Union des Comores

Agence Nationale de Développement Numérique

Direction Nationale de la Cybersécurité

STRATÉGIE NATIONALE DE CYBERSÉCURITÉ

Sommaire

1. INTRODUCTION

Dans un contexte d'intenses développements des technologies de l'information et de la communication, de nouvelles menaces surgissent pour nos sociétés : attaques visant les infrastructures essentielles, espionnages, piratages et vols de données des grandes entreprises, terrorisme du web, expansions des réseaux criminels transnationaux, blanchiment d'argent via les devises virtuelles, ingérence étrangère dans les élections et intrusion dans les systèmes de télécommunications et de l'information. La cybersécurité est devenue un élément essentiel des systèmes de défense des États et des entreprises privées. Les systèmes d'information et de communication se sont transformés en un terrain fertile pour les réseaux criminels et a laissé place à un nouveau terrain d'affrontements dans les conflits.

Les systèmes d'information et de communication présentent alors un risque provenant des failles intrinsèques et seront toujours sujets aux tentatives visant à en exploiter les failles, pour lancer des attaques. Cette menace ne peut pas être totalement éliminée. Elle peut néanmoins être considérablement réduite, pour permette à la société de continuer à prospérer et à tirer parti des grandes opportunités découlant de la technologie numérique. C'est dans ce sens que la cybersécurité suscite depuis quelques années l'intérêt des Etats pour mettre en place des mécanismes de protection efficace pour protéger les cyberespaces nationaux contre les risques de plus en plus fréquents et dévastateurs.

Compte tenu de la complexité et des dimensions multiples de la cybersécurité, la protection et la prévention contre les activités criminelles dans le cyberespace à travers le monde nécessite la coopération et la coordination de toutes les parties concernées aussi bien à l'échelle des cyberespaces nationaux qu'entre les pays et exige que les gouvernements procurent des réponses stratégiques pour contrer les cyber-menaces.

L'élaboration d'une stratégie nationale de cybersécurité soulève un ensemble de problématiques liées aux points suivants :

- Le cyberespace présente un périmètre étendu qui ne permet pas de prendre en considération tous les détails relatifs à la sécurité des systèmes d'information et de communication sur lequel ils sont déployés ;

- Le cyberespace implique des acteurs provenant de différents domaines d'exercice et qui présentent différents niveaux d'expertise dans les TIC ;

- La mise en œuvre de mécanismes pour la protection d'un cyberespace ne peut pas se faire sans la prise en considération des menaces provenant des autres espaces, pour ceci il est impératif d'établir des coopérations internationales en matière de cybersécurité pour garantir la résilience des mécanismes adoptés ;

- La conformité aux références internationales en matière de disposition réglementaire est un défi important car elle permet de faciliter les échanges et les coopérations en matière de lutte contre la cybercriminalité, surtout dans les domaines de l'échange des éléments de preuve et de la coordination des alertes relatives aux incidents de sécurité.

2. CONTEXTE

2.1 Contexte international

Selon le rapport relatif aux coûts des vulnérabilités (IBM/Ponemon Institute, 2019), 46% des entreprises en moyenne sont la cible d'une attaque, au moins, par année. Ce rapport, dont la Figure 2 révèle les conclusions majeures, a aussi révélé que certaines attaques restent jusqu'à 276 jours avant qu'une solution de sécurité adéquate ne soit trouvée (zero-day).

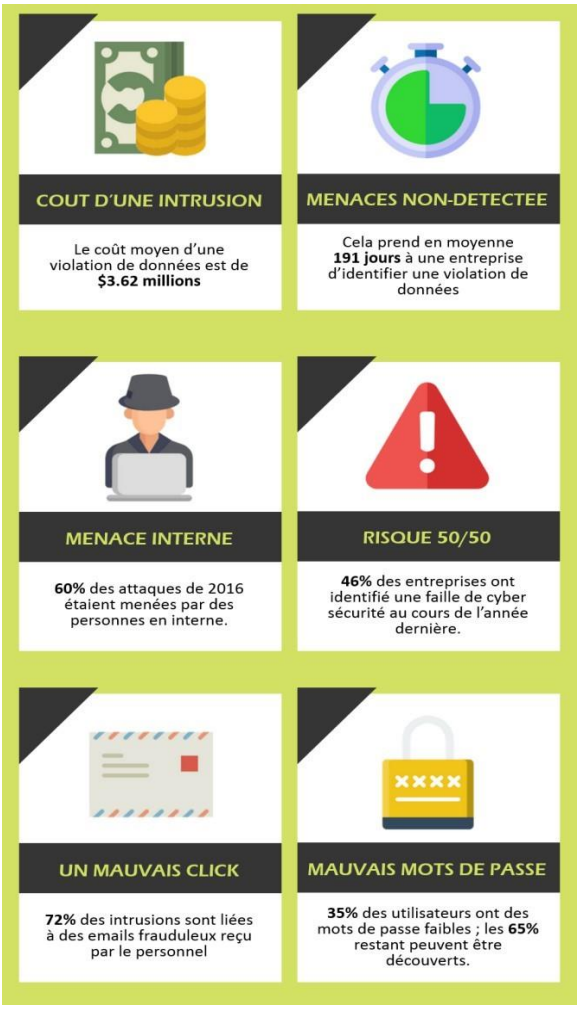

Figure 2 : Statistiques clés en matière de cybersécurité (IBM/Ponemon, 2019).

La cybersécurité est donc devenue une préoccupation majeure dans le monde entier, la sophistication des cyber-attaques et les dommages financiers causés au pays ont augmenté à un rythme exponentiel. En effet, le rythme rapide de l'innovation dans le secteur des TIC peut se traduire par des lacunes dans les cadres législatifs et réglementaires liés à cybersécurité. Le grand défi pour les législateurs est de combler le retard dans la reconnaissance des nouveaux types d'infractions dans le cyberespace et l'adoption d'amendements aux législations applicables.

Compte tenu de la complexité et des dimensions multiples de la cybersécurité, la protection et la prévention contre les activités criminelles dans le cyberespace à travers le monde nécessite la coopération et la coordination de toutes les parties concernées aussi bien à l'échelle des cyberespaces nationaux qu'entre les pays.

La première réglementation internationale, contribuant à appréhender la dimension internationale de la cybercriminalité est la Convention sur la cybercriminalité Budapest 23 novembre 2001, adoptée sous l'égide du Conseil de l'Europe et entrée en vigueur en juillet 2004 (dès sa ratification par au moins 5 Etats (dont 3 au moins doivent être du Conseil de l'Europe). Cette convention aborde les points suivants:

1. Disposition de droit pénal matériel concernant:
    - les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques;
    - les infractions informatiques;
    - infraction liée aux contenues
    - les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes;
2. Disposition de droit procédural concernant:
    - la conservation rapide des données informatiques, de données relatives au trafic et à sa divulgation rapide à l'autorité compétente;

- la conservation et la protection de l'intégrité des données pendant une durée aussi longue que nécessaire pour permettre aux autorités compétentes d'obtenir leur divulgation;
- l'injonction de produire;
- la perquisition et la saisie des données stockées;
- la collecte en temps réel des données;
- la protection adéquate des droits de l'homme et des libertés;

3. Chaque Etat doit adopter des mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans le respect de son droit interne:
   - l'accès intentionnel et sans droit à tout ou partie d'un système;
   - l'interception intentionnelle et sans droit de données lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système ; le fait intentionnel et sans droit d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données;
   - l'entrave grave intentionnelle et sans droit au fonctionnement d'un système;
   - la production, la vente, l'obtention pour l'utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif conçu ou adapté pour réaliser une des infractions mentionnées;
   - l'introduction, l'altération, l'effacement ou la suppression intentionnelle et sans droit de données, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques;
   - le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par l'introduction, l'altération, l'effacement ou la suppression de données, toute forme d'atteinte au fonctionnement d'un système, dans l'intention frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui;

4. Les Etats doivent établir leurs compétences à l'égard de toute infraction pénale lorsque cette dernière est commise:
   - sur son territoire;
   - à bord d'un navire battant pavillon de cet Etat;
   - par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève pas de la compétence territoriale d'aucun Etat;
5. Règles concernant la coopération internationale en matière:
   - d'extradition;
   - d'entraide aux fins d'investigation;
   - de procédures concernant les infractions pénales liées à des systèmes et données informatiques;
   - de recueil de preuves sous forme électronique d'une infraction pénale;
6. Création d'un réseau d'entraide
   - 24h/24, 7j/7;
   - point de contact national;
   - assistance immédiate pour les infractions;

2.2 Contexte africain

Les gouvernements Africains sont à différents niveaux d'avancement en matière d'établissement d'instruments politiques, de cadres législatifs, et de mécanismes techniques pour la protection des cyberespaces nationaux.

Bien que de nombreux pays aient proposé des législations, le niveau de déploiement des systèmes de sécurité à la fois dans le secteur privé et le secteur public reste faible. Pour promouvoir la culture de la cybersécurité et mettre en place des mesures efficaces visant à renforcer la confiance et la sécurité dans l'utilisation des réseaux de télécommunication, plusieurs défis restent à relever.

Ceci est corroboré par l'Indice Global de Cybersécurité, élaboré en 2017 par l'UIT, qui révèle que le classement des pays africains est en dessous de la moyenne des classements des autres régions. Ceci est illustré par la Figure 3 où :

- La couleur rouge représente les pays appartenant aux 50 derniers percentiles du classement (96 pays). Ces pays appartiennent à la catégorie C ;
- La couleur jaune représente les pays compris entre les 51ème et 90ème percentiles (77 pays). Ces pays appartiennent à la catégorie B ;
- La couleur verte représente les pays appartenant aux 10 premiers percentiles (21 pays). Ces pays appartiennent à la catégorie A.

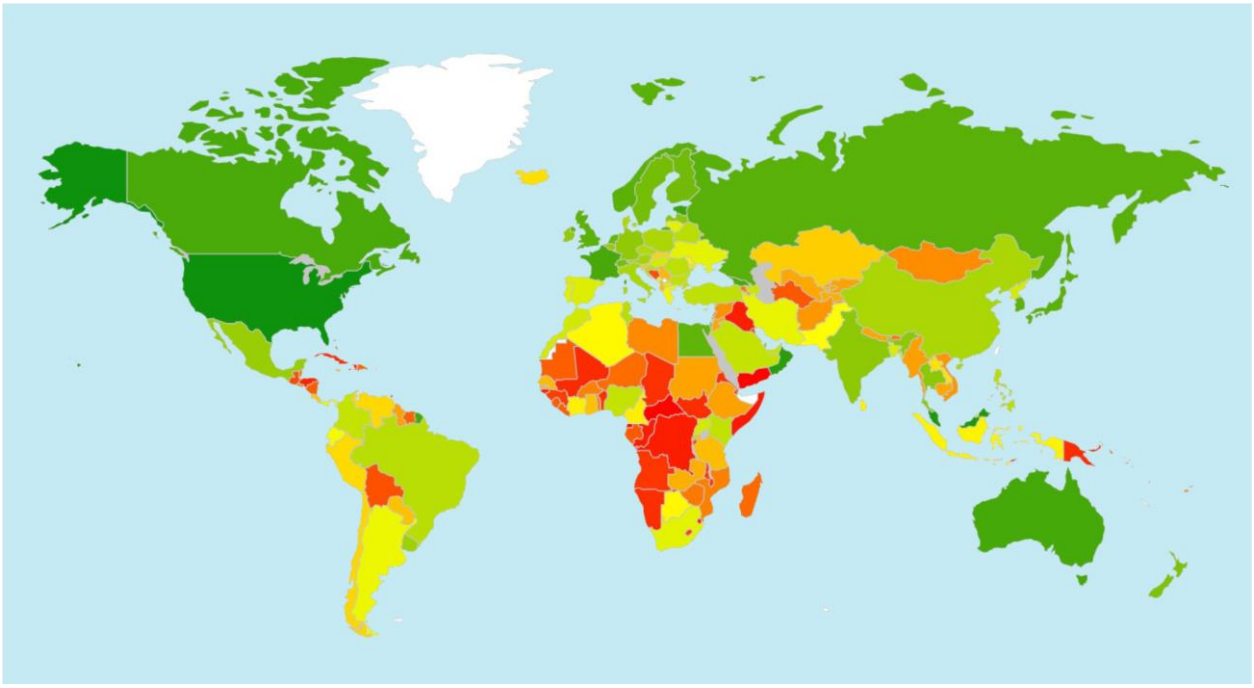

Figure 3 : Aperçu sur le classement international des pays selon l'IGC (UIT, 2017).

Cette figure montre que plusieurs lacunes existent par rapport à la manière avec laquelle les pays africains abordent la cybersécurité. Les scores moyens par région, donnés dans le Tableau 1, montrent que l'Afrique vient en dernière position pour les cinq piliers du score IGC à savoir le pilier juridique, le pilier technique, le pilier organisationnel, le pilier

renforcement des capacités et le pilier coopération. Il est important de noter que l'écart le plus important par rapport à la moyenne est enregistré pour le pilier technique. Le pilier pour lequel le score des pays africains est le plus proche du reste des continents concerne la coopération. Il est à noter que, dans le reste de ce rapport et dans le cadre de cette mission, le terme « score » traduit la performance national par rapport à un référentiel international.

Selon le score IGC, le Rwanda est classé deuxième en Afrique. Son meilleur score est obtenu dans le pilier organisationnel. Ce pays a mis en œuvre une politique de cybersécurité autonome qui s'adresse aux secteurs privé et public et il est engagé dans le développement d'une industrie solide de cybersécurité.

Tout en restant dans le même contexte, la troisième position est occupée par le Kenya qui fournit un bon exemple de coopération à travers son centre de coordination national **KECIRT/CC. Le CIRT de Kenya assure la coordination sur le plan national, régional et international avec un ensemble d'acteurs qui regroupe les institutions financières et éducationnelles et les autres CIRTs.**

Tableau 1 : Scores relatifs aux piliers du IGC .

Région	Juridique	Technique	Organisationnel	Renforcement des capacités	Coopération
AFRIQUE	0.29	0.18	0.16	0.17	0.25
AMERIQUE	0.40	0.30	0.24	0.28	0.26
PAYS ARABES	0.44	0.33	0.27	0.34	0.29
ASIE	0.43	0.38	0.31	0.34	0.39
COMMONWEALTH	0.58	0.42	0.37	0.38	0.40
EUROPE	0.61	0.60	0.45	0.49	0.46

Pour réagir aux difficultés posées par les activités criminelles commises sur le cyberespace d'une manière compatible au niveau régional et continental et aussi en réponse à la

nécessité d'harmoniser les législations dans le domaine de la cybersécurité et la protection des données a caractères personnel dans les États membres de l'Union Africaine, la 23ème Assemblée des chefs d'Etat et des gouvernements de UA, tenue à Malabo les 26-27 Juin 2014 a adopté la "Convention sur la cybersécurité et la protection des données à caractère personnel" de L'Union Africaine qui est aussi appelé la "Convention de Malabo".

Par conséquent, pour les pays africains, il est nécessaire de considérer la cybersécurité comme un problème important au niveau national et régional qui affecte leurs souverainetés et leurs sécurités nationales, ainsi que la protection des sociétés et des infrastructures critiques.

2.3 Contexte national

L'impact des attaques visant les composantes du cyberespace peut aussi avoir une connotation politique. De récents événements de part le Monde ont montré que les vulnérabilités présentes dans les systèmes d'information et de communication présentent des vecteurs d'attaques qui visent la réputation des hommes et des partis politiques, les systèmes de vote, voire même la stabilité politique nationale.

Ainsi, et en matière d'atteinte à la réputation, des années de fuites de WikiLeaks et d'autres sources ont poussé le public à supposer que les informations divulguées sont vraies par défaut. Même si des données communiquées dans le passé ont pu être authentiques, cette supposition pourrait facilement être exploitée pour influencer les électeurs. Lorsque des données divulguées sont altérées, le parti ciblé peut n'avoir aucun moyen raisonnable de prouver l'altération. Les systèmes de messagerie et d'échange d'information doivent alors être protégés contre ce type d'attaques.

Un autre type d'incident dont l'occurrence est de plus en plus fréquente concerne l'utilisation des réseaux sociaux dans l'objectif de porter atteinte à la sécurité nationale. Comme tous les lieux de socialisation, ces réseaux offrent une bonne image de l'opinion

d'un peuple à un moment donné. Ils hébergent aussi des échanges, qui sont autant de vecteurs possibles de propagation d'idéologies. Il n'est dès lors pas inenvisageable d'imaginer que les services de renseignement d'un pays puissent accéder à de précieuses informations sur ces espaces.

Étant donné l'importance du secteur des technologies de l'information et de la communication (TIC) et son impact direct et positif sur le développement social et économique des pays Africains, il existe un besoin urgent de développer une approche globale et une stratégie cohérente en matière de cybersécurité au niveau continental pour promouvoir la paix et la sécurité dans la société de l'information.

Afin d'illustrer l'impact du développement de l'écosystème national de cybersécurité sur le contexte socio-économique, nous donnons dans la Figure 4 un aperçu sur la corrélation entre le classement IGC et IDI (Indice de Développement de l'Information, UIT). Il ressort de cette figure qu'il existe un lien étroit entre les mécanismes mis en place pour la protection du cyberespace et le développement des indicateurs relatifs à la société de l'information. Ceci peut être expliqué par deux raisons principales :

1. Les systèmes d'information et de communication sont fortement présents dans le paysage économique de nos jours. Le fait de réduire les risques dont ils sont la cible génère un bénéfice dont le modèle économique s'articule du retour d'investissements de sécurité. Ce modèle économique se base sur l'adéquation entre le niveau de risque réduit et les investissements réalisés en matière de sécurité. De cette façon, les mécanismes et les processus de protection font partie intégrante du cycle de développement des composantes du cyberespace ;
2. L'impact social des systèmes d'information et de communication est de plus en plus palpable, notamment avec l'évolution des réseaux sociaux. Ainsi, les risques visant ces systèmes se répercutent nécessairement sur l'équilibre de la société. D'où la nécessité d'accorder aux incidents de sécurité dont l'impact est social l'importance qu'ils méritent.

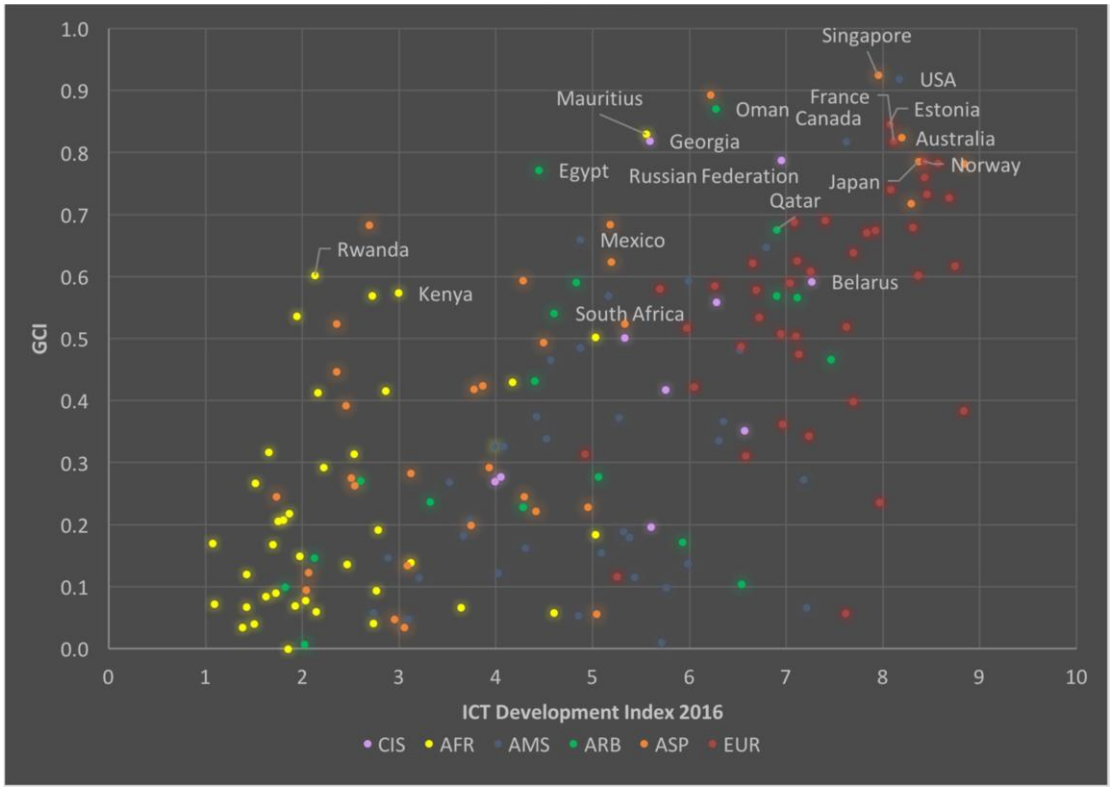

Figure 4 : Corrélation entre les indicateurs IGC et IDI.

L'accroissement continu des attaques sur les systèmes d'information et de communication met en évidence un ensemble de caractéristiques spécifiques dont nous citons :

- la coordination des attaques: les utilisateurs malveillants utilisent les ressources des systèmes d'information et de communication pour coordonner les éléments d'un scénario d'attaque. En d'autres termes, des attaques élémentaires peuvent être combinées de différentes manières en vue de former un scénario qui devient plus difficile à détecter et à contrecarrer. Les relations les plus utilisées entre les attaques d'un même scénario sont :
    - Dépendance : Il s'agit d'une relation de cause à effet entre deux ou plusieurs attaques ;

    - Enchaînement : Il s'agit d'une précédence temporelle entre deux ou plusieurs attaques ;
    - Parallélisme : Il s'agit d'une exécution parallèle de deux ou plusieurs attaques de manière à ce que la combinaison des objectifs élémentaires génère un objectif unifié.

- la multitude de motivations : les raisons qui peuvent expliquer la réalisation d'une attaque sont très nombreuses (exemples : vol d'argent, espionnage industriel, défi personnel, etc.) et ceci complique le processus d'investigation numérique ;
- la persistance : une attaque peut rester un certain temps sur le système avant qu'elle ne soit déclenchée. Le temps créé ainsi entre l'intrusion et son déclenchement complique le processus de détection ;
- Le contrôle à distance : l'attaquant peut souvent réaliser son objectif sans qu'il ne soit en contact direct avec le système cible. Ainsi, le sentiment d'être difficile à tracer accroît sa motivation.

Si une grande partie du matériel informatique et des logiciels développés à l'origine pour faciliter l'interconnexion de cet environnement numérique ont privilégié l'efficacité, les coûts et la commodité pour l'usager, ils n'ont pas toujours intégré la dimension sécurité dès le départ. Or, des acteurs malveillants — États hostiles, organismes ou individus criminels ou terroristes — peuvent exploiter cet écart entre commodité et sécurité ; le réduire constitue donc une priorité nationale.

Dans un environnement aussi complexe, hétérogène et vaste qu'un cyberespace national, la complexité de traiter les incidents de sécurité n'est qu'exacerbée. C'est dans ce sens que des décisions stratégiques doivent être conçues dans un premier temps pour faciliter la mise en place des solutions de sécurité. Ces décisions doivent ensuite être validées, déployées, testées, contrôlées et révisées.

3. ELEMENTS DE LA SNCS

3.1 Vision

L'ambition de l'Union des Comores en matière de sécurisation de son espace cybernétique se décline comme suit : « A l'horizon 2025 l'Union des Comores dispose d'un cybersespace de confiance favorable au développement économique et social ».

3.2 Les principes directeurs

L'élaboration de la stratégie nationale de cybersécurité doit obéir à un ensemble de valeurs de références citées ci-dessous en tant que principes directeurs :

- **La primauté du droit**: la SNCS sera mise en œuvre en respectant scrupuleusement les lois nationales et supranationales.
- **La responsabilité partagée**: la SNCS engage toutes les parties prenantes au niveau national dans la sécurisation du cyberespace Comorien.
- **Une approche fondée sur les risques** : l'Etat Comorien s'engage à ce que tous les acteurs du cyberespace adoptent une démarche basée sur les risques dans le cadre de la mise en œuvre des actions de la SNCS.
- **L'accès pour tous au cyberespace** : la non-discrimination, l'inclusion et le libre accès sont garantis dans le cadre de mise en œuvre de la SNCS.

3.3 Orientations stratégiques

Les valeurs fondamentales qui doivent être considérées dans le cadre de la mise en œuvre de la SNCS sont :

- faire de la lutte contre la cybercriminalité et du renforcement des capacités de cybersécurité une priorité;

- renforcer la coordination entre les différents acteurs du cyberespace et avec les homologues internationaux ;
- respecter les droits fondamentaux des personnes ;
- mettre en œuvre des mesures appropriées et proportionnées aux menaces ;
- mobiliser, fédérer et engager les différents acteurs privés du cyberespace et de la société civile autour des actions prévues dans la SNCS en vue de lutter contre la cybercriminalité.

3.4 Objectifs

3.4.1 Objectif général

L'objectif général de la stratégie nationale de cybersécurité est de garantir un cyberespace sûr qui contribue d'une manière efficace aux objectifs de transformation numérique de l'Union des Comores.

3.4.2 Objectifs spécifiques

Les objectifs spécifiques de la SNCS sont :

- Objectif 1 : mettre en place un cadre juridique de la cybersecurité
- Objectif 2 : Instaurer une synergie à l'échelle nationale ;
- Objectif 2 : Renforcer la coopération internationale ;
- Objectif 3 : Informer, former et sensibiliser les acteurs du cyberespace sur les risques encourus ;
- Objectif 4 : Instaurer une coopération avec le tissu universitaire et de recherche ;
- Objectif 5 : Mettre en place des normes, des standards et des référentiels d'exigence ;

- Objectif 6 : Améliorer la sécurité et la résilience des infrastructures sensibles et critiques ;
- Objectif 7 : Combattre la cybercriminalité.

En s'inspirant de ces bonnes pratiques, et en considérant l'état des lieux en matière de cybersécurité à l'Union des Comores, les objectifs stratégiques suivants sont définis pour la SNCS de l'Union des Comores :

- **Orientation 1 : Amélioration de la gouvernance de la cybersécurité**
  - Objectif 1 : Instaurer une synergie à l'échelle nationale ;
  - Objectif 2 : Renforcer la coopération internationale ;
- **Orientation 2 : Renforcement de la culture de la cybersécurité**
  - Objectif 3 : Informer, former et sensibiliser les acteurs du cyberespace sur les risques encourus ;
  - Objectif 4 : Instaurer une coopération avec le tissu universitaire et de recherche ;
- **Orientation 3 : Protection contre les risques de sécurité**
  - Objectif 5 : Mettre en place des normes, des standards et des référentiels d'exigence ;
  - Objectif 6 : Améliorer la sécurité et la résilience des infrastructures sensibles et critiques ;
  - Objectif 7 : Combattre la cybercriminalité.

4. PROGRAMMES DE LA SNCS

4.1 Axe 1 : Instaurer une synergie à l'échelle nationale

1. IDENTIFICATION ET ALLOCATION DES RESSOURCES HUMAINES ET BUDGETAIRES NECESSAIRES A LA PROTECTION DU CYBERESPACE

1.1 Le Gouvernement Comorien se chargera de recenser les infrastructures sensibles et critiques, afin de veiller à la mise en place d'un niveau de protection adéquat. Les besoins de protection spécifiques seront, le cas échéant, élaborés en étroite collaboration avec les opérateurs et les exploitants desdites infrastructures.

1.2 Ces besoins de protection seront utilisés afin d'identifier les moyens nécessaires pour développer une capacité nationale de protection du cyberespace, pour réagir aux incidents touchant le cyberespace et en réduire les risques. Ces incidents couvrent aussi bien les attaques ne visant qu'une seule organisation ainsi que les attaques nationales de grande envergure.

1.3 Les moyens humains et financiers seront gérés selon un processus caractérisé par la pérennité, l'efficacité et l'efficience. Les processus, les procédures et les bonnes pratiques qui seront appliquées dans la gestion des ressources dédiées à la protection du cyberespace devront être définies, communiqués, appliqués et respectés par les acteurs qui y sont impliqués.

1.4 Le plan opérationnel du fonctionnement du CERT fera l'objet d'un suivi régulier et périodique pour s'assurer de la bonne progression de son opérationnalisation selon les indicateurs de performance considérés. Les ressources humaines et financières mises à la disposition du CERT seront un facteur déterminant pour garantir son efficacité.

2. METTRE EN PLACE DES ACCORDS DE COOPERATION ENTRE LE CERT ET LES INSTITUTIONS GOUVERNEMENTALES HEBERGEANT DES SERVICES ET DES DONNEES SENSIBLES ET CRITIQUES

2.1 Des accords de coopération seront conclus entre le CERT et les institutions gouvernementales hébergeant des services et des données sensibles et critiques en vue de conjuguer les efforts destinés à sécuriser le cyberespace. Ces accords viseront à améliorer la capacité des structures publiques à protéger les services qu'ils déploient à travers le cyberespace.

2.2 Ces accords viseront à établir un cadre d'échange efficace pour recenser les services et les données hébergés sous la tutelle de structures publiques. Un inventaire sera alors établi pour classer les services et les données selon leur sensibilité et leur niveau de sécurité actuel.

2.3 A travers ces accords, le suivi des projets nationaux visant à protéger les composantes du cyberespace sera aussi amélioré. Entre autres, il sera important de veiller à ce que les solutions déployées soient conformes à la réglementation en vigueur et au référentiel général de sécurité.

2.4 Un cadre de concertation sera créé à travers ces accords en vue de rendre opérationnel l'audit annuel des structures étatiques. Cet audit permettra de vérifier la capacité des mécanismes de protection mis en place à assurer la détection et la réponse aux incidents de sécurité ainsi qu'à restaurer les dégâts qui résultent de leur occurrence.

2.5 Pour qu'ils soient efficaces, le partage d'information et le signalement d'incident doivent être à la fois encadrés et encouragés par les accords entre le CERT et les structures publiques. C'est ainsi que sera instauré le climat de confiance nécessaire pour donner des garanties que l'organisation qui partage des informations ne s'expose pas à des responsabilités excessives

3. METTRE EN PLACE DES ACCORDS DE COOPERATION ENTRE LE CERT ET LES OPERATEURS DE TELECOMMUNICATIONS ET LES FOURNISSEURS D'ACCES INTERNET

3.1 Des accords de coopération seront conclus entre le CERT et les opérateurs de télécommunications et les fournisseurs d'accès Internet, afin de rendre les services déployés sur le cyberespace Comorien difficiles à attaquer, tout en réduisant considérablement le potentiel de risque sur le pays.

3.2 Ces accords traiteront de la mise en place de mécanismes de protection contre le hameçonnage (*phishing*), du blocage des domaines et des adresses IP malveillantes et de la mise en œuvre de toute mesure capable de limiter la propagation des codes malveillants. Des mesures visant à sécuriser l'infrastructure de télécommunications et de routage Internet seront aussi considérées.

3.3 Sur un autre volet, ces accords porteront sur l'échange des informations relatives aux incidents de sécurité. En particulier, l'interception légale ainsi que les aspects sous-jacents (essentiellement la période de rétention et les procédures d'activation) feront l'objet de ces accords.

3.4 Ces accords de coopération viseront aussi à assurer une bonne coordination par rapport aux incidents de sécurité ayant lieu sur le cyberespace. Des canaux d'échange d'information seront alors définis à cet effet.

4. METTRE EN PLACE DES ACCORDS DE COOPERATION ENTRE LE CERT ET LES ASSOCIATIONS ACTIVES DANS LE DOMAINE DE LA CYBERSECURITE

4.1 Des accords de coopération seront conclus entre le CERT les associations actives dans le domaine de la cybersécurité afin de joindre les efforts en matière de sensibilisation et de formation.

4.2 Ces accords porteront essentiellement sur la sensibilisation à large échelle sur des thèmes relatifs à la cybersécurité et ceci en tirant profit des réseaux établis par les associations opérant dans le domaine de la cybersécurité.

5. METTRE EN PLACE DES ACCORDS DE COOPERATION ENTRE LE CERT ET LES INSTITUTIONS UNIVERSITAIRES ET DE RECHERCHE

5.1 Des accords de coopération seront conclus entre le CERT et les institutions universitaires et de recherche qui traitent les volets techniques et juridiques des systèmes d'information et de communication. L'objectif sera de faciliter l'insertion des diplômés dans le marché de la cybersécurité.

5.2 Ces accords permettront de collaborer dans l'encadrement des projets menés au sein de l'université pour qu'ils aient un impact technologique sur le terrain. Ces projets seront alors orientés vers des thématiques qui rejoignent les priorités du CERT et serviront à prospecter de nouvelles technologies ou à développer des prototypes de solutions de sécurité. Par conséquent, les diplômés et les jeunes chercheurs seront mieux outillés pour jouer un rôle prépondérant dans la protection du cyberespace national.

5.3 Des produits et services de pointe seront développés grâce à la collaboration des centres de recherche avec le CERT. Des incitations devront alors être créées à cette collaboration pour faciliter les transferts volontaires de technologie et des cycles courts de développement et de déploiement de meilleurs produits et services.

6. CREER UN POLE NATIONAL DE CYBERSECURITE VISANT A AMELIORER ET PARFAIRE LA GOUVERNANCE NATIONALE EN LA MATIERE

6.1 Un pôle national de cybersécurité sera créé afin de faciliter l'interaction entre les acteurs du cyberespace qui sont sous des tutelles différentes. Le pôle national de cybersécurité réunira très régulièrement les administrations compétentes de l'Union des Comores (économie numérique, sécurité, éducation, justice, affaires sociales, santé, économie, scientifique et recherche, direction du travail, etc.). Des autorités administratives indépendantes, des acteurs du secteur privé et des personnalités qualifiées pourront aussi être impliquées.

6.2 La mission de ce pôle sera notamment de mettre en œuvre un modèle de gouvernance permettant la réglementation des processus et des solutions en vue du développement d'une économie numérique durablement protégée où les acteurs impliqués dans la sécurité du cyberespace contribueront efficacement, chacun selon des prérogatives définies en termes de réglementation, de normalisation et de certification. Les principaux points abordés seront la gouvernance de la sécurité d'Internet, la protection des données personnelles ainsi que la sécurité informatique des opérateurs essentiels à l'économie.

6.3 Le pôle aura aussi pour mission de suivre les plans d'action découlant de la présente stratégie, d'identifier les technologies-clés pour le développement d'un environnement numérique de confiance. Il évaluera les besoins en formations initiales et continues, suivra les travaux de recherche et en accompagnera la valorisation, et adoptera un système de gestion des risques liés à la sécurité des systèmes d'information et de communication.

7. ADOPTER UN SYSTEME DE GESTION DES RISQUES LIES A LA SECURITE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

7.1 L'analyse des risques sera considérée comme un préalable à l'élaboration des directives et à la définition des contremesures permettant d'aider les responsables à tous les niveaux à protéger leurs systèmes d'information. A ce titre, un système de gestion des risques de sécurité sera adopté à l'échelle nationale et son application sera universelle sur le cyberespace.

7.2 Le système de gestion des risques comportera un volet relatif à l'évaluation des risques. Les aspects suivants feront partie de ce volet :

- Définir une grille d'évaluation du degré de criticité des données et des systèmes d'information et de communication des administrations, organismes publics et infrastructures d'importance vitale ;
- Recenser, identifier et classifier les systèmes sensibles et critiques des administrations, organismes publics et infrastructures d'importance vitale ;
- Évaluer périodiquement le niveau du risque pesant sur les infrastructures sensibles et critiques des administrations, organismes publics et infrastructures d'importance vitale ;
- Evaluer les plans de gestion du risque adoptés par les administrations, organismes publics et infrastructures d'importance vitale.

7.3 Le second volet sera relatif à l'utilisation des résultats de l'analyse des risques pour la prise de décision et ce à travers les actions suivantes :

- Mener des enquêtes pour collecter des données d'ordres juridiques, techniques et procédurales ayant trait à la sécurité des systèmes sensibles et critiques ;
- Produire des données statistiques et des indicateurs de suivi ;
- Assurer la veille technologique, juridique et réglementaire.

4.2 Axe 2 : Informer, former et sensibiliser les acteurs du cyberespace sur les risques encourus

1. DOTER CHAQUE NOUVEAU FONCTIONNAIRE D'UNE FORMATION BASIQUE EN CYBERSECURITE

1.1 Le programme d'une formation basique en cybersécurité sera mis en place pour que chaque nouveau fonctionnaire puisse se doter des connaissances élémentaires en cybersécurité avant de joindre son poste. Ces connaissances permettront de s'assurer que tous les fonctionnaires ayant accès aux données et systèmes hébergés sur le cyberespace, comprennent le rôle qu'ils jouent dans sa protection, et contribuent à cette protection dans leurs tâches quotidiennes.

8.2 Des sessions de formations de formateurs seront programmées pour assurer la couverture efficace de la cible du programme et la pérennité des actions qui se feront dans ce cadre. La répétition de telles actions fera en sorte que les employés aient les réflexes de cybersécurité et que la culture de la sécurité fasse partie intégrante de la culture des structures qui hébergent les données et les infrastructures sensibles et critiques.

2. INTRODUIRE DES FORMATIONS OBLIGATOIRES AU NIVEAU DE L'ENSEIGNEMENT SECONDAIRE ET PRIMAIRE

2.1 Au regard de la vulnérabilité des enfants et des adolescents connectés à Internet, des formations obligatoires seront conçues pour être prodiguées dans les écoles primaires, les collèges et les lycées secondaires. Ces formations viseront à sensibiliser cette population aux risques encourus à travers l'usage d'Internet et à la doter des bonnes pratiques permettant une interaction sécurisée avec les services en ligne. Les programmes de formation devront alors être élaborés pour satisfaire ce besoin.

9.2 Les programmes de formation devront renseigner les enfants et les adolescents sur les types de menaces auxquels ils sont sujets afin qu'ils puissent naviguer en ligne de façon la plus sécurisée possible, et les sensibiliser quant à leur responsabilité à protéger leur identité. Ils contribueront à diffuser les bonnes pratiques concernant l'utilisation sécurisée des ordinateurs et d'Internet (dont les réseaux sociaux) et finalement offrir aux parents des outils pour se protéger et pour protéger leurs enfants.

9.3 Les programmes de formation devront permettre aux enfants et adolescents de se familiariser avec la manière d'utiliser en toute sécurité les fonctions de leur appareil mobile (e.g., la caméra) et les services basés sur le mobile. Ce besoin est exacerbé par le fait que les appareils mobiles sont de plus en plus puissants et peuvent être utilisés pour réaliser toujours plus de tâches courantes. Une mauvaise utilisation de cet environnement pourrait donc constituer une menace sérieuse à l'encontre de cette population vulnérable.

9.4 Les programmes de formation seront mis en œuvre dans un premier temps dans un ensemble d'écoles primaires, de collèges et de lycées secondaires pour une expérience pilote avant d'être généralisés par la suite.

3. ELABORER UN PROGRAMME DE FORMATION ET DE SENSIBILISATION POUR LES DECIDEURS ET LES HAUTS CADRES

3.1 Les décideurs et les hauts cadres ont un rôle prépondérant à jouer dans l'écosystème de cybersécurité, en effet :

- Ils portent la responsabilité de prendre les décisions relatives aux fonctions de cybersécurité (identification, détection, protection, réponse, restauration) ;
- Ils représentent la cible privilégiée de plusieurs menaces telles que les *ransomwares*.

De ce fait, un programme de formation sera élaboré en vue de doter les hauts cadres des connaissances leur permettant de bien conduire les missions qui leurs incombent dans un environnement sain.

10.2 Le premier volet de ce programme portera sur la maîtrise des processus de décisions liés à la gestion des risques de sécurité. Ceci permettra aux décideurs et aux hauts cadres d'être des éléments actifs dans les actions nationales qui seront menées pour analyser les risques présents sur le cyberespace et prendre les contremesures adéquates.

10.3Le deuxième volet du programme de formation sera dédié aux bonnes pratiques permettant aux décideurs et aux hauts cadres d'interagir en toute sécurité avec les systèmes de leur environnement. Il s'articulera autour des points suivants :

- Comment communiquer en toute sécurité et de manière responsable ?
- Comment utiliser les médias sociaux de manière judicieuse ?
- Comment transférer les fichiers numériques de manière sécurisée ?
- Comment utiliser son mot de passe de façon appropriée ?
- Comment éviter la perte d'informations importantes?
- Comment s'assurer que seules les bonnes personnes puissent accéder à vos données ?
- Comment se protéger des virus et autres logiciels malveillants (malware) ?
- Qui avertir lorsque vous constatez un incident de sécurité potentiel ?
- Comment ne pas se faire piéger et divulguer des informations à des tiers malveillants ?

4. ELABORER UN PROGRAMME DE FORMATION POUR LES OPERATEURS D'INFRASTRUCTURES CRITIQUES

4.1 Un programme de formation destiné aux opérateurs d'infrastructures critiques sera mis en œuvre pour les assister à réduire la probabilité des incidents graves et, en cas de leur occurrence, d'en réduire la durée. En outre, la formation contribuera à améliorer la gestion et la compréhension des risques qu'encourent les infrastructures critiques.

11.2 Le programme de formation s'articulera autour d'études de cas permettant d'illustrer les concepts de base suivants :

- Gestion de la sécurité ;
- Gestion des risques ;
- Gestion de la continuité des affaires ;
- Gestion des crises ;
- Gestion des situations d'urgence ;
- Systèmes de contrôle interne.

11.3 Les participants au programme de formation auront pour rôle de créer des bases décisionnelles pour une affectation efficace des ressources (investissement minimal pour une augmentation maximale de la sécurité). Ils pourront alors expliciter les prestations qu'ils fournissent à la population et à l'économie et à évaluer les mesures visant à garantir ces prestations de concert avec les autorités compétentes. Ceci résultera en une amélioration continue de la disponibilité des infrastructures critiques présente sur le cyberespace.

5. ELABORER UN PROGRAMME DE FORMATION POUR LES ENTREPRISES PRIVEES QUI INTERAGISSENT AVEC DES SERVICES SENSIBLES ET CRITIQUES

5.1 Les entreprises privées qui interagissent avec les services sensibles et critiques (sans pour autant être des opérateurs) suivront un programme de formation qui les sensibilisera aux risques présents sur ces services et les responsabilisera quant à la criticité des tâches qui leur incombent. Des programmes de formation relatifs au développement et déploiement sécurisé d'applications ainsi qu'à la mise en place d'architectures réseau sécurisées seront élaborés.

12.2Les programmes de formation élaborés dans ce cadre devront considérer les études de cas illustrant l'utilisation des facteurs de risque suivants :

- Vies humaines (personnel et autres personnes présentes) : Il est essentiel de protéger de manière suffisante toutes les personnes présentes contre les incidences des aléas et de les mettre à l'abri en cas de danger imminent ;
- Terrains : Font partie des terrains toutes les surfaces en plein air destinées à la circulation, au stockage ou au parking, les espaces verts et les aires essentielles à l'activité de l'établissement ;
- Bâtiments : Les bâtiments comprennent toutes les structures construites en souterrain ou en surface.

6. REALISER DES PROGRAMMES NATIONAUX POUR VULGARISER LES CONCEPTS DE SECURITE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

6.1 Des programmes nationaux seront élaborés en vue de promouvoir la culture de la cybersécurité. L'effort de sensibilisation sera ainsi intensifié, tant auprès des jeunes qu'auprès des adultes, tant du côté du secteur public que du côté du secteur privé, et ceci pour viser une large cible au sein de laquelle les connaissances de base en matière de cybersécurité seront diffusées et partagées.

13.2 Des conventions de partenariat seront établies avec des acteurs du cyberespace en vue de permettre aux programmes nationaux de vulgarisation des concepts de sécurité des systèmes d'information et de communication d'atteindre une grande proportion de la cible visée.

13.3 Des actions pilotes seront réalisées pour la réalisation pratique des programmes nationaux pour la vulgarisation des concepts de sécurité des systèmes d'information. Ces actions seront concrétisées selon les dimensions suivantes :

- Développement de sites Internet ;
- Conception de brochures et d'imprimés ;
- Animation de séminaires, d'ateliers et de camps ;
- Réalisation de vidéos de sensibilisation ;
- Développement de supports interactifs.

7. ORGANISER DES COMPETITIONS NATIONALES EN CYBERSECURITE

7.1 Des compétitions nationales en cybersécurité seront organisées pour identifier les jeunes talents et les inciter à développer leurs compétences techniques. Afin de garantir la pérennité de ces compétitions, des communautés qui intègrent des comités techniques et des comités d'organisation seront créés.

14.2 Une prospection sur les compétitions internationales sera réalisée pour permettre aux lauréats des compétitions locales d'y participer. Les compétitions seront sélectionnées en fonction de leur adéquation avec les priorités technologiques définies dans la présente stratégie.

4.3 Axe 3 : Mettre en place des normes, des standards et des référentiels de sécurité

1. IDENTIFICATION DES OPERATEURS D'INFRASTRUCTURE CRITIQUE

1.1 Le Gouvernement se chargera de recenser les opérateurs d'infrastructure critique, afin de veiller à la mise en place d'un niveau de protection adéquat. Les besoins de protection spécifiques seront, le cas échéant, élaborés en étroite collaboration avec les opérateurs et les exploitants desdites infrastructures. Une commission intersectorielle sera créée à cet effet.

15.2 La liste des opérateurs d'infrastructure critique élaborée par la commission intersectorielle fera l'objet d'un texte réglementaire.

15.3 La commission intersectorielle procédera à la définition des besoins de protection des opérateurs d'infrastructures critiques et ceci par rapport aux indicateurs suivants :

- Fiabilité : Capacité de l'opérateur d'infrastructure critique à fournir les services requis tel que spécifié ;
- Disponibilité : Capacité de l'opérateur d'infrastructure critique à fournir les services requis par les entités légitimes ;

- Sûreté : Capacité de l'opérateur d'infrastructure critique à fournir les services requis sans l'occurrence d'incidents menant à un désastre ;
- Sécurité : Capacité de l'opérateur d'infrastructure critique à fournir les services requis en étant protégé contre les utilisateurs malveillants.

2. ETABLIR UN INVENTAIRE DES NORMES, DES STANDARDS ET DES BONNES PRATIQUES POUR TOUS LES DOMAINES D'APPLICATION

2.1 Un inventaire des normes, standards et bonnes pratiques qui sont en vigueur dans les domaines d'application des systèmes d'information et de communication sur le cyberespace Comorien sera dressé. Ses domaines d'application seront définis en fonction des opérateurs d'infrastructures critiques identifiés dans la présente stratégie.

3. DEFINITION DES NORMES DE CLASSIFICATION DES INFORMATIONS ECHANGEES ET STOCKEES SUR LE CYBERESPACE

3.1 Les échelles de classification des informations stockées et échangées sur le cyberespace seront définies en fonction du contexte global. Chaque échelle de classification sera associée à un niveau d'impact.

17.2 Les échelles d'impact seront définies selon les trois fonctions fondamentales de la cybersécurité : confidentialité, intégrité et disponibilité. Quatre dimensions seront utilisées à cet effet, à savoir l'impact sur la conformité, l'impact opérationnel, l'impact sur la réputation et l'impact financier.

17.3 Sur la base des échelles définies dans les deux points précédents, une analyse terrain des informations sera effectuée. Des ateliers de classification de l'information seront alors organisés en coordination avec les principaux acteurs concernés, en identifiant les interlocuteurs compétents et qualifiés, ayant autorité de décision sur les processus et informations pour lesquels ils sont sollicités.

17.4 Une politique nationale de classification des informations sera élaborée de manière à intégrer les règles et les mesures de sécurité à appliquer pour assurer leur adéquate protection. Cette politique devra traduire une approche de mise en œuvre pragmatique des mesures de protection pour chaque niveau de classification et à chaque étape du cycle de vie de l'information.

17.5 Un plan de mise en œuvre sera défini pour faciliter le déploiement de la politique nationale de classification des informations échangées et stockées sur le cyberespace. Les responsables des mesures de déploiement, les échéances de déploiement ainsi que les ressources requises seront alors définis à ce niveau.

4. DEFINITION DES NORMES D'EVALUATION DES RISQUES LIES A LA SECURITE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

4.1 Pour assurer l'uniformité des données collectées et traitées lors de la conduite du processus de gestion des risques par les acteurs du cyberespace, une norme sera mise en œuvre pour définir les valeurs qui seront adoptées pour les paramètres clés, à savoir :

- L'échelle d'impact ;
- L'échelle de probabilité ;
- L'échelle des risques.

18.2 Une politique de sécurité type pour les structures hébergeant des données et des infrastructures sensibles ou critiques sera développée et distribuée pour pallier à l'absence de politiques de sécurité pour la majorité des acteurs présents sur le cyberespace.

18.3 Des guides et des référentiels seront élaborés pour un déploiement efficace des politiques de sécurité. Ces guides traiteront aussi bien les aspects organisationnels, techniques et systémiques.

5. DEFINITION DES NORMES D'ECHANGE DE DONNEES SECURISEES SUR LE CYBERESPACE

5.1 Des échelles de protection de trafic seront définies de manière à prendre en compte les exigences adéquates en termes de confidentialité, d'authentification, de non-répudiation, d'anonymat et de propriétés anti-rejeu.

19.2 Chacune des échelles de protection définies dans le point précédent sera associée à une classe de données (définie selon la norme nationale de classification des données échangées et stockées sur le cyberespace). Ainsi, une norme nationale d'échange de données sécurisées sur le cyberespace sera établie.

6. DEFINITION DES NORMES DE GESTION DES DONNEES A CARACTERE PERSONNEL

6.1 Des normes de protection des données à caractère personnels seront définies en vue d'être appliquées par les acteurs du cyberespace qui gèrent directement les données personnelles des citoyens Comoriens ou indirectement via les informations de production. Un groupe de travail sera constitué à cet effet pour associer des processus de validation et de mise à jour aux normes qui seront mises en place.

20.2 Le groupe de travail sur la protection des données à caractère personnel procédera à l'élaboration de règles de protection des données personnelles tout au long de leur cycle de vie comprenant essentiellement le profilage, la création de sous-ensembles, le masquage, l'échange et l'archivage des données.

20.3 Le groupe de travail sur la protection des données à caractère personnel préparera un référentiel d'audit et de contrôle pour :

- Détecter les tentatives d'accès non autorisé aux données à caractère personnel échangées ou stockées sur le cyberespace ;
- Détecter les fonctions au niveau des applications qui ne sont pas en conformité avec les normes de protection des données à caractère personnel établie dans le cadre de la présente stratégie ;
- Assurer le respect de ces normes lors des phases de développement d'applications et de services qui utilisent des données à caractère personnel.

7. DEFINITION DES NORMES D'HOMOLOGATION DES SOLUTIONS DE SECURITE

7.1 Des normes d'homologation seront définies pour contrôler les outils logiciels et matériels utilisés lors du déploiement de services sur le cyberespace. Ces normes devront permettre de mesurer et de maîtriser les risques encourus derrière l'utilisation de ces composantes. Les éléments à prendre en compte dans la préparation de la démarche d'homologation sont :

- L'identification des systèmes soumis à l'homologation ;
- La définition des propriétés de sécurité devant être homologuées et de la profondeur requise dans le processus d'homologation ;
- La définition des acteurs impliqués dans la démarche d'homologation ;
- L'élaboration d'un modèle organisationnel pour la démarche d'homologation.

21.2 Une analyse des risques sera conduite en vue de déterminer les risques qui existent derrière l'utilisation des systèmes soumis à l'homologation, de les hiérarchiser et de déterminer des objectifs généraux qui permettront de diminuer certains d'entre eux et, à terme, de les amener à un niveau acceptable. Des critères d'homologation seront alors déduits de ces objectifs.

21.3 Des procédures d'audit et de contrôle seront définies pour assurer la détection des écarts relatifs aux critères d'homologation. La mise en œuvre des ces procédures sera aussi étudiée pour que des mesures de sécurité de nature technique, organisationnelle ou juridique soient proposées.

4.4 Axe 4 : Améliorer la sécurité et la résilience des infrastructures sensibles et critiques

1. **CREATION D'UN OBSERVATOIRE DE CYBERSECURITE**

1.1 Un observatoire de cybersécurité sera créé en vue d'analyser les données et les tendances émanant du terrain. Le rôle de cet observatoire sera focalisé sur les aspects de l'économie de la connaissance dans le domaine de la cybersécurité, en rassemblant les efforts publics et privés permettant de fournir, d'analyser et de diffuser des informations et tendances en la matière. La création de ce type de service réduira considérablement l'effort individuel et les coûts de la cybersécurité, tout en augmentant l'efficacité des mesures de protection et en fédérant les moyens mis pour l'analyse des informations et des tendances liées à la cybersécurité.

22.2 L'observatoire fournit, en se basant sur des données collectées avec son réseau de partenaires :

- des renseignements techniques ;
- un aperçu des menaces spécifiques aux différents secteurs d'activité utilisant les services et les infrastructures déployés sur le cyberespace ;
- un aperçu des mécanismes de protection ainsi que des métriques et des chiffres clés, nécessaires à une bonne gouvernance.

22.3 Un modèle économique sera défini pour valoriser l'intérêt commun autour des informations traitées par l'observatoire. Ceci permettra de développer des relations de partenariat avec des partenaires spécialisés dans les différents domaines d'applications de la cybersécurité.

2. ELABORER DES INDICATEURS DE PERFORMANCE POUR LE SUIVI DE L'ETAT DU CYBERESPACE EN MATIERE DE SECURITE

2.1 Une évaluation critique des rapports issus d'enquêtes et de recherches internationales sera menée afin d'obtenir une vue d'ensemble sur le savoir-faire existant permettant de mesurer le risque de la cybercriminalité et les indicateurs à utiliser. Les deux dimensions fondamentales utilisées dans ce cadre seront :

- L'impact : Reflète les dégâts créés par l'occurrence d'une menace ;
- La fréquence : Reflète le nombre d'occurrence moyen d'une menace à l'échelle d'une année.

23.2 A l'échelle nationale, différentes sources de données concernant la cybercriminalité à l'Union des Comores seront identifiées et analysées et une évaluation sera faite des données manquantes. A moyen terme, ceci donnera une vue mieux informée et scientifiquement fondée sur la menace, grâce au modèle national spécifique permettant de mesurer le coût et l'impact de la cybercriminalité et de recueillir des informations comparables et solides dans les années à venir.

23.3 Les indicateurs de performances collectés feront l'objet de directives et d'orientations stratégiques destinées aux décideurs politiques pour leur fournir un support à la décision sur la façon de faire progresser la mise en œuvre des principes intégrés dans la SNCS.

3. METTRE EN PLACE LES PROCEDURES DE GESTION DES INCIDENTS LIES A LA SECURITE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

3.1 Le Gouvernement mettra en œuvre des procédures pour garantir aux citoyens, entreprises, institutions, organismes publics et privés l'accès aux informations utiles pour se défendre contre les incidents liés à la sécurité des systèmes d'information et de communications.

24.2 Ces procédures viseront à développer la capacité des acteurs du cyberespace en matière de gestion des incidents et ce à travers les actions suivantes :

- mettre en échec la vaste majorité des activités malveillantes à volume élevé et à faible complexité ;
- augmenter la capacité à contrecarrer les menaces à volume faible et à impact significatif ;
- développer la capacité à gérer (collecter, vérifier, sceller, enregistrer, présenter) les preuves relatives aux incidents ayant lieu (totalement ou partiellement) sur le cyberespace Comorien ;
- développer la capacité à améliorer les mécanismes et les politiques de protection du cyberespace en fonction de l'expérience par la gestion des incidents.

24.3 Ces procédures seront diffusées et communiquées afin qu'elles puissent avoir l'effet escompté sur une grande proportion du cyberespace.

4. METTRE EN PLACE LES OUTILS DE GESTION DES INCIDENTS LIES A LA SECURITE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

4.1 Avant de procéder au déploiement des outils de gestion des incidents, leur architecture matérielle et logicielle sera conçue de manière à assurer une couverture des sites sensibles du cyberespace et une flexibilité d'extension. La possibilité d'utiliser (en totalité ou en partie) les équipements existants au niveau du CERT sera envisagée à ce niveau.

25.2 Des outils de gestion des incidents seront déployés sur le cyberespace afin de:

- Collecter les données relatives aux incidents de sécurité ;
- Assurer une notification fiable et protégée de l'occurrence d'incidents de sécurité ;
- Analyser les données collectées pour déceler les preuves et les éléments de preuve en relation avec les incidents auxquelles elles sont relatives ;
- Préserver les preuves collectées contre les modifications non-autorisées et l'accès illicite ;
- Archiver les données collectées et générées tout au long du processus de gestion des incidents.

25.3 En outre, une expérience pilote sera initiée en installant des sondes de collecte de données sur un ensemble de structures hébergeant des données et des infrastructures sensibles et critiques.

5. PUBLIER DES RAPPORTS ANNUELS RELATIFS AUX PERFORMANCES DE RESSOURCES ET DES SERVICES DEPLOYES SUR LE CYBERESPACE EN TERMES DE SECURITE ET DE RESILIENCE

5.1 Les données collectées lors de l'exécution du processus de gestion des incidents sur le cyberespace seront analysées en vue de générer des rapports annuels visant à diffuser les informations suivantes :

- Analyse du nombre d'incidents ;
- Analyse de la distribution des cibles (par métier, taille,...) ;

- Analyse de l'impact des incidents ;
- Analyse de la distribution des incidents par type ;
- Analyse de la distribution des incidents par objectif (motivation) ;
- Analyse de la durée des incidents ;
- Analyse des tendances.

26.2 Un événement national sera organisé pour présenter les résultats des rapports annuels et d'en tirer les leçons. Les discussions menées lors de cet événement seront ensuite diffusées sous formes d'actes en vue de valoriser les échanges susceptibles d'avoir lieu entre les acteurs du cyberespace.

6. ORGANISER DES EXERCICES NATIONAUX IMPLIQUANT LES ACTEURS PRIVES ET LES ASSOCIATIONS

6.1 Des exercices nationaux seront organisés pour évaluer la capacité des acteurs du cyberespace à répondre aux incidents de sécurité selon les plans de continuité et de restauration prévus. Des acteurs privés et publics seront impliqués dans ces exercices en vue de renforcer la synergie au sein du cyberespace.

27.2 Des simulations d'attaques seront réalisées pour sensibiliser les acteurs locaux aux risques encourus et renforcer leur capacité à maîtriser les techniques d'intrusion. Ceci améliorera leur aptitude à mettre en œuvre des solutions de sécurité adaptées à la réalité imposée par l'évolution des techniques utilisées pour réaliser des attaques sur les systèmes sensibles et critiques.

7. FEDERER ET MUTUALISER LES EFFORTS ENTRETENUS POUR LA SECURISATION DU CYBERESPACE

7.1 Les efforts entretenus par les acteurs publics et privés dans la sécurisation du cyberespace seront fédérés pour améliorer la résilience des systèmes sensibles et critiques déployés sur le cyberespace. A ce titre, un portail national sera créé pour assurer une visibilité des projets liés à la cybersécurité et susciter la constitution de consortia autour de ces projets.

28.2 Ce portail servira aussi à centraliser les livrables de veille stratégique en matière de cybersécurité élaborés par les acteurs du cyberespace.

28.3 De même, des initiatives seront menées pour mutualiser les ressources disponibles pour la collecte d'informations relatives aux incidents de sécurité.

4.5 Axe 5 : Renforcer la coopération internationale

1. ETABLIR UN INVENTAIRE DES ACCORDS ET DES CONVENTIONS EN MATIERE DE CYBERSECURITE

1.1 Une liste d'acteurs nationaux impliqués dans la cybersécurité sera établie. Les différents domaines d'applications des systèmes d'information et de communication seront considérés lors de la sélection de ces acteurs. De même, un point focal sera identifié pour chacun des acteurs considérés.

29.2 Un inventaire des accords et conventions signés par ces acteurs à l'échelle internationale sera dressé dans la perspective de mutualiser les efforts déployés pour l'implication des acteurs Comoriens à l'échelle internationale et améliorer l'efficacité des échanges mis en œuvre avec des partenaires internationaux.

2. CREER UN GROUPE DE REFLEXION SUR L'ADHESION A LA CONVENTION DE BUDAPEST ET LA CONVENTION DE MALABO

2.1 Un groupe de réflexion constitué d'experts en cybersécurité sera créé en vue d'étudier les opportunités et les risques derrière l'adhésion aux conventions de Budapest et de Malabo sur le cybercrime. Ce groupe sera pluridisciplinaire afin d'assurer que ses travaux traitent tous les aspects reliés à ces conventions.

30.2 Une étude d'opportunité sera élaborée pour synthétiser les résultats des travaux du groupe de réflexion. Elle portera sur l'analyse du contexte Comorien, l'étude des expériences d'autres pays et la prospection des évolutions prévues dans le domaine de la cybercriminalité. A la lumière de ces études, un ensemble de recommandations sera proposé quant à l'adhésion de l'Union des Comores aux conventions de Budapest et de Malabo.

3. DEFINIR DES PROCEDURES DE GESTION DE LA PREUVE NUMERIQUE EN CONFORMITE AVEC LES BONNES PRATIQUES UTILISEES A L'ECHELLE INTERNATIONALE

3.1 Des procédures de collecte et de constitution de preuves numériques seront définies de manière à considérer les points suivants :

- Définir les acteurs qui fournissent chaque élément de preuve ;
- Spécifier où, quand et par qui l'agrégation des éléments de preuve a lieu ;
- Définir les mesures de contrôle d'intégrité et d'authenticité des éléments de preuve ;
- Définir les formats de collecte, d'échange et d'enregistrement des éléments de preuve ;
- Concevoir le processus de vérification permettant de savoir si un élément de preuve est probant.

31.2 Des procédures de conservation et restitution de preuves numériques seront définies de manière à considérer les points suivants :

- Spécifier les modalités de transmission des éléments de preuve aux entités en charge de leur conservation ;
- Spécifier les modalités de restitution des données conservées ;
- Définir la politique d'archivage adoptée.

31.3 Des procédures de consultation et d'accès aux éléments de preuve seront définies de manière à considérer les points suivants :

- Concevoir la politique de consultation des éléments de preuve ;
- Définir les conditions d'accès aux éléments de preuve ;
- Définir les propriétés de sécurité vérifiée pour chaque mode de consultation.

31.4 Des procédures de vérification des éléments de preuve seront définies de manière à considérer les points suivants :

- Identifier les entités autorisées à vérifier les éléments de preuve ;
- Définir les conditions de vérification des éléments de preuve ;
- Concevoir le processus de vérification des éléments de preuve.

31.5 Des procédures définissant les modalités d'acceptation des éléments de preuve seront définies de manière à considérer les points suivants :

- Définir les conditions d'acceptation explicite et implicite des éléments de preuve ;
- Spécification des conventions de preuves utilisées pour les différents services du cyberespace ainsi que des éléments de preuve auxquels ils font référence.

4. FAVORISER LA CREATION DES LIENS DE RECONNAISSANCE MUTUELLE ENTRE LES ACTEURS DU CYBERESPACE COMORIEN ET LEURS HOMOLOGUES A L'INTERNATIONAL

4.1 Une recherche à l'échelle internationale sera menée pour identifier des entités homologues aux acteurs nationaux impliqués dans la sécurité du cyberespace. Cette recherche tiendra compte de la proximité des acteurs Comoriens avec les entités identifiées, et ce par rapport au contexte socio-économique.

32.2 Un processus sera amorcé pour solliciter la création de liens de reconnaissance avec les structures homologues. A ce titre, des notes conceptuelles et des dossiers de soumission seront préparés.

5. FAVORISER LES COOPERATIONS ENTRE LES ACTEURS PRIVES NATIONAUX ET INTERNATIONAUX OPERANT DANS LES DOMAINES DE LA CYBERSECURITE

5.1 Des incitations seront prévues pour encourager une collaboration étroite entre les acteurs privés nationaux et ceux opérant au niveau international pour échanger les informations sur les menaces, les vulnérabilités et l'efficacité des traitements. Ceci permettra de mettre en place une prévention efficace, une détection fiable et une mitigation efficiente.

33.2 Des incitations seront prévues pour encourager une collaboration étroite des acteurs privés nationaux et ceux opérant au niveau international pour développer conjointement des solutions aptes à être déployées sur le cyberespace Comorien. Pour garantir l'efficience de ces incitations, un ensemble de thématique d'intérêt sera défini pour canaliser l'effort de développement fruit des coopérations avec l'international vers les opportunités et les risques du cyberespace.

6. FAVORISER LES COOPERATIONS ENTRE LES ASSOCIATIONS NATIONALES ET INTERNATIONALES OPERANT DANS LE DOMAINE DE LA CYBERSECURITE

6.1 Une collaboration étroite sera établie entre les associations opérant au niveau national et celles opérant au niveau international pour améliorer l'efficacité des efforts de sensibilisation et de communication prévus dans cette stratégie. Des actions, des événements et des missions d'échange seront alors prévus pour concrétiser ces collaborations.

34.2 Des incitations seront prévues pour encourager l'inclusion des experts nationaux dans les communautés regroupant les experts internationaux en matière de cybersécurité. Ceci catalysera la constitution de communautés nationales regroupant les experts opérant dans les différents domaines d'application relatifs à la cybersécurité.

7. PARTICIPER ACTIVEMENT AUX CONCERTATIONS REGIONALES ET INTERNATIONALES RELATIVES AUX DOMAINES DE LA CYBERSECURITE

7.1 Le gouvernement devra encourager l'implication des acteurs de l'écosystème à des concertations (e.g., colloques, séminaires, conférences) régionales et internationales qui traitent des méthodes de gestion de risques, des standards et normes de sécurité, des systèmes d'accréditation et de certification, ainsi que dans le domaine de la gestion de la conformité.

35.2 Des groupes de travail seront créés pour développer la capacité des experts nationaux à maîtriser les techniques, les technologies et les outils relatifs aux méthodes de gestion de risques, standards et normes de sécurité, systèmes d'accréditation et de certification, ainsi que la gestion de la conformité. Ceci est de nature à permette, à moyen terme, de faciliter l'adhésion des experts nationaux aux instances internationales actives dans le domaine de la cybersécurité.

4.6 Axe 6 : Combattre la cybercriminalité

1. CREER UN GROUPE DE TRAVAIL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE

1.1 Un groupe de travail interministériel sera constitué en vue de faire des propositions en matière de lutte contre la cybercriminalité. Les questions abordées par le groupe de travail toucheront aux domaines suivants :

- La prévention de la cybercriminalité ;
- La formation et la sensibilisation des publics ;
- La gestion des preuves numériques ;
- Le contrôle des outils de sécurité déployés sur le cyberespace.

36.2 Des mécanismes de suivi seront définis pour que les travaux réalisés par le groupe de travail soient conformes aux priorités nationales et à l'évolution des technologies. Une fois validées, les recommandations établies par le groupe de travail seront soumises aux acteurs concernés pour assurer leur mise en œuvre éventuelle.

2. METTRE EN ŒUVRE LES MECANISMES POUR ANALYSER LE CADRE REGLEMENTAIRE ACTUEL D'UNE MANIERE PERMANENTE

2.1 Un mécanisme sera mis en œuvre pour prospecter, d'une manière permanente, les dispositions en vigueur au niveau du Ministère du Développement de l'Economie Numérique dans les domaines relatifs à la cybersécurité.

37.2 Un mécanisme sera mis en œuvre pour prospecter, d'une manière permanente, les dispositions en vigueur au niveau du Ministère de la Sécurité dans les domaines relatifs à la cybersécurité.

37.3 Un mécanisme sera mis en œuvre pour prospecter, d'une manière permanente, les dispositions en vigueur au niveau du Ministère de la Défense dans les domaines relatifs à la cybersécurité.

37.4 Un mécanisme sera mis en œuvre pour prospecter, d'une manière permanente, les dispositions en vigueur au niveau du Ministère de la Justice dans les domaines relatifs à la cybersécurité.

3. PROSPECTER LES DISPOSITIONS EN VIGUEUR (EN MATIERE DE LUTTE CONTRE LA CYBERCRIMINALITE)

3.1 Des actions seront menées pour étudier l'évolutivité du cadre réglementaire actuel en matière de lutte contre la cybercriminalité en considérant les éléments suivants :

- Evolution de l'état de sécurité du cyberespace ;
- Tendances liées aux technologies utilisées sur le cyberespace ;
- Retour sur expérience du cadre réglementaire actuel.

38.2 Sur la base de l'étude mentionnée dans le point précédent, des propositions seront élaborées pour faire évoluer le cadre réglementaire Comorien en matière de lutte contre la cybercriminalité.

4. TRANSPOSER LES DIRECTIVES REGIONALES ET INTERNATIONALES AU CONTEXTE COMORIEN

4.1 Des actions seront menées pour analyser l'évolution des initiatives internationales en la matière, essentiellement celles de Budapest et Malabo. Cette analyse englobera notamment l'impact de l'adhésion de certains pays à ces initiatives.

39.2 Sur la base de l'étude mentionnée dans le point précédent, des propositions seront élaborées pour faire intégrer certaines dispositions des directives régionales et internationales le cadre réglementaire Comorien en matière de lutte contre la cybercriminalité.

5. REFORMER LA GOUVERNANCE POUR GARANTIR UNE COOPERATION FLUIDE ENTRE LES ACTEURS DANS LA LUTTE CONTRE LA CYBERCRIMINALITE

5.1 Les acteurs nationaux impliqués dans la lutte contre la cybercriminalité seront identifiés et leurs rôles précisés. L'identification de ces acteurs englobera les institutions gouvernementales et publiques, les entreprises privées, les associations et les organisations non gouvernementales (ONG).

40.2 Un nouveau modèle de gouvernance pour la lutte contre la cybercriminalité sera proposé en tenant compte des profils et des capacités des acteurs identifiés ainsi que des actions prévues dans la présente stratégie. Les rôles de chacune des entités impliquées ainsi que les échanges et les partages de données et d'informations seront détaillés à ce niveau.

40.3 Des points focaux appartenant aux acteurs impliqués dans la lutte contre la cybercriminalité seront désignés pour faciliter l'application du nouveau modèle de gouvernance. Les canaux de communication adéquats seront aussi définis à ce niveau.

6. PREVOIR DES MECANISMES POUR LA PROSPECTION DES NOUVELLES TECHNIQUES D'ATTAQUE

6.1 Des mécanismes de prospection des nouvelles techniques d'attaque seront définis. En sus de l'effort de veille qui sera déployé à cet effet, un intérêt majeur sera accordé à l'expérimentation et la simulation des techniques identifiées.

41.2 Des points focaux dans les structures impliquées dans la prospection des techniques d'attaques seront désignés pour faciliter les échanges d'informations sous-jacents.

7. PREVOIR DES MECANISMES POUR LA PROSPECTION DES NOUVELLES TECHNIQUES DE PROTECTION

7.1 Des mécanismes de prospection des nouvelles techniques de protection seront définis. En sus de l'effort de veille qui sera déployé à cet effet, un intérêt majeur sera accordé à l'expérimentation et la simulation des techniques identifiées.

42.2 Des points focaux dans les structures impliquées dans la prospection des techniques de protection seront désignés pour faciliter les échanges d'informations sous-jacents.

4.7 Axe 7 : Instaurer une coopération avec le tissu universitaire et de recherche

1. ELABORER UN INVENTAIRE DES INSTITUTIONS ET DES ENSEIGNANTS-CHERCHEURS OPERANT DANS LE DOMAINE DE LA CYBERSECURITE

1.1 Les programmes de formation universitaire dans les domaines liés à la cybersécurité seront étudiés pour identifier les institutions présentant un potentiel leur permettant de contribuer à l'écosystème national de cybersécurité.

43.2 L'adhésion des institutions candidates pour faire partie de l'écosystème national de cybersécurité sera sollicitée. Les réponses reçues seront utilisées pour établir une base d'institutions opérant dans le domaine de la cybersécurité.

43.3 Les enseignants-chercheurs dont le domaine d'expertise se rapporte à la cybersécurité seront identifiés sur la base des modules enseignés et des publications scientifiques.

43.4 Les enseignants-chercheurs identifiés seront alors sollicités pour contribuer à l'écosystème national de cybersécurité. Les réponses reçues seront utilisées pour établir une base d'enseignants-chercheurs opérant dans le domaine de la cybersécurité.

2. DEVELOPPER LE PROGRAMME UNIFIE D'UN CURSUS UNIVERSITAIRE EN CYBERSECURITE

2.1 Le Gouvernement entend mettre en place un cursus universitaire dans le domaine de la sécurité de l'information pour pallier le risque d'un manque d'experts de la sécurité de l'information, ce qui constituerait un frein au développement de l'écosystème de la sécurité.

44.2 Un ensemble d'institutions universitaires sera défini pour qu'il soit la cible d'une expérience pilote où sera ce cursus sera déployé dans un premier temps.

44.3 Un programme unifié sera mis en œuvre pour inculquer aux diplômés qui suivront le cursus universitaire de cybersécurité un contenu homogène, de manière à faciliter leur intégration dans l'écosystème national de cybersécurité et leur collaboration sur le terrain sur la base des bonnes pratiques.

3. OFFRIR UN ENVIRONNEMENT FAVORABLE A LA VALORISATION DES PROJETS ISSUS DE L'UNIVERSITE SUR LE CYBERESPACE

3.1 Un concours national pour les projets universitaires dans le domaine de la cybersécurité sera organisé à une fréquence annuelle. Une thématique sera définie pour chaque édition en tenant compte des priorités nationales en matière de cybersécurité.

45.2 Les projets lauréats feront l'objet d'un accompagnement pour favoriser le développement de solutions nationales en matière de cybersécurité.

4. FAVORISER L'IMPLICATION DES ENSEIGNANTS UNIVERSITAIRES ET DES CHERCHEURS DANS LES ACTIVITES DE RECHERCHE ET DEVELOPPEMENT LIEES A LA CYBERSECURITE

4.1 L'implication des enseignants-chercheurs dans les activités de formation dans le domaine de la cybersécurité sera encouragée. Notamment, des efforts seront entretenus pour la création de laboratoires conjoints entre les institutions universitaires et des partenaires privés visant à :

- renforcer les capacités pratiques des enseignants-chercheurs à manipuler les solutions de cybersécurité ; et
- préparer les étudiants à accéder aux certifications internationales en cybersécurité.

46.2 Des incitations seront prévues aux enseignants-chercheurs pour la valorisation de leur expertise dans l'encadrement de projets liés à la cybersécurité et l'implication dans les actions de formation prévues dans la présente stratégie.

5. MONTER DES PROJETS POUR LE DEVELOPPEMENT D'OUTILS DE CYBERSECURITE

5.1 Des consortiums regroupant différents acteurs de l'écosystème national de la cybersécurité seront définis pour la réalisation d'outils de cybersécurité. Les efforts de ces consortia seront orientés vers les thématiques d'intérêt national en matière de cybersécurité.

47.2 Un suivi des projets de développement d'outils sera assuré pour contrôler leur avancement et monter des dossiers permettant une recherche de financement à l'échelle internationale.

6. IMPLIQUER LES UNIVERSITES DANS LES ACTIVITES DE VEILLE TECHNOLOGIQUE LIEE A LA CYBERSECURITE

6.1 Un mécanisme de collecte d'informations au sein des universités sera conçu et déployé au sein des institutions universitaires pour renforcer leur implication dans l'effort de veille technologique liée à la cybersécurité. Les sources d'information visées engloberont notamment les rapports des projets de fin d'études et les publications scientifiques.

48.2 Les données collectées seront analysées et consolidées pour dégager des tendances en matière de cybersécurité qui seront utilisées comme éléments de veille technologique.

7. MUTUALISER LES INFRASTRUCTURES DES LABORATOIRES DE RECHERCHE ET DES UNIVERSITES DANS LE DOMAINE DE LA CYBERSECURITE

7.1 Les ressources matérielles et logicielles existant au niveau des institutions universitaires et de recherche et pouvant être utilisées dans des projets liés à la cybersécurité seront recensées. L'association entre ces ressources et les besoins des projets de formation et de développement mentionnés dans la présente stratégie sera établie.

49.2 Un cadre visant à mutualiser les ressources identifiées sera mis en place pour tirer profit du partage d'expérience entre les utilisateurs multiples et améliorer le taux d'utilisation de ces ressources.

5. DISPOSITIF DE MISE EN ŒUVRE

5.1 Organes de gouvernance

Le dispositif de mise en œuvre et de supervision comprend les organes et les instances.

5.1.1 Pôle national de cybersécurité (PNC) :

Le Pôle national de cybersécurité représente l'organe à qui incombe la supervision de la SNCS. Ceci consiste principalement à :

- Veiller à l'alignement de l'exécution des actions avec les orientations de la SNCS ;
- Assurer la cohérence de la mise en œuvre des actions ;
- Normaliser les processus de gouvernance et de suivi de la SNCS.

Chargé de l'évaluation des programmes, des projets et des résultats. Il procède également à l'évaluation des établissements qui pilotent des programmes de cybersécurité.

Cet organe se réunit une fois par an et a pour mission de créer les conditions pour l'implémentation des programmes et actions prévus dans la SNCS.

A ce titre, il est chargé de :

- apprécier les stratégies d'intervention proposées ainsi que les rapports de suivi et d'évaluation des plans d'actions et recommandations ;
- faire des recommandations relatives à la mise en œuvre des programmes de la SNCS ;
- mobiliser les ressources nécessaires à la mise en œuvre des programmes de la SNCS ;
- harmoniser les efforts des parties impliquées dans la mise en œuvre des programmes de la SNCS.

5.1.2 L'observatoire national de cybersécurité

Les missions de l'observatoire national de l'incubation numérique consistent en les points suivants :

1. Veille scientifique et technologique ;
2. Etudes stratégiques et prospectives ;
3. Banque et base de données sur les résultats scientifiques et technologiques réalisés par les structures nationales de recherche et d'innovation ;
4. Base de données sur les associations scientifiques et les compétences nationales ;
5. Indicateurs scientifiques et technologiques.

5.2 Risques associés à la mise en œuvre de la SNCS

Risques	Programme affecté	Mesures d'atténuation
Instabilité institutionnelle Ce risque aurait pour effet d'impacter la solidité des liens au sein de l'écosystème entrepreneurial et d'affecter les perspectives de financement.	La gouvernance et par effet induit les autres programmes	Bien que ce risque soit difficile à anticiper, il convient d'ancrer le dispositif au plus tôt dans le paysage institutionnel après adoption des programmes de manière à assurer leur légitimité et leur pérennité. Un tel ancrage, dès lors qu'il remporte l'approbation politique, est moins sensible aux changements de la vie politique et institutionnelle.
Dispersion des responsabilités Ce risque provient de la multitude d'acteurs qui contribuent aux comités de pilotage, de mise en œuvre, et de veille et de prospection. Il consiste en la possibilité de diluer les prérogatives prévues dans le modèle de gouvernance de	Activités de pilotage et de mise en œuvre	L'atténuation du risque a lieu par la mise en œuvre rigoureuse du dispositif de gouvernance sur la base des dispositions à prévoir lors de la phase initiale du plan d'actions.

manière à perdre la traçabilité des actions et la responsabilité des acteurs.		
L'inertie légale et réglementaire Ce risque met en exergue le déphasage entre le rythme accéléré de l'innovation numérique et le rythme plus lent de l'adaptation du cadre légal et règlementaire. Cela peut conduire à des situations de blocage au regard de développements de nouvelles applications ou de nouveaux services dont la prise en compte dans le cadre juridique et réglementaire est substantiellement retardée.	Toutes les sous-actions	L'atténuation de ce risque repose essentiellement sur un renforcement des capacités des acteurs majeursdans les domaines liés aux aspects de la réglementation et de la régulation du cyberespace.
Incertitude du financement Le risque réside dans le désistement de certains partenaires financiers sollicités ou dans les retards qui peuvent être engendrés dans l'engagement du budget.	L'ensemble des actions	En vue de bénéficier de l'accompagnement des PTBA pour une mise en œuvre réussie de la stratégie, il est indispensable de procéder à une priorisation des actions. Le suivi régulier et rigoureux doit également être de mise afin de rassurer les PTBA et éviter des retards éventuels.

6. GLOSSAIRE

- CERT : Computer Emergency Response Team
- NIST : National Institute for Standards and Technology
- PNC : Pôle National de Cybersécurité
- SNCS : Stratégie Nationale de Cybersécurité

+