier que l'action a été menée à bien.

Le cycle de vie d'une stratégie ne se termine pas avec son adoption. Les phases suivantes consistent à **mettre en œuvre** la stratégie, puis à en assurer **le suivi et l'évaluation**. Après quelques années, une actualisation de la stratégie est généralement lancée et le cycle recommence.

Pendant la mise en œuvre de la stratégie, une assistance internationale permet de soutenir le renforcement des cybercapacités dans différents domaines, notamment : la réponse aux incidents, la protection de la CNI et des infrastructures d'information critiques, la lutte contre la cybercriminalité, la sensibilisation du public, les compétences de la main-d'œuvre, les normes et la cyberdiplomatie. Les responsables peuvent également obtenir de l'aide pour élaborer les politiques nationales en matière de cybersécurité et de cybercriminalité qui relèvent de la stratégie.

LES LEVIERS PERMETTANT DE PILOTER LA MISE EN ŒUVRE DE LA STRATÉGIE

Un gouvernement dispose d'une série de leviers pour piloter la mise en œuvre de sa SNCS. Comme nous le verrons dans la suite de ce module, deux de ces leviers sont la législation et la réglementation, mais ce ne sont pas les seuls. Les leviers qu'un gouvernement choisit

d'utiliser, et la façon de procéder, dépendent des circonstances nationales et de l'approche de la politique.

Un gouvernement dispose des leviers suivants :

- Créer des normes et des outils liés à la cybersécurité pour favoriser la certitude et la facilité dans les activités de cybersécurité. Exemples : établissement d'un système de certification pour permettre aux entreprises de choisir plus facilement des fournisseurs sûrs ou compétents ; création d'un outil en ligne que toute entreprise, organisation ou agence peut utiliser pour confirmer la sécurité de son site Web ; création de mécanismes de partage d'informations et de communautés de confiance.

- Fournir des connaissances et une éducation aux organisations et aux citoyens. Exemples : campagnes de sensibilisation du public ; programmes d'enseignement ; remise de guides/boîtes à outils de cybersécurité aux petites entreprises ; diffusion par une CSIRT nationale ou un centre de cybersécurité d'alertes sur les vulnérabilités et les menaces.

- Fournir des récompenses ou des incitations pour une bonne cybersécurité. Exemples : utiliser la politique des marchés publics pour acheter des services informatiques auprès d'entreprises dotées de certificats de cybersécurité, en vue de les inciter à achever la certification.

- Le gouvernement montre l'exemple par la pratique de la cybersécurité. Exemples : le gouvernement peut commencer à déployer de meilleures approches de cybersécurité (par exemple, l'authentification à deux facteurs ou l'authentification par e-mail) en les adoptant d'abord dans les ministères puis en les faisant connaître à l'industrie.

- Exercer une pression sans criminaliser. Exemple : établir des listes de « mauvais élèves » concernant la mise en œuvre d'une pratique de cybersécurité recommandée spécifique qu'ils devraient mettre en œuvre ; ces listes pourraient être publiées ou partagées avec les seules entreprises concernées.

- Investissements publics et partenariats public-privé. Exemple pour lequel les gouvernements et le secteur privé partagent des informations sur les vulnérabilités de la CNI pour y remédier de manière adéquate par la collaboration.

- Financement de la recherche universitaire.

Outre les leviers susmentionnés, un gouvernement dispose d'une législation et d'une réglementation, qui se prêtent à de nombreuses utilisations, notamment :

- Conférer de nouveaux rôles, pouvoirs ou autorités à une agence gouvernementale ou à un organisme externe auquel le gouvernement a confié un rôle national en matière de cybersécurité ;

- Créer une nouvelle agence ou organisation ;

- Confier aux entreprises, aux autres organisations ou aux citoyens la responsabilité de certaines actions que le gouvernement souhaite promouvoir (par exemple, la protection des données d'une manière définie ou le signalement des violations) ; et

- Faire une infraction des actes que le gouvernement veut dissuader.

Les leviers à la disposition d'un gouvernement peuvent être considérés sur une échelle allant de l'encouragement fort (la « carotte »), à une extrémité, à la dissuasion forte (le « bâton »), à l'autre.

Étude de cas pour le levier de l'encouragement :

1. La boîte à outils pour les PME au Nigeria
2. Sensibilisation à la cybersécurité au Ghana
3. Africa CERT est un bon exemple de collaboration entre les gouvernements et le secteur privé sur le continent africain.

RÔLE DE LA LÉGISLATION ET DE LA RÉGLEMENTATION

Chaque pays a une approche spécifique de la législation et de la réglementation. D'un point de vue procédural, la législation est produite par un corps législatif (par exemple, le parlement), tandis que la réglementation (législation secondaire, législation déléguée ou législation subordonnée) est émise par la bureaucratie. Toutefois, la publication d'une directive particulière en matière de cybersécurité sous forme de législation ou de réglementation relève de la tradition politique et juridique de chaque pays.

En outre, les pays ne sont pas la seule source de réglementation de la cybersécurité : celle-ci peut également provenir d'organismes internationaux de plus haut niveau. Par exemple, le Forum mondial de l'harmonisation des règlements concernant les véhicules a adopté en 2020 un règlement des Nations Unies sur la cybersécurité des logiciels dans les véhicules. Dans le contexte africain, l'Union africaine (UA) a adopté la Convention sur la cybersécurité et la protection des données à caractère personnel (connue sous le nom de Convention de Malabo) en 2014. Cette convention a été suivie par la publication des Lignes directrices sur la protection des données personnelles pour l'Afrique, une mesure collaborative entre l'Internet Society et l'UA en 2018.

Dans bien des cas, les gouvernements nationaux sont libres de choisir s'ils adoptent les réglementations négociées au niveau international dans leurs propres lois et réglementations nationales. Cependant, les gouvernements peuvent avoir déjà accepté d'adopter toutes les réglementations émises par un organisme international spécifique. L'adoption de normes industrielles internationales fait également l'objet de fortes incitations économiques : par exemple, si un pays veut exporter des voitures, ses entreprises doivent respecter les normes internationales en matière de sécurité automobile.

Une façon de simplifier l'approche de la législation et de la réglementation consiste à commencer par la stratégie nationale. Cette stratégie doit définir la vision et les objectifs nationaux en matière de cybersécurité. Lors de l'élaboration de la stratégie, les responsables examinent quelle législation et quelle réglementation seront nécessaires pour atteindre ces objectifs et vérifient s'il existe des lacunes ou des faiblesses dans le cadre juridique et réglementaire existant. En présence de lacunes importantes ou lorsque des changements majeurs s'imposent, la stratégie peut stipuler qu'ils soient traités, par exemple en chargeant un ministère de préparer et de présenter au Parlement un projet de loi avant une certaine date.

Le *Guide pour l'élaboration d'une stratégie nationale de cybersécurité* décrit plusieurs éléments du cadre juridique et réglementaire sur lesquels une SNCS pourrait donner des instructions, à savoir :

- la définition de la notion de cyberactivité illégale ;

- la reconnaissance juridique des droits individuels et des libertés civiles ;
- l'institutionnalisation des entités et agences essentielles ;
- la mise en place de mécanismes de conformité pour prévenir, combattre et atténuer les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes et infrastructures TIC ; ces mécanismes peuvent notamment comprendre des règles d'approvisionnement, des programmes de partage d'informations, la divulgation des vulnérabilités, des normes minimales de diligence, des bases de référence de sécurité et des programmes de certification ; et
- la coopération internationale en matière de cybercriminalité et de cybersécurité est importante.

(Source : *Guide pour l'élaboration d'une stratégie nationale de cybersécurité*, p.40, 46)

PROCESSUS D'ÉLABORATION DE LA LÉGISLATION ET DE LA RÉGLEMENTATION PARTIE 1
(DE LA STRATÉGIE À LA POLITIQUE)

Après avoir identifié la législation et la réglementation comme certains des leviers qu'un gouvernement peut déployer pour mettre en œuvre une stratégie nationale, il est nécessaire d'examiner le processus de conversion des objectifs en législation. Le processus d'élaboration de la législation et de la réglementation varie largement d'un pays à l'autre. Dans cette section, nous allons présenter une approche générique qui peut être appliquée dans la plupart des pays.

Comme mentionné plus haut, la SNCS est un document présentant la vision, les objectifs de haut niveau, les principes et les priorités qui guideront le pays dans la prise en charge de la cybersécurité. Cela signifie que, dans la plupart des cas, le sujet qui nécessite un effet de levier par le biais de la législation a été identifié dans la SNCS. Ainsi, le processus d'élaboration de la stratégie devrait avoir contribué à produire une liste hiérarchisée des problèmes de cybersécurité que le gouvernement doit traiter.

Sur la base de ces domaines prioritaires et de ces objectifs, la pratique courante consiste à décomposer les objectifs et les domaines prioritaires en orientations politiques, qui pourraient constituer la base de la législation ou de la réglementation. Cette opération peut intervenir soit pendant le processus d'élaboration de la stratégie, soit pendant les années qui séparent la rédaction de la stratégie de sa mise en œuvre. Certains pays désignent un groupe chargé de la politique de cybersécurité, composé d'experts au sein (et parfois à l'extérieur) du gouvernement, pour fournir des conseils sur les domaines d'action à privilégier et sur le contenu des politiques elles-mêmes. Au Ghana, il s'agissait du groupe de travail national sur la cybersécurité, tandis qu'au Nigeria, il était appelé groupe de travail nigérian sur la cybercriminalité.

Parmi les domaines d'action possibles, citons l'interdiction de la cybercriminalité, la protection des données, la cybersécurité dans les secteurs clés (par exemple, l'énergie, la finance, l'administration en ligne et la santé), l'assurance technologique, l'éducation, la main-d'œuvre et la sensibilisation. Le « double diamant décisionnel » décrit dans le document *National Cybersecurity Strategies: Lessons Learned and Reflections from The Americas and Other Regions* est un outil qui peut aider à passer des objectifs stratégiques aux initiatives politiques (et donc aux domaines politiques). Parmi les questions typiques de cybersécurité qui devraient être abordées figurent la cybercriminalité, la protection des données personnelles, la protection des réseaux critiques, les réglementations sectorielles, par exemple la finance, l'énergie, la santé, les réglementations spécifiques aux produits, par exemple les appareils, les avions, les

voitures, les transactions électroniques, les signatures numériques, la certification des normes de cybersécurité des entreprises/organisations, etc.

À l'étape suivante, après avoir identifié un domaine d'action clé, un gouvernement décide généralement d'élaborer une politique correspondante. C'est dans cette politique que le gouvernement décidera des leviers à utiliser pour mettre en œuvre la politique et déterminera si la législation ou la réglementation doit en faire partie. L'élaboration d'une politique commence généralement par une orientation ministérielle, afin de fixer le cadre et le calendrier, puis par une consultation qui peut être informelle ou formelle.

La consultation informelle peut avoir lieu avant que « les choses ne soient mises par écrit ». Un bon moment pour amorcer la consultation informelle correspond à l'élaboration de la SNCS, mais la consultation ne doit pas être remise à plus tard simplement parce qu'aucune stratégie n'est en cours d'élaboration à ce moment-là. La consultation informelle aide les responsables à élaborer un cadre d'idées sur le problème et les solutions politiques qui peuvent être discutées avec les ministres, puis soumises à un processus de consultation formel.

La *consultation formelle* implique généralement la publication de documents sur lesquels les parties prenantes peuvent donner leur avis. En Afrique du Sud, par exemple, l'élaboration des politiques suit une approche commune de la consultation, en utilisant deux séries de documents. Le premier cycle est basé sur un document de discussion appelé « livre vert ». Le livre vert exprime la position du gouvernement sur une question particulière. Il est publié en sollicitant une demande de commentaires du public. Il arrive que le livre vert soit suivi d'un document de discussion plus précis, appelé livre blanc. Le livre blanc est une déclaration générale de la politique du gouvernement, et peut inviter des commentaires publics supplémentaires sur la question. Les commissions parlementaires compétentes peuvent proposer des amendements ou d'autres propositions, puis renvoyer le document de politique générale au ministère pour de nouvelles discussions et des décisions finales.

Le processus de consultation répartira les parties prenantes en groupes, en fonction de leurs caractéristiques ou de leur niveau d'intérêt, et appliquera une approche spécifique propre à chacun. L'un des groupes les plus importants sera celui des experts techniques qui possèdent des connaissances et une expérience approfondies dans le domaine de la politique. Si certains de ces experts font déjà partie du gouvernement, ils travaillent souvent en dehors de celui-ci, dans des universités, des entreprises ou des organisations de la société civile. Des conseils pour consulter et travailler avec les parties prenantes dans un contexte de cybersécurité figurent dans le document intitulé « *A Short Guide to Stakeholder Engagement on National Cybersecurity Strategy Development* » *(Weisser Harris et al. 2022).*

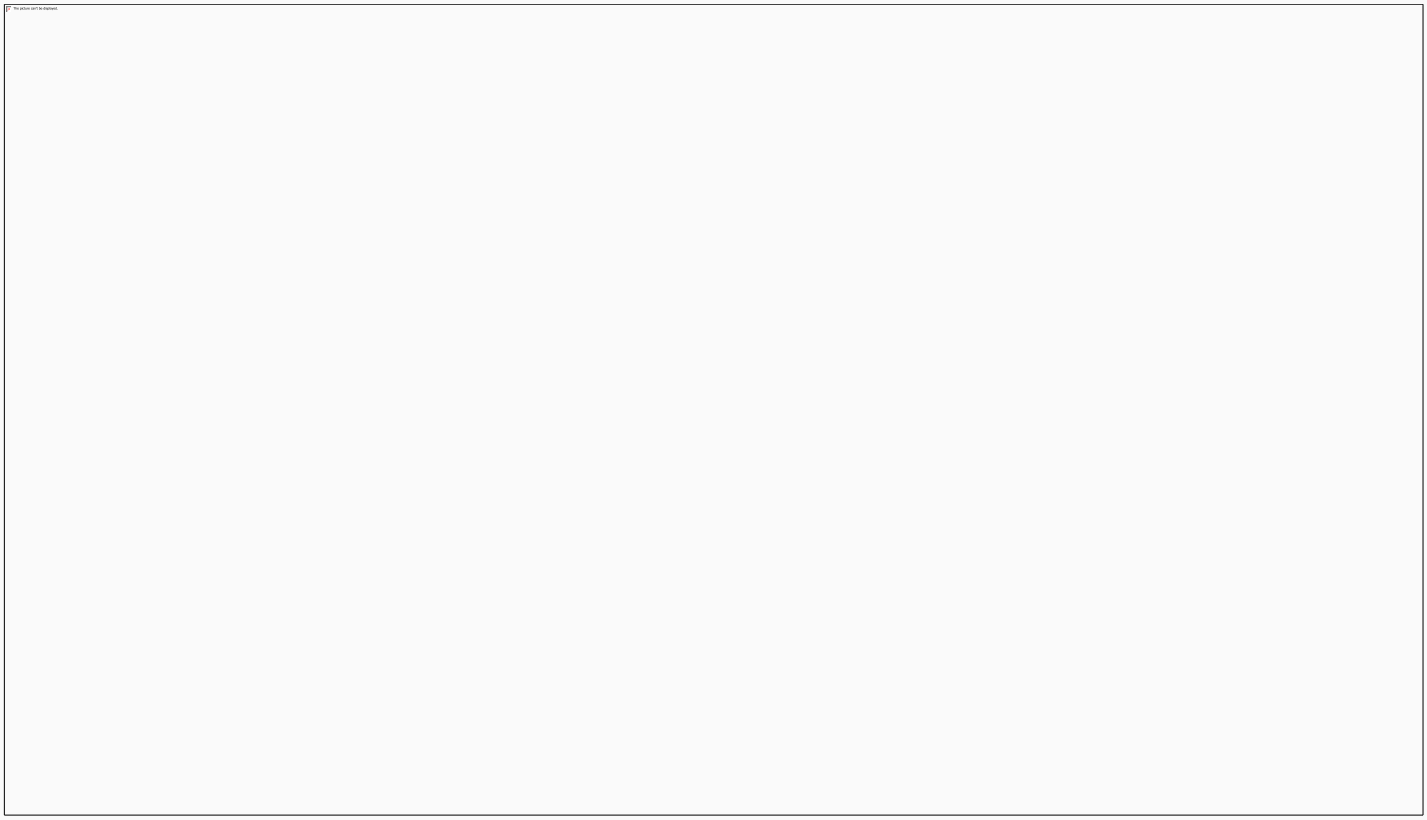


Figure 6. Différents moyens de consultation et d'engagement des parties prenantes.

À la fin du processus d'élaboration de la politique, un ministre ou le cabinet approuvera une position politique finale. Il est bon de la publier, comme le fait l'Afrique du Sud avec ses Livres blancs (mentionnés ci-dessus). Au Nigeria, ces politiques sont approuvées par le Conseil exécutif fédéral, qui rassemble tous les ministres du gouvernement fédéral, sous la présidence du président.

De nombreuses politiques nécessiteront une législation ou une réglementation formelle pour soutenir ou mener leur mise en œuvre. Il arrive que la nature d'une question politique détermine le type de levier à appliquer pour sa mise en œuvre. Par exemple, il serait plus approprié d'utiliser la législation pour traiter les questions de cybercriminalité, qui sont généralement des activités qui doivent être interdites et traitées comme des crimes, par opposition aux politiques qui visent à réglementer des secteurs spécifiques ou des activités liées à la cybersécurité, comme le traitement des données et les mesures de sécurité numérique.

Une politique de lutte contre la cybercriminalité nécessitera toujours une législation primaire pour définir les droits et les responsabilités en droit civil, ainsi que les crimes et les peines en droit pénal (droit matériel). Elle nécessitera également une législation primaire pour définir comment les cybercrimes doivent être traités par le système judiciaire (droit procédural). Vous trouverez de plus amples informations à ce sujet dans le module de connaissances sur la cybercriminalité.

En revanche, les politiques qui visent à réglementer un secteur ou un type d'activité lié à la cybersécurité, comme le traitement des données, nécessiteront une réglementation qui, à son tour, pourra ou non nécessiter une nouvelle législation primaire. Veuillez noter que la législation et la réglementation peuvent parfois être liées. La réglementation peut être liée à la législation primaire de trois façons principales :

1. La réglementation est publiée via la législation primaire. Exemple : la loi sud-africaine sur la protection des informations personnelles (POPIA) n° 4 de 2013.

2. La réglementation est émise par un ministère/une agence/une organisation qui dispose déjà de l'autorité pour le faire. Aucune nouvelle législation primaire n'est nécessaire. Exemple : la réglementation nigériane sur la protection des données, 2019 (« NDPR ») a été publié par l'Agence nationale de développement des technologies de l'information (« NITDA »).

3. Une législation primaire est nécessaire afin de conférer à un organisme existant une nouvelle autorité pour émettre une réglementation ou créer un nouvel organisme doté de cette autorité. Exemple : la loi du Kenya sur la protection des données (DPA) de 2019 a créé le Bureau du commissaire à la protection des données (ODPC), qui, en collaboration avec un groupe de travail sur la réglementation, avait pour mandat de créer une réglementation en vertu de la DPA, ce qu'il a fait par la suite dans le Réglementation sur la protection des données de 2021.

Le processus d'élaboration de la législation sur la cybercriminalité est décrit dans le module de connaissances sur la cybercriminalité. Le processus d'élaboration de la réglementation est décrit dans la section suivante.

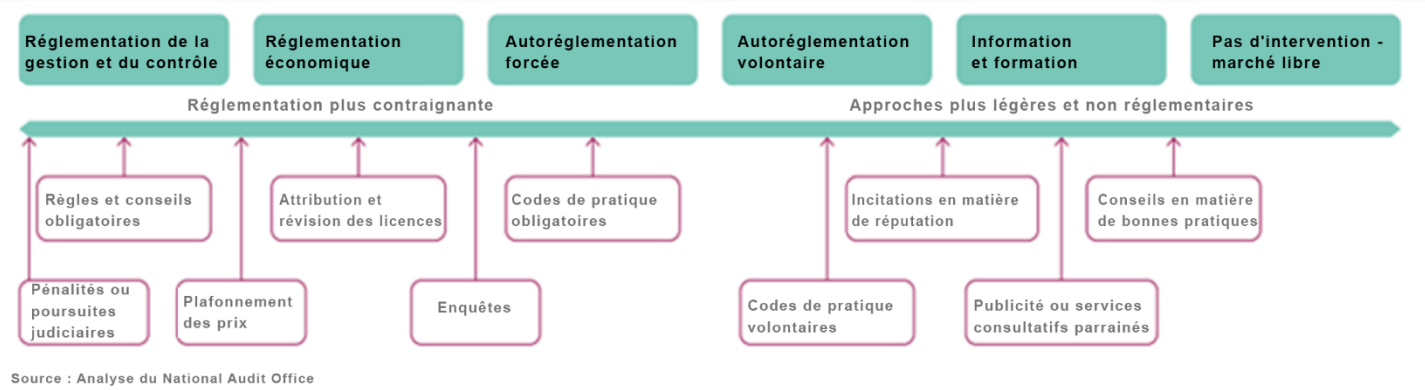
PROCESSUS D'ÉLABORATION DE LA LÉGISLATION ET DE LA RÉGLEMENTATION PARTIE 2 (DE LA POLITIQUE À LA RÉGLEMENTATION)

Dans les sections précédentes, nous avons abordé le passage des objectifs de la stratégie à la politique. Nous avons également mentionné divers domaines qui seraient mieux traités par la législation et d'autres pour lesquels le recours à la réglementation pourrait être un meilleur levier afin d'aborder la mise en œuvre. Dans cette section, nous allons donner un aperçu de la manière dont les orientations politiques peuvent être transformées en réglementations.

La tâche technique des responsables chargés de la réglementation consiste à convertir les objectifs et les idées politiques en un ensemble détaillé de règles et de processus. Ces règles et processus doivent être conçus pour atteindre les objectifs proposés par l'orientation politique. Au départ, il s'agit avant tout de déterminer le type d'approche réglementaire qui permettrait le mieux d'atteindre l'objectif politique. Il est en effet nécessaire de trouver un équilibre entre le recours à la réglementation pour contrôler et restreindre les activités inacceptables dans le cyberespace, sans pour autant renoncer aux vastes avantages qui en découlent.

Lorsqu'une réglementation est envisagée, une première décision à prendre concerne le type d'approche réglementaire qui sera suivie. Il existe toute une série d'options, d'une approche lourde à une approche légère. L'approche lourde est la plus adaptée aux questions qui nécessitent des restrictions afin de prévenir les dommages ou la destruction. L'approche légère peut être utilisée lorsqu'il est nécessaire de donner des conseils pour atteindre un objectif particulier. Le diagramme ci-dessous présente le spectre des options réglementaires, de l'approche lourde à l'approche légère.

.



Source : (National Audit Office du Royaume-Uni 2021, 8)

Bien qu'il n'existe pas de processus réglementaires spécifiques conçus pour la réglementation de la cybersécurité, divers processus réglementaires génériques peuvent être adaptés pour être utilisés dans la réglementation de la cybersécurité. Le document « *Good practice guidance: Principles of effective regulation* » *du NAO, au Royaume-Uni, en est un bon exemple.* Ce guide des bonnes pratiques recommande d'appliquer à la réglementation en matière de cybersécurité le cycle de vie suivant pour l'élaboration de la réglementation.

Conception • Définir l'objectif général de la réglementation • Fixer les objectifs de la réglementation • Assurer la responsabilité • Déterminer le degré d'indépendance de la réglementation • Décider des pouvoirs • Déterminer un modèle de financement • Concevoir la structure et la culture organisationnelles	Analyse • Utiliser les informations et les données • Intégrer la perspective du citoyen • Contrôler la conformité et les incitations des prestataires de services • S'engager avec les parties prenantes • Garantir les capacités et les compétences • Adopter une approche prospective
Intervenir • Développer une théorie du changement • Hiérarchiser les interventions • S'appuyer sur une gamme d'outils réglementaires • Intégrer la cohérence et la prévisibilité • Veiller à ce que les interventions soient proportionnées • Être réactif	Apprendre • Établir des processus de gouvernance • Mesurer la performance • Évaluer l'impact et les résultats • Encourager la coopération et la coordination • Assurer la transparence

Lors de l'élaboration d'une réglementation, le gouvernement examinera quelle architecture est nécessaire pour superviser, maintenir et appliquer la réglementation. Il arrive qu'une législation primaire puisse contenir des dispositions sur la manière dont les réglementations produites par un organisme particulier doivent être mises en œuvre, recommandant ainsi l'architecture de ces réglementations. Les niveaux typiques de l'architecture peuvent inclure :

- Organisme(s) chargé(s) de superviser le cadre réglementaire et de contrôler sa mise en œuvre ;

- Organisme(s) chargé(s) d'élaborer des réglementations sur une ou plusieurs questions particulières ;
- Organisme(s) chargé(s) de faire appliquer ou de gérer la réglementation ;
- Les entités qui sont réglementées et qui doivent suivre la réglementation ; et
- Le consommateur, le citoyen ou le bénéficiaire qui est protégé par la réglementation.

Il peut parfois être nécessaire de créer de nouvelles entités pour mettre en œuvre et faire appliquer un règlement ou d'attribuer un nouveau pouvoir d'exécution à une entité juridique existante.

Il convient de noter que les considérations relatives à l'élaboration des réglementations ne doivent pas se limiter aux seules questions nationales. Les responsables qui élaborent les réglementations devront comprendre le paysage réglementaire international pour le domaine politique concerné. En Afrique, la Convention de l'UA sur la cybersécurité et la protection des données à caractère personnel (connue sous le nom de Convention de Malabo) contient des dispositions relatives à la réglementation de la protection des données et des transactions électroniques.

Au niveau international, il existe des cadres de bonnes pratiques en matière de cybersécurité dont la réglementation peut s'inspirer, comme le NIST et l'ISO. Il existe également un grand nombre de réglementations nationales et sectorielles auxquelles les entreprises doivent se conformer et dont les gouvernements devraient tenir compte lorsqu'ils élaborent leur propre réglementation. Par exemple, le règlement général sur la protection des données (RGPD) de l'UE réglemente la protection des données des citoyens de l'UE et s'applique aux organisations qui traitent ces données, même si elles se trouvent en dehors de l'UE.

Les gouvernements peuvent utiliser les réglementations d'autres juridictions pour trouver des idées dans leur propre réglementation nationale. Par exemple, la loi égyptienne sur la protection des données (loi n° 151 de 2020) contient de nombreuses dispositions similaires au RGPD de l'UE. (PWC 2020, 16) Lorsque les entreprises doivent suivre un processus unique pour se conformer aux réglementations de plusieurs marchés, cela réduit leurs coûts de conformité et leur charge de travail.

Étude de cas
En 2016, le Royaume-Uni a pris la décision d'utiliser des leviers politiques moins interventionnistes. Par exemple, s'attacher à former les conseils d'administration des entreprises plutôt que de les réglementer. Lorsque le Royaume-Uni a revu son approche en 2022, il a conclu que les entreprises amélioraient leur gestion des cyberrisques, mais pas assez rapidement pour faire face à l'évolution de la menace. Il a donc décidé de s'orienter vers « une approche plus interventionniste visant à utiliser les incitations et les réglementations du marché afin d'établir rapidement de meilleures pratiques ». Cela illustre la façon dont les gouvernements peuvent revoir régulièrement leur utilisation des leviers politiques et modifier l'équilibre des leviers qu'ils utilisent. [Source de cette étude de cas : (Ministère britannique du numérique, de la culture, des médias et du sport 2022, section 4)]

SOUTIEN À LA PRODUCTION DE LA RÉGLEMENTATION
Il existe diverses sources d'acquisition des bonnes pratiques pour l'élaboration des réglementations, dont les pays peuvent s'inspirer. L'Organisation de coopération et de développement économiques (OCDE) a produit pendant plus de vingt ans des orientations sur les caractéristiques d'une bonne réglementation. Elle encourage les pays à se doter de leurs propres principes de bonne réglementation, ce que beaucoup font, et qui devrait constituer un

point de référence pour ceux qui élaborent une réglementation nationale en matière de cybersécurité.

Les chercheurs qui ont évalué la qualité de la réglementation dans le cadre de la loi sur les marchés numériques ont produit un cadre régissant les principes de bonne réglementation (s'inspirant des orientations de l'OCDE et du FEM), qui pourrait être utile aux responsables dans un contexte de cybersécurité. (Bauer et al. 2022, 6) Les grands principes sont les suivants :

1. Objectifs politiques clairs basés sur la résolution d'un problème factuel bien identifié par des mécanismes d'intervention éprouvés
2. Clarté des règles de conformité
3. Proportionnalité et adaptabilité

Les sources d'orientation et de soutien spécifiques à la cybersécurité pour l'élaboration de réglementations sont les suivantes :

- Projets de formation et de conseil en matière de réglementation (par exemple, Secrétariat du Commonwealth, UIT, Cyber4Dev ?)
- Certains programmes de renforcement des capacités, notamment ceux de la Banque mondiale, prévoient un soutien à la réglementation sectorielle parallèlement aux investissements dans les infrastructures (par exemple, le projet Digital Malawi de la Banque).
- Des ateliers régionaux sont organisés pour discuter de l'harmonisation de la réglementation, comme le séminaire CNUCED-CEDEAO sur l'Afrique de l'Ouest 2015 dans le cadre de la semaine du commerce électronique.

SUIVI ET ÉVALUATION

La phase de suivi et d'évaluation doit inclure une évaluation afin de déterminer si les plans d'action sont mis en œuvre sur la base des calendriers convenus et, lorsqu'ils sont mis en œuvre, s'ils ont les résultats escomptés. À ce stade, il devrait y avoir un processus formel en vue de déterminer si la mise en œuvre a atteint les objectifs de la SNC et d'évaluer s'il est nécessaire de la revoir pour le prochain cycle du processus. Les activités de cette étape sont les suivantes :

1. Création d'un processus formel

Afin de garantir que les objectifs sont atteints, il est nécessaire de créer un processus formel pour le suivi de la mise en œuvre de la SNC et d'évaluer les résultats en vue de déterminer si les objectifs ont été atteints. La plupart des pays identifient, ou établissent, une entité gouvernementale indépendante qui assurera le suivi et l'évaluation du processus de mise en œuvre. Dans certains cas, l'entité qui coordonne la mise en œuvre de la SNC crée un rôle de suivi et d'évaluation pour garantir que les objectifs sont atteints. Le cadre de suivi doit comporter des indicateurs de performance qui sont spécifiques, mesurables, réalisables, responsables et liés à un calendrier.

2. Suivi de la mise en œuvre de la stratégie

Une fois le processus formel de suivi et d'évaluation créé, l'entité responsable doit en mesurer la mise en œuvre sur la base des paramètres convenus. En présence d'écarts par rapport aux délais convenus ou de raisons pour lesquelles les objectifs fixés n'ont pas été atteints, il convient d'en prendre note, car cela constituera un apport précieux pour les itérations futures de la stratégie lorsque la SNC sera revue pour un autre cycle. Cette approche permettra de

confirmer que les parties prenantes concernées assument les responsabilités qui leur ont été attribuées pour la mise en œuvre.

3. Évaluer les résultats de la stratégie

Outre l'évaluation des progrès de la mise en œuvre sur la base de la matrice convenue, il est également nécessaire d'évaluer les résultats et de les comparer aux objectifs fixés dans la SNC. Cela permettra de déterminer si les objectifs de la SNC mènent le pays dans la bonne direction. L'évaluation, ainsi que les recommandations associées, doivent être compilées dans un rapport destiné au responsable du projet, et inclure les moyens de mettre à jour le plan d'action de la mise en œuvre et de confirmer qu'il est à jour et adapté à l'évolution de la politique et du paysage des risques.

FINANCEMENT

Le financement est un autre aspect fondamental du processus de mise en œuvre. Le financement traditionnel du processus de mise en œuvre passe par l'allocation de fonds provenant du budget du gouvernement. Cette approche présente son lot de difficultés. Outre le fait que les ressources financières de la plupart des gouvernements sont faibles et présentent des intérêts contradictoires, l'appropriation du processus par les parties prenantes devrait inclure des accords de financement innovants. Cet aspect doit être spécifiquement abordé dans les stratégies et le plan d'action. Par exemple, au Nigeria, la loi sur la cybercriminalité de 2015 prévoit qu'un certain pourcentage de frais doit être prélevé sur les transferts de fonds électroniques et que ces frais sont réservés au financement des activités de cybersécurité. De même, la politique nationale de cybersécurité suggère également qu'un certain pourcentage du budget des agences gouvernementales soit consacré aux activités de cybersécurité.

Ouvrages cités

Ajijola, Abdulhakeem, et Nate Allen. *African Lessons in Cyber Strategy*. 8 mars 2022. *Centre d'études stratégiques de l'Afrique*, https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/.

Azmi, Riza, et al. « Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. » *www.researchgate.com*, Research Gate, Décembre 2016, https://www.researchgate.net/publication/308470260_Motives_behind_Cyber_Security_Strategy_Development_A_Literature_Review_of_National_Cyber_Security_Strategy. Consulté le 25 novembre 2022

Union internationale des télécommunications. *Guide pour l'élaboration d'une stratégie nationale de cybersécurité*. UIT Genève, 2018. *Guide pour l'élaboration d'une stratégie nationale de cybersécurité*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

Bauer, Matthias, Fredrik Erixon, Oscar Guinea, Erik van der Marel et Vanika Sharma. 2022. « The EU Digital Markets Act: Assessing the Quality of Regulation. » ECIPE. https://www.researchgate.net/publication/362092853_The_EU_Digital_Markets_Act_Assessing_the_Quality_of_Regulation.

Union internationale des télécommunications (UIT), Banque mondiale, Organisation des télécommunications du Commonwealth (CTO), Centre d'excellence de l'OTAN pour la cyberdéfense coopérative (COE CCD de l'OTAN) et Secrétariat du Commonwealth. 2018. « Guide pour l'élaboration d'une stratégie nationale de

cybersécurité. » https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.
National Audit Office du Royaume-Uni. 2021. « Good Practice Guidance: Principles of Effective Regulation. » https://www.nao.org.uk/wp-content/uploads/2021/05/Principles-of-effective-regulation-SOff-interactive-accessible.pdf.
Organisation des États américains (OEA) et Global Partners Digital. 2022. « National Cybersecurity Strategies: Lessons Learned and Reflections from The Americas and Other Regions. » https://cybilportal.org/wp-content/uploads/2022/08/National-Cybersecurity-Strategies.-Lessons-learned-and-reflections-ENG.pdf.
PWC. 2020. « Data Privacy in Egypt: What You Need to Know. » https://www.pwc.com/m1/en/services/assurance/risk-assurance/documents/webcast-data-privacy-egypt-what-you-need-know.pdf.
Ministère britannique de la culture, des médias et des sports. 2022. « 2022 Cyber Security Incentives and Regulation Review. » Ministère britannique de la culture, des médias et des sports. https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review/2022-cyber-security-incentives-and-regulation-review.
Weisser Harris, Carolin, Daniela Schnidrig, Elizabeth Orembo, James Boorman et Kerry-Ann Barrett. 2022. « A Short Guide to Stakeholder Engagement on National Cybersecurity Strategy Development. » Global Forum on Cyber Expertise. https://cybilportal.org/wp-content/uploads/2022/08/GFCE-NCS-Development-Stakeholder-Engagement-Paper.pdf.