الجمهورية الإسلامية الموريتانية
شرف - إخاء - عدل

RÉPUBLIQUE ISLAMIQUE DE MAURITANIE
Honneur - Fraternité - Justice

وزارة التحول الرقمي والابتكار وعصرنة الإدارة
Ministère de la Transition Numérique, de l'Innovation et de la Modernisation de l'Administration

STRATÉGIE NATIONALE DE SÉCURITÉ NUMÉRIQUE 2022-2025

Organised Crime: West African Response on Cybersecurity and fight against Cybercrime (OCWAR–C)

TABLE DES MATIÈRES

EDITORIAL

MOHAMED OULD BILAL MESSOUD
Premier Ministre

Après le renforcement de notre connectivité nationale en fibre optique ces dernières années, l'augmentation significative du taux de pénétration qui a atteint 70% en 2021 et la préparation de projets importants d'infrastructures télécoms à l'instar de celui de la connectivité par un second câble sous-marin, notre pays est désormais fortement connecté au cyberespace.

Nous profitons ainsi des avantages d'Internet mais nous nous exposons davantage aux cybermenaces capables de nuire gravement à notre développement et menacer notre sécurité nationale.

Devant une telle situation, la cybersécurité devient une urgence afin de mitiger les risques qui pèsent sur nos systèmes informatiques qui constituent le support de notre patrimoine numérique.

En effet, de par les perspectives économiques offertes par les technologies numériques où se généralisent l'Internet des objets, l'informatique en nuage (Cloud) et le big data, il est à rappeler qu'une transition réussie vers le cyberespace passe par la mise en œuvre de la sécurité de l'information en rempart face aux menaces croissantes et pour installer la confiance numérique.

Par conséquent, nous devons renforcer nos services de cybersécurité et adopter un plan intégré pour cet objectif en conformité avec les standards internationaux afin de garantir son efficacité.

Ces préoccupations partagées au niveau de la sous-région et du continent ont conduit à des initiatives, dans lesquelles notre pays est très actif, à la fois dans le cadre de la Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de l'Afrique de l'Ouest (CEDEAO et Mauritanie) et de la Stratégie de transformation numérique pour l'Afrique (2020-2030). Pour cette dernière, un axe spécifique est consacré à la cybersécurité et à la protection de la vie privée et des données personnelles.

La Stratégie nationale de sécurité numérique mise en place par notre Gouvernement est la traduction concrète de la volonté du Président de la République de soutenir le développement du numérique dans notre pays tout en assurant la sécurité nécessaire des usagers et des entreprise. Conçue en étroite collaboration avec les différents acteurs, elle s'adresse aux particuliers comme aux acteurs publics et privés qui doivent se protéger durant leurs usages de l'Internet, ainsi, tous ensemble nous contribuerons à une meilleure cybersécurité nationale.

Des objectifs importants sont fixés dans cette Stratégie. La création, depuis le mois de mai 2021, d'un Département Ministériel chargé de la transition numérique, de l'innovation et de la modernisation de l'Administration permettra un suivi rigoureux de la mise en œuvre dans les délais de cette Stratégie. Le Gouvernement apportera tout le soutien nécessaire pour réussir cette mission.

Notre **cyberespace sera ainsi ouvert, résilient, de confiance**, assurant la sécurité et la défense des systèmes numériques du pays et luttant contre la cybercriminalité.

Le plan d'action de la cybersécurité sera mis en œuvre dans le respect strict des libertés fondamentales et des droits de l'homme inscrits dans notre Constitution et les Conventions et Traités dont nous sommes partie.

Abdel Aziz DAHI
Ministre de la Transition Numérique, de l'Innovation et de la Modernisation de l'Administration

La création d'un Département Ministériel chargé de la transition numérique, de l'innovation et de la modernisation de l'Administration témoigne de la volonté de l'État de faire des technologies de l'Internet un levier pour améliorer le fonctionnement et l'efficacité des administrations ainsi que le bien-être de la population. Cependant, ces technologies sont sujettes à des risques et des menaces croissantes exposant les usagers et les entreprises à la perte de confiance dans le numérique et à plus de réticence à l'exploiter et à profiter ainsi du potentiel important qu'il offre.

Au-delà de ces problèmes déjà cités, les infrastructures critiques et les services essentiels du pays peuvent être interrompus, créant ainsi des situations particulièrement graves pour la Nation, son économie, sa sécurité et sa population.

Face à ces risques et menaces, l'État met en place cette Stratégie nationale de sécurité numérique et engage notre Département pour sa mise en œuvre.

Cette Stratégie doit garantir la sécurité et la résilience des dispositifs numériques du pays, dans tous les secteurs d'activité et donc de manière globale et transversale.

Elle adresse des problématiques diverses avec des dimensions multiples, notamment techniques avec une complexité qui ne cesse de croitre pour prendre en compte la multiplication, la variété et la sophistication des technologies, des architectures et des usages. La Stratégie nationale de sécurité numérique prévoit également des mesures au niveau politique, en particulier législatives, notamment pour fixer des obligations de protection des opérateurs les plus critiques et pour mettre en place les mesures de sécurisation du dispositif de l'État. Elle a aussi une dimension opérationnelle forte, tant pour la prévention des attaques informatiques que pour la remédiation des incidents affectant les systèmes numériques et pour la gestion des conséquences de ces incidents sur le fonctionnement des administrations et des acteurs privés.

La Stratégie nationale de sécurité numérique répond aux enjeux nouveaux auxquels doit répondre notre pays pour protéger son développement économique tout en se basant sur nos engagements régionaux et continentaux. En effet, notre pays est signataire de la Convention de l'Union africaine de 2014 sur la cybersécurité et la protection des données à caractère personnel, dite Convention de Malabo, qui fixe les mesures de cybersécurité et de lutte contre la cybercriminalité à prendre au niveau national. Nous avons aussi adopté une législation spécifique dans ce domaine, le renforçant et permettant plus de coopération avec les autres ? États.

Avec les orientations stratégiques inscrites et le plan d'action à horizon 2025, notre Département veillera à atteindre les objectifs et le plan d'action fixés par le Gouvernement dans la présente stratégie.

Ces objectifs sont basés sur les deux grands piliers de la politique nationale destinée à renforcer la sécurité numérique, à savoir : la cybersécurité, qui consiste à renforcer la sécurité et la défense des systèmes numériques publics et privés, notamment les plus critiques pour le pays, face aux menaces, et la lutte contre toutes les formes de cybercriminalité.

Notre cyberespace sera ainsi plus sûr et favorable à un développement économique et social plus rapide.

1. LA TRANSFORMATION NUMERIQUE DE LA MAURITANIE ET SES ENJEUX DE SECURITE

Les technologies numériques désignent principalement les techniques de l'informatique, de l'Internet et des télécommunications qui permettent à tous de communiquer, d'accéder aux sources d'information, de stocker, de réaliser des transactions électroniques pour l'achat de biens ou la souscription de contrats, de produire et de transmettre l'information sous différentes formes.

Ces technologies jouent un rôle moteur et transversal pour la croissance économique, l'implication citoyenne et l'amélioration de la qualité et de l'accessibilité des services publics. En effet, elles structurent les échanges, l'économie, la vie au travail et la vie sociale à travers une transformation profonde. Elles simplifient l'accès aux services de santé et d'éducation, favorisent l'inclusion financière et les échanges de biens et services à distance.

Grâce à la contribution des technologies numériques, de nombreuses possibilités émergent : paiement électronique, gestion intelligente des ressources, réduction des coûts de production, e-Gouvernement, accès aux sciences, transition vers les villes intelligentes. Ces technologies représentent ainsi un élément crucial dans la réalisation de la plupart des 17 Objectifs de Développement Durable (ODD) inscrits dans l'Agenda 2030 des Nations Unies.

Pour tirer profit de ces technologies, le Gouvernement a mis en place un programme ambitieux, composé des six axes suivants :

- (i) Mise à niveau du cadre juridique et institutionnel du secteur du numérique ;
- (ii) Alphabétisation et développement des compétences dans le domaine du numérique ;
- (iii) Renforcement de la cybersécurité et de la confiance numérique ;
- (iv) Développement des infrastructures numériques ;
- (v) Développement de l'Administration électronique (e-Gouvernement) ;
- et enfin (vi) Développement des Systèmes d'Information qui constituent le socle sur lequel se base l'Administration électronique.

Des réalisations importantes ont été effectuées ces dernières années dans chacun des axes de ce programme.

(i) Le premier axe, consacré à la mise à niveau du cadre juridique et institutionnel du secteur du numérique, a pour objectifs de disposer d'un environnement institutionnel et règlementaire propice au développement harmonieux et durable des usages numériques, de favoriser l'émergence d'un marché télécom concurrentiel encourageant l'investissement et de garantir la protection des données à caractère personnel utilisées dans des applications numériques.

Dans ce cadre, un Haut Conseil du Numérique (HCN) a été créé afin de fournir un cadre d'orientation, favoriser la mutualisation des ressources, renforcer la concertation et la coordination des politiques et stratégies de développement du numérique et rationaliser les ressources. La mise en place récente de ce Haut Conseil témoigne de la volonté politique et du rôle grandissant que l'État entend donner au numérique dans les différents domaines de la vie économique et sociale.

En complément, un programme de réformes a été lancé pour favoriser l'émergence d'un marché télécom concurrentiel propice à l'investissement et à l'amélioration de la régulation des services télécoms. Certaines de ces réformes sont déjà adoptées et d'autres sont en cours de finalisation. Elles portent sur :

- L'opérationnalisation du régime des autorisations prévu dans la loi sur les communications électroniques ;

- Le renforcement de la régulation de l'accès aux infrastructures essentielles et au haut débit y compris à celles possédées par des sociétés ne disposant pas de licences télécom ;
- La préparation d'une loi pour réduire le coût de déploiement des infrastructures numériques grâce à la promotion de la coordination intersectorielle des travaux de génie civil menés dans le cadre de projets publics d'infrastructure.

Pour ce qui est du cadre juridique de la Société Mauritanienne de l'Information, constitué de lois adoptées entre 2016 et 2018 sur la protection des données à caractère personnel, les transactions électroniques et la lutte contre la cybercriminalité, tous les décrets d'application ont été promulgués ou le seront début 2022. Ils mettent en place des mesures nécessaires pour instaurer un climat de plus grande confiance numérique, protéger les libertés fondamentales et les transactions des individus dans un environnement numérique, répondre aux risques d'intrusion et d'attaques visant les systèmes d'information du pays et particulièrement ceux des Infrastructures critiques nationales (ICN), et permettre le développement d'une administration plus transparente, responsable et accessible grâce au numérique.

Par ailleurs, une assistance technique a été lancée récemment en coopération avec le PNUD pour la création d'une Agence du Numérique de l'État, qui sera chargée des aspects opérationnels de développement du numérique.

(ii) Le deuxième axe, dédié à l'alphabétisation et au développement des compétences dans le domaine du numérique, a pour objectifs de répandre la culture numérique, d'impulser la créativité et l'innovation et de permettre aux couches de population, aux jeunes et aux entreprises d'atteindre les performances requises pour développer et exploiter les technologies numériques.

Le statut antérieur d'Association d'utilité publique du Centre de Formation et d'Échanges à Distance CFED/Mauritanie a été remplacé par celui d'établissement public administratif (EPA), plus adapté à sa mission de formation et de renforcement de compétences par le biais des technologies de l'Information et de la Communication pour l'Éducation (TICE).

Par ailleurs, suite à l'avènement de la pandémie de COVID-19, le Département a mis en place des plateformes de formation en ligne pour favoriser la continuité pédagogique dans le contexte d'arrêt des cours en présentiel.

(iii) Le troisième axe, portant sur le renforcement de la cybersécurité et de la confiance numérique, vise à assurer la protection et la sécurisation des systèmes d'information et des transactions électroniques, et à protéger les usagers des services Internet.

De façon préalable à la mise en place de la présente Stratégie nationale de sécurité numérique, la Mauritanie a rejoint le projet OCWAR-C (projet destiné à renforcer la cybersécurité et la lutte contre la cybercriminalité en Afrique de l'Ouest). Ceci nous a permis d'être un acteur actif dans la mise en place de la Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de l'Afrique de l'Ouest (CEDEAO et Mauritanie). Nous avons aussi activement contribué à l'élaboration de la Stratégie de transformation numérique pour l'Afrique (2020-2030) de l'Union africaine, dont un axe spécifique est consacré à la cybersécurité et à la protection de la vie privée et des données personnelles. Rappelons que notre pays est signataire de la Convention de l'Union africaine de 2014 sur la cybersécurité et la protection des données à caractère personnel, dite Convention de Malabo, qui fixe les mesures de cybersécurité et de lutte contre la cybercriminalité à prendre au niveau national.

Sur le plan opérationnel dans le domaine de la cybersécurité, le MTNIMA prépare la mise en place d'un Centre national de veille, d'alerte et de réponse aux incidents informatiques du type CERT/CSIRT (*Computer Emergency Response Team / Computer Security Incident Response Team*) conforme aux standards

internationaux. Il prévoit aussi la création d'un centre opérationnel de la sécurité (SOC, *Security Operation Center*) pour assurer la cybersécurité de l'infrastructure informatique de l'Administration.

(iv) Le quatrième axe portant sur le développement des infrastructures numériques fait l'objet d'une Stratégie de promotion du haut débit et d'accès universel, en cours d'approbation, qui permettra de disposer d'un plan cohérent, à moyen terme, pour développer rapidement la couverture Internet et le haut débit. En effet, il est établi que les pays disposant de haut débit sont deux fois plus efficaces en matière de numérique que les pays qui n'en disposent pas. Cette Stratégie fixe trois principaux objectifs :

- Élargir l'accès aux services de télécommunications, connecter tous les chefs-lieux des Willayas et Moughataas au réseau large bande national et développer l'Internet haut débit ;
- Sécuriser la connectivité internationale permettant l'accès aux réseaux mondiaux de télécommunication ;
- Et disposer de capacités d'hébergement propices au développement des contenus et applications de l'économie numérique.

Région ou pays	2019
Pays développés	128,9%
Pays en développement	103,8%
Monde	103,0%
Mauritanie	118,0%
Afrique	80,1%
Monde arabe	100,6%
Asie pacifique	111,7%
CEI (Communauté des États Indépendants)	140,1%
Europe	118,4%
Amérique	110,1%

Figure 1 Benchmark du taux de pénétration du téléphone mobile en 2019

Région ou pays	2019
Pays développés	33,6%
Pays en développement	11,2%
Monde	14,9%
Mauritanie	0,3%
Afrique	0,4%
Monde arabe	8,1%
Asie pacifique	14,4%
CEI (Communauté des États Indépendants)	19,8%
Europe	31,9%
Amérique	22,0%

Figure 2 Benchmark du taux de pénétration de l'Internet fixe en 2019

Région ou pays	2019
Pays développés	121,7%
Pays en développement	75,2%
Monde	83,0%
Mauritanie	63,0%
Afrique	34,0%
Monde arabe	67,3%
Asie pacifique	89,0%
CEI (Communauté des États Indépendants)	85,4%
Europe	97,4%
Amérique	104,4%

Figure 3 Benchmark du taux de pénétration de l'Internet mobile 2019

Région ou pays	2019
Pays développés	35,6%
Pays en développement	7,4%
Monde	12,2%
Mauritanie	1,5%
Afrique	0,8%
Monde arabe	8,8%
Asie pacifique	8,9%
CEI (Communauté des États Indépendants)	19,4%
Europe	33,6%
Amérique	22,5%

Figure 4 Benchmark du taux de pénétration du téléphone fixe en 2019

Dans le cadre du premier objectif, la construction de 1 700 km de réseau en fibre optique a été achevée en 2021 grâce au Projet WARCIP-Mauritanie financé par la Banque Mondiale, faisant passer le réseau national de fibre optique de 2 300 km à 4 000 km. Elle a permis de sécuriser certaines liaisons existantes du backbone national et d'étendre la connectivité Internet haut débit provenant du câble sous-

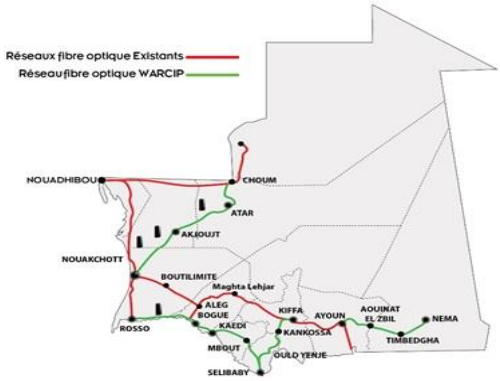

Figure 5 Réseau national de fibre optique

marin à des régions mal desservies. Ont ainsi été créés une boucle locale à Nouakchott et les tronçons « Nouakchott-Atar-Choum », « Rosso-Boghé-Kaédi-Sélibabi-Kiffa » et « Aioun-Nema ».

Par ailleurs, une révision des cahiers des charges des opérateurs télécoms est en cours dans le cadre du renouvellement des licences 2G/3G et de l'octroi de licences LTE-4G. Avec l'octroi des licences 4G, le haut débit mobile couvre Nouakchott et Nouadhibou depuis 2021 et s'étendra vers les autres capitales des wilayas d'ici 2023.

Les efforts consentis ont permis un développement important de la couverture. Le taux de pénétration de la téléphonie fixe et mobile est passé de 106% en 2017 à 117% en 2020 alors que le taux pénétration de l'accès à l'Internet est passé, durant la même période, de 35% à 62%. En même temps, la qualité de l'accès à l'Internet s'est améliorée du fait de l'augmentation de la bande passante internationale disponible, passée de 21 Gbps en 2018 à plus de 100 Gbps en 2021. Ainsi la bande passante par utilisateur est passée de 10 kbps en 2018 (voir les comparaisons ci-dessous réalisées par l'UIT en 2018) à plus de 20 kbps fin 2020.

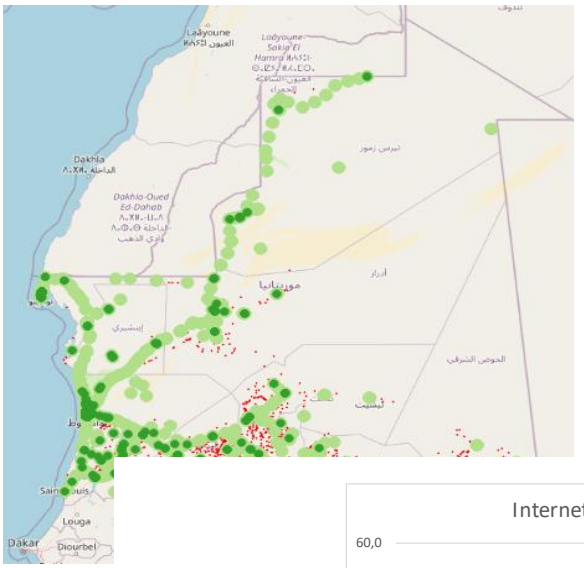

Figure 6
rés

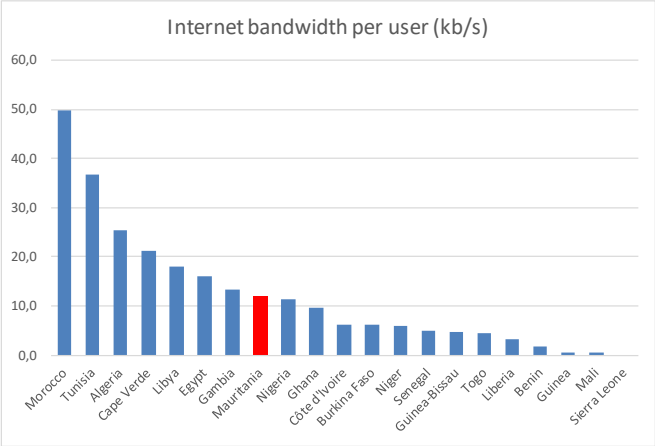

Figure 7 Comparaison des capacités Internet par utilisateur en 2018

Pour le second objectif de sécurisation de la connectivité internationale, la mobilisation des financements a eu lieu et la Banque Européenne d'Investissement a annoncé son intérêt pour y contribuer.

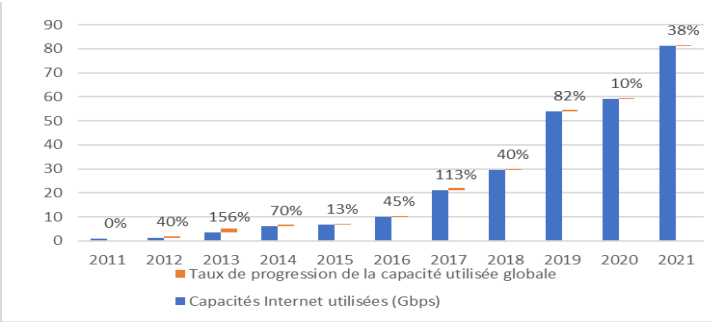

Figure 5 Évolution de la capacité internationale utilisée

(v) L’axe cinq du plan d’action, relatif au développement de l’Administration électronique (e-Gouvernement), comporte les objectifs suivants :

- Simplifier l'accès à l'information publique et aux contenus numériques ;
- Améliorer la qualité et l’accessibilité des services publics par l'usage des technologies numériques ;
- Et favoriser la collaboration entre les services de l'Administration publique et le développement des services en ligne intégrés.

Ainsi, une étude de faisabilité a été lancée afin de préparer la mise en place d’une solution e-Gouvernement permettant la dématérialisation des principales démarches administratives, la digitalisation des moyens de paiements du secteur public et la protection des données de l’Administration. Un appel d’offres a été lancé pour la mise en place d’une plateforme de dématérialisation des services publics et le développement d’un premier lot de 25 services en ligne durant les années 2021/2022.

Enfin, afin de favoriser la collaboration entre les services de l'Administration publique, l’extension du réseau Intranet administratif haut débit (RIAD) est en cours de préparation.

(v) Pour ce qui est du dernier axe du plan d’action, consacré au développement des Systèmes d'Information (SI) de l’Administration publique, une nouvelle approche de mise en place des SI est en cours de préparation pour permettre le développement rapide de modules autonomes au profit des usagers et rompre avec la situation où les SI sont centrés sur des problématiques de backoffice dont l’une des missions était de générer des impressions de masse pour les démarches administratives des citoyens et des entreprises.

Le pays est prêt à développer son e-Gouvernement. En effet, les principaux référentiels (référentiel des personnes - État civil, référentiel des entreprises - SI Impôt, ….) et les préalables pour le paiement électronique (cadre juridique et systèmes et moyens de paiement, solutions techniques au niveau de la Banque Centrale et au niveau du GIMTEL) sont d’ores et déjà en place. Le classement EGDI (*e-Government Development Index*) de la Mauritanie est passé en 2020 à la position 176/193, ce qui lui a permis de rejoindre le groupe de pays ayant un EGDI moyen.

Pour ce qui est des perspectives, d’autres projets sont en cours de préparation et devraient permettre à la Mauritanie d’atteindre les objectifs qui ont été fixés par la Commission des Nations Unies sur le large bande pour le développement durable à horizon 2025 :

a) Disposer d'un plan ou d'une Stratégie nationale de large bande, avec son financement : cette Stratégie a été mise en place en février 2019 et les financements sont en cours de mobilisation ;
b) Les services à large bande d'entrée de gamme devraient être proposés à la population à un tarif inférieur à 2% du revenu national brut (RNB) par habitant ;
c) La pénétration des utilisateurs de l'Internet à large bande devrait atteindre au moins 35% ;
d) 60% des jeunes et des adultes devraient avoir atteint au moins un niveau minimum de compétences numériques durables afin d’accéder, d’utiliser et de bénéficier du haut débit et des ressources Internet ;
e) 40% de la population mondiale devrait utiliser les services financiers numériques ;
f) Réduire de 50% la non-connexion des micro, petites et moyennes entreprises (MPME) par secteur ;
g) Et l'égalité des sexes devrait être atteinte dans tous les objectifs y compris en termes d’utilisateurs d'Internet, de compétences numériques, de services financiers numériques et des MPME.

Par ailleurs, le Département entame actuellement, en collaboration avec l’ESCWA, l’élaboration d’une Stratégie de transition numérique pour le pays, couvrant les cinq prochaines années.

Au bilan, on constate qu'en Mauritanie, l'usage des technologies numériques se généralise rapidement sur le territoire et s'intègre dans les services critiques comme dans la population. L'économie devient de plus en plus numérique et les échanges avec l'extérieur, à travers l'Internet, de plus en plus importants.

2. LA SITUATION ACTUELLE DE LA SECURITE NUMERIQUE ET LES DEFIS A RELEVER

Partout dans le monde, la criminalité se développe en même temps que le numérique investit peu à peu toutes les activités humaines, dans tous les secteurs. Les menaces dans le cyberespace impactent les individus, les institutions, les États et les sociétés. De nouveaux concepts apparaissent : Cyber-incivilité, Cyber-vandalisme, Cyber-délinquance, Cybercriminalité, Cyber-espionnage, Cyber-terrorisme et Cyber-conflit. La cybersécurité et la lutte contre la cybercriminalité deviennent donc des enjeux critiques et stratégiques. Un État qui ne dispose pas des moyens d'assurer la protection de son espace virtuel ne peut pas garantir la sécurité de ses échanges électroniques, de ses flux financiers, de ses infrastructures critiques et des données personnelles de ses citoyens.

En Mauritanie, à l'instar du reste du monde, on assiste depuis quelques années à l'apparition d'une nouvelle délinquance qui exploite les réseaux numériques, les failles de sécurité en forte augmentation avec l'arrivée de nouvelles technologies et de nouveaux usages numériques, la vulnérabilité de nombreux systèmes informatiques non à jour des correctifs de sécurité, et la sensibilisation insuffisante des usagers aux menaces cybercriminelles. Nous faisons ainsi face à des attaques et à des menaces très variées, parmi lesquelles : le défacement des sites web institutionnels, la Cyber-escroquerie visant à soutirer des sommes d'argent assez significatives à des citoyens, la saturation des réseaux et serveurs par des attaques en déni de service utilisant des Botnets, ou encore la prise de contrôle de systèmes numériques par dissémination de malwares exploitant les vulnérabilités des logiciels et des réseaux.

Face à cette situation, il est essentiel que la Mauritanie renforce la sécurité et la résilience de son cyberespace, ainsi que la lutte contre les atteintes aux systèmes numériques du pays et les utilisations malveillantes du cyberespace. Tel est l'objectif de la présente Stratégie nationale de sécurité numérique.

Si la Mauritanie a procédé au renforcement de son cadre législatif, notamment à travers l'adoption de la loi 2016-007 relative à la cybercriminalité et de la loi 2018-002 portant sur les transactions électroniques, un travail important reste à faire. La présente Stratégie fixe dans ce but des objectifs stratégiques et les actions à mettre en œuvre dans les cinq années à venir, de façon efficace et intégré.

Cette Stratégie nationale de sécurité numérique doit répondre aux besoins grandissants dans ce domaine. Rappelons à titre d'exemple que :

- Notre dépendance vis-à-vis des technologies numériques ne cesse de croître dans tous les secteurs d'activité, alors que les menaces liées à l'utilisation de ces technologies augmentent tous les jours.
- L'ampleur et les préjudices causés par des cyberattaques dans le monde ont explosé ces dernières années, pour atteindre un coût global de 1 000 milliards de dollars (1 % du PIB mondial).
- Ce chiffre est en forte croissance (15% par an en moyenne), aggravé encore par l'utilisation de l'Internet résultant de la pandémie COVID-19.
- Un rapport de McAfee Labs indique qu'au 1er trimestre 2020, les incidents recensés touchant plusieurs secteurs à la fois ont augmenté de 94 %. Une hausse a également été enregistrée pour le secteur public (73 %), les individus (59 %) et la fabrication (44 %).

3. LES OBJECTIFS STRATEGIQUES A ATTEINDRE ET LES ACTIONS A REALISER

Relever les défis qui se posent à la Mauritanie pour garantir un cyberespace ouvert, résilient et de confiance nécessitent la mise en œuvre de nombreuses actions, réparties en six grands objectifs stratégiques (OS) :

- OS1 : Doter la Mauritanie des institutions nécessaires à sa sécurité numérique
- OS2 : Renforcer la sécurité du cyberespace mauritanien et des infrastructures critiques
- OS3 : Renforcer le dispositif national de lutte contre la cybercriminalité
- 0S4 : Développer la sensibilisation et les compétences
- OS5 : Développer la collaboration nationale
- OS6 : Développer la coopération régionale et internationale

3.1. OBJECTIF STRATEGIQUE 1 : DOTER LA MAURITANIE DES INSTITUTIONS NECESSAIRES A SA SECURITE NUMERIQUE

Pour définir et mettre en œuvre la politique publique destinée à assurer la sécurité numérique dans ses diverses dimensions, la Mauritanie se dotera des institutions nécessaires :

- Une structure de gouvernance de la politique nationale de sécurité numérique : le Haut Conseil du Numérique (HCN) verra sa mission élargie pour être aussi la structure de gouvernance de la cybersécurité et de la lutte contre la cybercriminalité en Mauritanie ;
- Une structure consultative pour éclairer par ses avis les décisions de la structure de gouvernance : un sous-comité du Comité Technique d'Appui du Haut Conseil du Numérique sera spécifiquement dédié à la sécurité numérique (CTA-HCN-SCSN) ;
- Une structure de mise en œuvre de la cybersécurité : l'Agence nationale de la cybersécurité assurera le pilotage au quotidien des actions de l'État en matière de cybersécurité ; elle deviendra l'autorité nationale de cybersécurité ; elle abritera notamment un centre opérationnel, le Centre national de veille, d'alerte et de réaction aux attaques informatiques (CSIRT) ;
- Une autorité nationale de certification électronique : cette fonction, prévue par loi sur les transactions électroniques pour définir et faire appliquer la politique mauritanienne de certification, sera assurée par l'Agence nationale de la cybersécurité.

Ces institutions seront créées ou modifiées et leurs missions et attributions fixées par voie législative et réglementaire. L'opportunité de fixer ce cadre institutionnel dans une loi spécifique sur la cybersécurité sera examinée.

3.1.1. Doter la Mauritanie d'une structure de gouvernance de la sécurité numérique et de la lutte contre la cybercriminalité

La gouvernance de la politique nationale de sécurité numérique sera assurée par le Haut Conseil du Numérique (HCN) créé par le décret 2020-045/PM du 20 mars 2020, qui sera corrigé en conséquence.

Cette structure destinée à préparer les décisions du gouvernement sur toutes les questions relatives aux Technologies de l'Information et de la Communication (TIC) traitera donc désormais en particulier, sous la présidence du Premier Ministre, des deux volets complémentaires de la sécurité numérique : la cybersécurité et la lutte contre la cybercriminalité.

Une réunion par an au moins du HCN sera dédiée à la sécurité numérique. Le directeur de l'Agence nationale de la cybersécurité sera invité à y participer. Il proposera aux membres permanents l'ordre du jour des réunions, leur présentera en introduction la situation et rédigera le relevé de décisions.

Le Ministre de la Justice participera en tant que membre à toutes les réunions du HCN traitant de questions relatives à la lutte contre la cybercriminalité. Dans certaines circonstances, les réunions dédiées à la sécurité numérique pourront se tenir en comité réduit, en présence des Ministres chargés de la Transition numérique, de l'Intérieur, de la Justice et de la Défense.

3.1.2. Créer une instance consultative de la sécurité numérique

Un sous-comité du Comité Technique d'Appui du Haut Conseil du Numérique spécifiquement dédié à la sécurité numérique (CTA-HCN-SCSN) sera créé. La modification du décret 2020-045/PM du 20 mars 2020 officialisera cette création.

Présidé par le directeur de l'Agence nationale de la cybersécurité, le CTA-HCN-SCSN réunira des représentants des ministères et des membres qualifiés de la société civile ayant une bonne connaissance de la sécurité numérique. Il aura pour mission de faire des propositions pour renforcer l'efficacité du dispositif national de sécurité numérique, et plus particulièrement de cybersécurité, et d'éclairer par ses avis le HCN sur les projets du gouvernement dans ces domaines. Il se réunira au moins trois fois par an.

L'Agence nationale de la cybersécurité assurera le secrétariat du Comité consultatif.

3.1.3. Créer l'Agence nationale de la cybersécurité et le CSIRT national

Placée sous l'autorité du Premier Ministre, l'Agence nationale de la cybersécurité assurera la fonction d'autorité nationale de cybersécurité. A ce titre, elle aura pour missions de :

- Proposer au Haut Conseil du Numérique (HCN) les actions nécessaires pour renforcer le dispositif national de sécurité numérique et la cybersécurité des systèmes numériques déployés en Mauritanie ;
- Piloter et suivre la réalisation des actions décidées par le HCN en matière de cybersécurité et l'informer régulièrement de l'état d'avancement de ces actions ;
- Animer les travaux du sous-comité du Comité Technique d'Appui du Haut Conseil du Numérique spécifiquement dédié à la sécurité numérique, et les restituer au HCN ;
- Animer et coordonner les travaux interministériels en matière de cybersécurité ;
- Élaborer et proposer les mesures de cybersécurité, diffuser les mesures adoptées et veiller à leur application ;
- Conseiller et assister les services de l'État et les opérateurs d'infrastructures critiques pour la sécurisation de leurs systèmes numériques sensibles ;
- Apporter son concours aux organismes de l'État chargés du développement des services numériques et de la protection des données à caractère personnel ;
- Conduire des audits de sécurité des systèmes numériques, notamment dans les services de l'État et chez les opérateurs d'infrastructures critiques ;
- Coordonner les actions de sensibilisation et de formation en matière de sécurité numérique ;
- Promouvoir le développement d'un écosystème de cybersécurité en Mauritanie ;
- Mener et soutenir les activités de recherche dans le domaine de la cybersécurité ;
- Qualifier les produits de cybersécurité et les prestataires de service de cybersécurité ;
- Entretenir des liens avec ses homologues régionaux et internationaux dans le domaine opérationnel et pour le développement des capacités ;
- Conseiller les autorités gouvernementales en cas de crise liée à la cybersécurité.

L'Agence nationale de la cybersécurité assurera la création en son sein et la montée en puissance d'un centre national d'alerte et de réaction aux attaques informatiques (CSIRT national), chargé, sous son autorité, de :

- Assurer une veille sur les risques et menaces liées aux attaques informatiques ou aux vulnérabilités logicielles qui pourraient affecter les systèmes numériques et les réseaux nationaux ;
- Diffuser les alertes correspondantes et les recommandations nécessaires pour parer ces risques et menaces ;
- Assister les organismes prioritaires affectés par un incident de sécurité pour identifier l'origine de l'incident et restaurer la sécurité des systèmes compromis.

Par ailleurs, elle pourra, sur réquisition, assister les autorités judiciaires avec ses capacités d'analyse numérique.

Elle disposera d'un site Internet sécurisé destiné à informer le public sur la réglementation, les mesures et bonnes pratiques de sécurité numérique, les risques et menaces et ses recommandations. Le CSIRT national disposera également d'un site Internet sécurisé destiné à diffuser sans délai et le plus largement possible ses alertes de sécurité et ses recommandations, et à recueillir les signalement d'incidents de sécurité.

Une équipe de projet sera constituée sans délai au sein du Ministère de la Transition Numérique, de l'Innovation et de la Modernisation de l'Administration (MTNIMA) pour préparer la mise en œuvre de la présente Stratégie et notamment la création de l'Agence nationale de la cybersécurité dans tous les aspects (définition précise de sa mission, de ses attributions, de son rattachement et de son organisation, besoin en ressources humaines, formations, équipements, locaux et financement, rédaction des textes législatifs et réglementaires nécessaires et du plan de montée en puissance, etc.). L'objectif est de disposer dès l'année 2022 d'une préfiguration de l'Agence, installée au sein du MTNIMA jusqu'au moment où l'Agence pourra être officiellement créée.

3.1.4. Promouvoir la création de CSIRT sectoriels

Un CSIRT national n'a jamais la possibilité de faire bénéficier de tous ses services l'ensemble des organisations utilisant des systèmes numériques d'un pays. Son action doit donc être complétée par des CSIRT sectoriels, chargés d'assurer les missions de veille, d'alerte et de réponse à incident pour un ensemble d'organisations utilisant des systèmes numériques similaires. Ces CSIRT sectoriels seront coordonnés par le CSIRT national et agiront en complémentarité avec lui et avec la meilleure subsidiarité possible, afin d'éviter les duplications d'effort : veille et alerte sur les vulnérabilités des logiciels spécifiques de leur « audience » et les techniques d'attaques propres à ces logiciels, élaboration des recommandations spécifiques, assistance de leur « audience » en cas d'incident informatique.

Il conviendra donc de promouvoir la création de CSIRT sectoriels dans les secteurs les plus sensibles. Toutefois, compte tenu de la faible ressource disponible en experts, la priorité sera donnée à la constitution et à la montée en puissance du CSIRT national. La période de mise en œuvre de la présente Stratégie sera mise à profit pour préparer la constitution de CSIRT sectoriels.

Durant la période de la présente Stratégie au moins, le CSIRT national assurera également le rôle de CSIRT sectoriel pour les services de l'État. L'expérience ainsi acquise permettra de juger de la nécessité de créer ensuite un CSIRT gouvernemental.

3.1.5. Créer une Autorité nationale de certification électronique

Les certificats électroniques constituent un outil très important pour sécuriser les usages numériques. Ils permettent de signer électroniquement les documents transmis, garantissant ainsi leur intégrité, d'authentifier une personne physique ou un serveur, interdisant ainsi l'usurpation d'identité, et d'assurer le

chiffrement des échanges, assurant ainsi leur confidentialité. La génération, la distribution et l'usage des certificats électroniques doivent cependant respecter un certain nombre de règles de sécurité pour garantir leur fiabilité.

C'est ce constat qui a conduit la Mauritanie à adopter des dispositions législatives sur la certification électronique dans la loi n° 2018-022 du 12 juin 2018 portant sur les transactions électroniques. Cette loi régit notamment la signature électronique et les conditions pour qu'elle soit considérée comme sécurisée (articles 82 à 87), les certificats électroniques (articles 88 à 91) et les conditions de qualification des prestataires de certification électronique (articles 92 à 101).

La loi n° 2018-022 prévoit divers textes réglementaires d'application , en particulier pour créer une Autorité de certification chargée de définir et de faire appliquer la politique mauritanienne de certification (article 90). Ces textes n'ont pas encore publiés, malgré le travail important déjà réalisé pour les préparer. Leur publication, ainsi que la constitution effective de l'autorité nationale de certification et son opérationnalisation, constituent une priorité de la présente stratégie.

La fonction d'Autorité nationale de certification électronique sera assurée par l'Agence nationale de la cybersécurité. Son objectif prioritaire sera de développer le plus rapidement possible l'usage des certificats électroniques en Mauritanie.

Dans un horizon plus lointain, il sera envisagé de mettre en œuvre une infrastructure à clés publiques (IGC/PKI) nationale assurant la génération d'un certificat racine de l'État mauritanien.

3.2. OBJECTIF STRATEGIQUE 2 : RENFORCER LA SECURITE DU CYBERESPACE MAURITANIEN ET DES INFRASTRUCTURES CRITIQUES

Le renforcement de la cybersécurité des systèmes numériques et des réseaux déployés en Mauritanie nécessite la mise en œuvre de mesures de sécurité aussi nombreuses que diverses, de nature notamment technique, opérationnelle ou organisationnelle. Une étude juridique identifiera les mesures qui doivent être prévues ou inscrites dans des textes législatifs ou réglementaires pour pouvoir être rendues d'application obligatoire. Les textes rendant une mesure obligatoire prévoiront un délai raisonnable pour son application.

Tout organisme comme tout particulier qui met en œuvre des systèmes numériques doit parfaitement respecter un socle minimal de cybersécurité, constitué des règles dites d'hygiène informatique.

Ce socle minimal ne saurait cependant suffire à assurer la sécurité des systèmes numériques. Des mesures complémentaires adaptés à chaque type de système sont nécessaires. Ces mesures doivent être proportionnées aux enjeux de sécurité de chaque organisme et, au sein de chaque organisme, de chaque système numérique qu'il met en œuvre. Il s'agit de trouver le juste équilibre entre le l'impact humain, financier et fonctionnel de ces mesures et celui que pourrait provoquer une disfonctionnement grave lié à un défaut de cybersécurité, tout en ayant conscience que ce dernier impact peut souvent être bien plus coûteux que les investissements à consentir pour l'éviter. Tout projet de mise en place d'un système numérique nouveau ou de renforcement de la cybersécurité d'un système ancien doit donc être précédé d'une analyse de risque.

Les conclusions de l'analyse de risque et les mesures de cybersécurité qui en découlent doivent être approuvées par la direction de l'organisme concerné, et dans certains cas, qui seront précisés par un texte officiel, validées par l'Agence nationale de la cybersécurité.

L'ensemble de ces démarches s'imposera tout particulièrement aux organismes de l'État, dont les services sont essentiels à la sécurité nationale, à l'ordre public et aux citoyens, et qui se doivent d'être exemplaires dans ce domaine également, et aux infrastructures publiques et privées du pays qui présentent un caractère

critique soit pour les services essentiels qu'elles assurent au profit de la Nation et de la population, soit en raison de leur caractère dangereux.

Cet objectif stratégique nécessite de mettre en place un cadre législatif et réglementaire permettant d'identifier et de désigner les infrastructures critiques, et d'imposer des mesures renforcées de sécurité numérique aux services de l'État et à ces infrastructures critiques.

Les autres organismes ne seront, dans un premier temps au moins, qu'incités à respecter aussi strictement que possible les mesures ainsi définies.

L'Agence nationale de la cybersécurité aura la responsabilité d'établir et de diffuser les mesures de sécurité numérique applicables en Mauritanie. Elle s'inspirera pour cela des règles et bonnes pratiques de cybersécurité internationalement reconnues.

Tous les documents établis dans ce cadre seront diffusés sur Internet aussi largement que leur confidentialité le permettra afin, outre de servir les organismes qui auront l'obligation de les appliquer, de permettre aux autres organismes de s'en inspirer. Cette diffusion permettra aussi de contribuer à la sensibilisation et à la formation de tous les utilisateurs, et de disposer de supports facilement accessibles pour les campagnes de formation et de sensibilisation qui seront menées dans le pays.

3.2.1. Élaborer, diffuser et faire appliquer les règles de cybersécurité

L'Agence nationale de la cybersécurité sera chargée d'élaborer, diffuser et faire appliquer les règles de cybersécurité destinées à gérer les risques et menaces pesant sur les systèmes numériques, à éviter les incidents de nature à porter atteinte à ces systèmes, et en cas d'incident, à en minimiser l'impact et à restaurer la sécurité sans détruire les preuves qui permettront d'en comprendre l'origine.

Elle établira tout d'abord les règles d'hygiène informatique constituant le socle minimal de cybersécurité ainsi que toute autre recommandation pertinente à respecter par tous les utilisateurs ou administrateurs de systèmes numériques.

Elle rédigera également en priorité un guide méthodologique de mise en œuvre des démarches d'analyse de risque.

Les autres règles générales seront regroupées dans un Référentiel général de sécurité des systèmes d'information (RGSSI). Avant son adoption, le RGSSI sera présenté pour avis au Comité Technique d'Appui dédié à la sécurité numérique.

Les règles de cybersécurité spécifiques à certains secteurs d'activité seront établies en liaison avec les ministères chargés de la tutelle de ces secteurs.

Enfin, l'Agence nationale de la cybersécurité établira un document fixant les exigences minimales des audits de cybersécurité qui seront réalisés par ses services ou par des prestataires de service de cybersécurité.

3.2.2. Renforcer la cybersécurité des services de l'État

Les systèmes numériques des services de l'État sont essentiels à l'action publique et il convient d'en assurer la sécurité au meilleur niveau possible. Dans ce but, l'Agence nationale de la cybersécurité définira les mesures à appliquer par les ministères, établissements publics, services déconcentrés et autorités administratives indépendantes, tant dans leurs projets informatiques que pour les systèmes en place.

Ces mesures comprendront au minimum les obligations suivantes :

- Désigner dans chaque ministère un responsable de haut niveau, appelé Fonctionnaire de la sécurité des systèmes d'information (FSSI), chargé d'assurer la liaison du ministère avec l'Agence nationale de la cybersécurité et de coordonner toutes les questions de cybersécurité intéressant le ministère et les organismes et secteurs placés sous sa tutelle ;
- Créer dans chaque service de l'État, au sein de la direction informatique et éventuellement dans les autres structures traitant de numérique, la fonction de responsable de la sécurité des systèmes d'information (RSSI), assurée à temps partiel ou à temps complet suivant la taille et les enjeux de cybersécurité de l'organisme, pour veiller au quotidien à la sécurité des systèmes numériques en appliquant notamment les mesures techniques de cybersécurité prescrites par l'Agence nationale de la cybersécurité. Le RSSI ministériel sera le correspondant désigné du CSIRT national, avec lequel il se tiendra en liaison régulière ;
- Déclarer rapidement à l'Agence nationale de la cybersécurité tout incident de sécurité ayant affecté un système numérique sensible.

Les mesures techniques, opérationnelles et organisationnelles seront regroupées dans une Politique de sécurité des systèmes d'information de l'État (PSSIE), fixant les principes de cybersécurité à respecter, notamment en matière de gouvernance, d'organisation, de gestion des risques, d'acquisition de nouveaux systèmes, de maintien en condition de sécurité des systèmes en service, de charte pour les utilisateurs, et de gestion des incidents. La PSSIE pourra s'appuyer sur le RGSSI sans en reprendre le détail.

Les grands services de l'État établiront chacun une Politique de sécurité des systèmes d'information (PSSI) fixant les dispositions qu'ils prennent pour respecter les principes fixés par la PSSIE. La PSSI fera partie des documents à analyser lors des audits de cybersécurité des organismes.

L'Agence nationale de la cybersécurité établira une PSSI générique fixant la structure exigée pour les PSSI et fournissant un guide de rédaction.

Par ailleurs, les modalités de définition et de gouvernance des grands projets technologiques de l'État seront revues pour garantir la prise en compte de la cybersécurité dans leurs objectifs et dans leur réalisation.

Enfin, il sera créé, au sein de l'équipe d'administration de chaque réseau numérique de l'État, la fonction de SOC (*Security Operations center*), chargée d'assurer en temps réel la gestion de la sécurité du réseau.

3.2.3. Garantir la cybersécurité et la résilience des infrastructures critiques

De nombreux services matériels ou immatériels fournis par des opérateurs publics ou privés sont essentiels pour la Mauritanie, en particulier pour le fonctionnement de l'État, pour l'économie et pour la santé, la sûreté, la sécurité et le bien-être de la population. Ces services reposent eux-mêmes sur un ensemble d'infrastructures, physiques ou numériques, ainsi que sur les données nécessaires à leur fonctionnement. D'autres infrastructures, comme des barrages ou des usines chimiques par exemple, peuvent présenter un grand danger pour la population en cas d'action malveillante ou de dysfonctionnement grave.

Une démarche particulière doit garantir la sécurité et la résilience de ces diverses infrastructures, appelées infrastructures critiques nationales. L'Agence nationale de la cybersécurité aura la responsabilité d'organiser et de veiller à la cybersécurité de ces infrastructures critiques.

Une première action consistera à identifier les infrastructures critiques nationales (ICN) et leurs opérateurs, en appliquant une méthodologie interministérielle qui sera élaborée. Chaque ministère proposera la liste des infrastructures critiques des secteurs d'activité placés sous sa tutelle à une Commission des infrastructures critiques nationales (CICN) chargée d'assurer la cohérence interministérielle de cette démarche. L'Agence

nationale de la cybersécurité pourra également proposer de désigner des ICN après consultation des ministères de tutelle. Les ICN seront alors désignés par décision administrative non publiée. La liste des ICN sera tenue secrète. La procédure prévoira que les opérateurs pressentis pour être ICN puissent adresser leurs observations avant la décision de la CICN.

L'Agence nationale de la cybersécurité élaborera ensuite, en liaison avec chaque opérateur et son autorité de tutelle, les mesures à respecter pour garantir la sécurité et la résilience des systèmes numériques dont le dysfonctionnement, accidentel ou à la suite d'attaques informatiques, pourrait faire courir un risque grave pour le fonctionnement de l'État, pour l'économie et pour la santé, la sûreté, la sécurité et le bien-être de la population.

Les opérateurs d'infrastructures critiques nationales auront notamment l'obligation de :

- désigner au sein de leur direction une autorité chargée d'organiser et de veiller à la protection de leurs installations, et qui sera le point de contact permanent des autorités publiques dans ce domaine ;
- respecter les mesures de protection qui leur seront imposées pour renforcer la sécurité physique et la cybersécurité de leurs installations ;
- rédiger une Politique de sécurité des systèmes d'information décrivant les enjeux et risques de cybersécurité de l'infrastructure ainsi que l'organisation et les mesures de sécurité prises pour y faire face ;
- créer la fonction de responsable de la sécurité des systèmes d'information (RSSI), assurée à temps partiel ou à temps complet suivant la taille et les enjeux de cybersécurité de l'organisme, pour veiller au quotidien à la sécurité des systèmes numériques de l'opérateur en appliquant notamment les mesures techniques de cybersécurité prescrites par l'État ou par la direction de l'organisme ;
- déclarer rapidement tout incident pouvant avoir un impact grave aux autorités de tutelle et à l'Agence nationale de la cybersécurité en cas d'incident de sécurité ayant affecté un système numérique sensible ;
- collaborer franchement et sans réserve avec les autorités en cas de nécessité.

Ces dispositions seront établies par des actes législatifs et réglementaires constituant le cadre juridique de protection des infrastructures critiques nationales.

3.3. OBJECTIF STRATEGIQUE 3 : RENFORCER LE DISPOSITIF NATIONAL DE LUTTE CONTRE LA CYBERCRIMINALITE

La cybercriminalité est un fléau mondial qui ne cesse de s'aggraver dans nos sociétés de plus en plus numérisées et interconnectées.

Des attaques informatiques de plus en plus nombreuses et sophistiquées mettent en danger les systèmes et échanges numériques qui se développent dans tous les secteurs d'activité pour améliorer la qualité et l'efficacité des services publics et des entreprises, l'économie, l'éducation, la santé et le bien-être des citoyens. Les auteurs de ces cyberattaques bénéficient actuellement le plus souvent d'une impunité totale, en raison de la difficulté technique de les identifier formellement, notamment quand ils ont agi depuis des pays étrangers, parfois situés à l'autre bout du monde.

Par ailleurs, l'extraordinaire capacité apportée par les outils numériques pour échanger et diffuser des informations en temps réel vers de très larges audiences, est de plus en plus exploitée pour mener des actions illégales, souvent en profitant de la dissimulation d'identité que permet Internet : arnaques, chantages, appels à la haine et à la violence, production et diffusion de pornographie enfantine, etc. La Mauritanie, de plus en plus connectée sur son territoire comme avec le reste du monde, n'échappe hélas pas à cette montée de la cybercriminalité.

Cette situation impose que chaque pays recherche et réprime les actions de cybercriminalité conduites sur ou depuis son sol. En outre, en raison de l'absence de frontières dans le cyberespace, elle impose également une coopération régionale et internationale étroite pour sécuriser le cyberespace mondial en luttant ensemble contre la cybercriminalité.

La Mauritanie s'est déjà dotée d'un cadre législatif pour réprimer la cybercriminalité, avec la loi 2016-007 du 20 janvier 2016, et de quelques capacités techniques et humaines. Elle a toutefois la volonté de lutter de manière plus résolue encore contre la cybercriminalité.

3.3.1. Renforcer le cadre institutionnel de la lutte contre la cybercriminalité

Dans le domaine de la lutte contre la cybercriminalité, la recherche du renseignement, les investigations et le traitement judiciaire constituent un charge croissante qui excède toujours les capacités des ressources disponibles.

Il conviendra donc de renforcer ces capacités tout en recherchant la plus grande synergie entre les divers services de police et de gendarmerie qui y concourent. Une étude sera conduite dans ce but. Elle envisagera notamment la constitution d'un office central spécialisé regroupant des forces de différents ministères. Les missions et attributions des institutions chargées de la lutte contre la cybercriminalité seront alors précisées par voie législative ou réglementaire.

3.3.2. Renforcer les capacités opérationnelles de lutte contre la cybercriminalité

Un effort sera fait pour dispenser une formation de haut niveau aux magistrats et aux enquêteurs impliqués dans la lutte contre la cybercriminalité

Les capacités d'investigation seront renforcées, notamment par le recrutement de nouveaux experts et par la création d'un laboratoire central d'investigation numérique.

3.3.3. Adhérer aux Conventions internationales relatives à la cybercriminalité

L'adhésion aux Conventions internationales relatives à la cybercriminalité sera recherchée, tant pour concourir à la lutte internationale contre la cybercriminalité que pour faciliter les investigations et le traitement judiciaire des crimes et délits commis depuis l'étranger à l'encontre de la Mauritanie.

3.3.4. Mettre la législation pénale et de procédure pénale au niveau des standards internationaux

La législation pénale et de procédure pénale sera mise autant que nécessaire au niveau des standards internationaux pour renforcer la capacité de la Mauritanie à identifier les auteurs, sanctionner ceux qui opèrent sur son sol et mettre en œuvre la coopération judiciaire internationale.

3.3.5. Renforcer la valeur probante des preuves électroniques

Les preuves électroniques sont de plus indispensables dans les investigations et le traitement judicaire des crimes et délits de toute nature. Les évolutions législatives prévues pour la lutte contre la cybercriminalité seront mises à profit pour apporter les améliorations juridiques qui apparaitraient nécessaires pour renforcer la valeur probante des preuves électroniques devant les tribunaux.

3.4. OBJECTIF STRATEGIQUE 4 : DEVELOPPER LA SENSIBILISATION ET LES COMPETENCES

3.4.1. Conduire des campagnes de sensibilisation et de responsabilisation

La sécurisation du cyberespace mauritanien est d'abord une responsabilité de l'État, et c'est à ce titre que l'État mauritanien affirme sa volonté et prévoit de nombreuses actions dans la présente Stratégie nationale de sécurité numérique. La sécurité numérique ne pourra cependant s'améliorer significativement que si chaque personne physique ou morale mettant en œuvre des systèmes numériques, chaque décideur, chaque usager, chaque administrateur informatique n'a pas une conscience suffisante des risques, des enjeux et de sa propre responsabilité, et la connaissance des règles d'hygiène et bonnes pratiques qu'il doit respecter pour limiter les risques sur ses propres installations.

Dans ce but, des campagnes de sensibilisation et de responsabilisation seront lancées au profit des différents publics concernés, notamment la population, les décideurs, les agents publics et les opérateurs privés. L'utilisation de toutes les formes possibles sera recherchée : interventions dans les écoles, les universités, les services de l'État et les entreprises, messages sur les réseaux sociaux, à la radio et à la télévision, ateliers réunissant les décideurs, etc.

Ces campagnes s'appuieront sur les guides et outils de sensibilisation qui seront élaborés par l'Agence nationale de la cybersécurité. Dans la mesure du possible, cette Agence nouera des partenariats avec les organismes publics, privés ou associatifs pouvant relayer ses messages et assurera la formation des intervenants.

3.4.2. Favoriser le développement d'un écosystème national de cybersécurité

Compte tenu de la variété et de la complexité des technologies de l'information et de la communication, les actions de sensibilisation ne suffiront pas à sécuriser au niveau nécessaire les systèmes numériques des organismes publics et privés, et notamment des infrastructures critiques. Des entreprises spécialisées sont nécessaires pour installer des systèmes sécurisés dès leur conception, renforcer la cybersécurité des systèmes anciens, conduire des audits, et assister les victimes d'incidents de sécurité pour restaurer les systèmes compromis.

Dans ce but, l'État favorisera l'éclosion et le renforcement d'entreprises spécialisées efficaces et viables économiquement. Cet écosystème national de cybersécurité profitera d'une demande croissante avec la prise de conscience des décideurs publics et privés et les mesures de cybersécurité qui leur seront imposées. Il permettra également de générer des emplois à forte valeur ajouté.

3.4.3. Créer des cursus de formation à la cybersécurité

Enfin, pour répondre aux immenses besoins en compétences pour conduire l'ensemble des actions prévues dans la présente Stratégie, des formations seront créées, tant dans les universités que dans les écoles publiques ou privées de formation professionnelle ou dans le cadre de la formation permanente, pour disposer d'un nombre croissant d'ingénieurs et de techniciens experts en cybersécurité.

Des modules dédiés à la cybersécurité seront par ailleurs intégrés dans les formations en informatique afin que les concepteurs, les installateurs et les administrateurs de systèmes numériques ne créent pas de vulnérabilités dans leurs tâches quotidiennes et sachent réagir en cas d'incident de sécurité.

Des stages courts pourront être organisés pour donner une première compétence aux FSSI, aux RSSI et aux administrateurs de la sécurité des systèmes numérique en attendant de disposer du nombre suffisant d'experts parfaitement formés.

Une priorité sera donnée à la formation de formateurs, en Mauritanie ou à l'étranger, afin que notre pays puisse peu à peu satisfaire ses besoins de manière autonome, voire exporter son savoir-faire.

L'Agence nationale de la cybersécurité coordonnera les diverses démarches conduites dans le domaine de la formation. Elle fixera le contenu des formations et fournira autant que possible des supports de cours. Elle nouera des partenariats avec les organismes de formation ou avec leurs autorités de tutelle pour atteindre aussi vite que possible les objectifs fixés.

La recherche sera également favorisée par l'inscription de thématiques de cybersécurité dans le plan de travail des organismes de recherche.

3.5. OBJECTIF STRATEGIQUE 5 : RENFORCER LA COLLABORATION NATIONALE

Les actions prévues dans les objectifs stratégiques précédents ne permettront réellement d'instaurer un cyberespace mauritanien de confiance que si une collaboration étroite s'établit entre toutes les parties prenantes, notamment entre les autorités et institutions chargées de la cybersécurité et :

- les autorités et institutions chargées de la lutte contre la cybercriminalité ;
- les opérateurs des infrastructures critiques nationales ;
- les fournisseurs de produits de cybersécurité ou sécurisés ;
- les prestataires de services de cybersécurité ;
- les institutions de formation et de recherche ;
- les organisations privées ou associatives de la société de l'information ;
- les médias et autres relais des messages de sécurité numérique.

L'Agence nationale de la cybersécurité favorisera par ailleurs la création de cercles permettant aux personnes ayant des responsabilités similaires en cybersécurité de partager leur expérience et à l'Agence de capitaliser sur cette expérience : FSSI, RSSI, opérateurs d'infrastructure critique nationale, opérateurs de télécommunication, fournisseurs d'accès à Internet, .

Les ministères chargés de l'Intérieur et de la Justice réuniront au moins une fois par an des magistrats et des enquêteurs pour permettre à chacune de ces deux populations de partager leur expérience, et aux deux de comprendre les contraintes et attentes de l'autre et d'améliorer ainsi leur collaboration.

3.6. OBJECTIF STRATEGIQUE 6 : DEVELOPPER LA COOPERATION REGIONALE ET INTERNATIONALE

La coopération régionale et internationale sera développée dans toutes ses dimensions possibles par les diverses autorités ayant des responsabilités dans la sécurité numérique, et en particulier :

- Dans le domaine du développement des capacités :
  Cette coopération visera à développer les capacités de la Mauritanie en matière de cybersécurité et de lutte contre la cybercriminalité tout en économisant les efforts. Ainsi seront recherchés le partage de bonnes pratiques, de règles et procédures, ainsi que les synergies et mutualisations possibles, notamment en matière de formation.

- Dans le domaine institutionnel :

L'objectif sera d'harmoniser les stratégies, les organisations et les procédures, notamment pour assurer la sécurité des infrastructures critiques transnationales.

- Dans le domaine opérationnel :
  Cette coopération, essentiellement conduite par l'Agence nationale de la cybersécurité et le CSIRT national, visera à partager avec leurs homologues étrangers les évaluations de la menace, les alertes, les recommandations et d'autres informations de cybersécurité. Les liens ainsi noués faciliteront la coordination, entre les pays concernés, de la réponse à apporter en cas de cyberattaque touchant plusieurs pays, notamment si elles affectent des infrastructures critiques transnationales.

- Dans le domaine judiciaire :
  La Mauritanie s'inscrira pleinement dans la démarche d'entraide judiciaire internationale, en conformité avec les engagements pris par la Mauritanie dans les Conventions, Traités et Accords dont elle est partie, dans un double but :
    - Dénier aux cybercriminels l'impunité actuelle dont ils bénéficient en agissant depuis un pays vers un autre, en collaborant avec les services de police et de justice étrangers, notamment dans le cadre de coopération internationale contre la cybercriminalité que constitue la Convention de Budapest ;
    - Participer à la lutte contre toutes les formes de criminalité transnationale, en développant chaque fois que possible l'accès transnational aux preuves numériques.

4. LA MISE EN ŒUVRE DE LA STRATEGIE NATIONALE ET SES MODALITES DE SUIVI ET DE MISE A JOUR

La présente Stratégie nationale fixe les actions qui devront menées d'ici 2025 pour atteindre les objectifs stratégiques les plus importants et les plus urgents.

Le plan d'action joint en appendice I récapitule les actions à conduire, en indiquant pour chacune sa priorité (de P1, la plus élevée, à P3), l'organisme responsable de son pilotage, les autres organismes devant contribuer à sa réalisation, son échéance, l'évaluation de l'éventuel budget nécessaire et des indicateurs de performance.

Sous la gouvernance du Haut Conseil du Numérique (HCN), l'Agence nationale de la cybersécurité, ou en attendant sa création, l'équipe de projet puis la préfiguration qui seront constituées au sein du MTNIMA, assurera le pilotage et la coordination de la mise en œuvre de cette stratégie, en liaison étroite avec les ministères chargés de l'Intérieur et de la Justice pour ce qui concerne la lutte contre la cybercriminalité.

Sous la coordination de l'Agence nationale de la cybersécurité, les organismes désignés pour assurer le pilotage d'une des actions prévues dans le plan d'action rédigeront, avant mi-2022 pour les actions de priorité 1 et avant fin 2022 pour les autres, une note de cadrage de chaque action de leur ressort, qui précisera les conditions qu'ils proposent pour la réalisation ainsi que leurs besoins en matière de ressources humaines, de formation, de budget et de dispositions légales. Ces notes de cadrage seront analysées par le sous-comité du Comité Technique d'Appui du Haut Conseil du Numérique dédié à la sécurité numérique (CTA-HCN- SCSN) puis corrigées et complétées si nécessaire par les pilotes d'action. Une synthèse et les éventuels besoins d'arbitrage seront soumis au HCN avant fin 2022.

Par la suite, pour chaque action, une note d'avancement sera rédigée chaque année par les pilotes d'action pour présenter les objectifs atteints, les éventuelles difficultés rencontrées et les prévisions de réalisation de

l’année suivante. Après étude de ces notes d’avancement par le CTA-HCN- SCSN, une synthèse sera transmise au HCN à titre de compte rendu et pour provoquer les éventuelles décisions nécessaires.

Une mise à jour de la présente Stratégie sera initiée dès le début de l’année 2024, en s’appuyant sur l’état d’avancement et les difficultés mis en évidence par la démarche de suivi décrite ci-dessus. L’objectif sera de publier fin 2024 une nouvelle Stratégie pour la période 2025-2028.

APPENDICE I :

PLAN D'ACTION 2022-2025

N°	Objectifs stratégiques et actions	Priorité	Responsable	Autres participants	Échéance	Budget (Millions de MRU)	Indicateurs de performance
A0.1	Créer une équipe de projet au sein du MTNIMA pour préparer la mise en œuvre de la Stratégie nationale de sécurité numérique	P1	MTNIMA	HCN/CTA-HCN	Janvier 2022	1	Équipe projet créée
A0.2	Rédiger des notes de cadrage pour toutes les actions P1 de la Stratégie nationale de sécurité numérique en vue de les soumettre au Haut Conseil du Numérique	P1	Équipe de projet MTNIMA		Mars 2022	1	Notes initiales rédigées pour toutes les actions en P1
OS1	DOTER LA MAURITANIE DES INSTITUTIONS NÉCESSAIRES						
A1.1	Confier au Haut Conseil du Numérique (HCN) la responsabilité de la gouvernance de la politique nationale de sécurité numérique	P1	MTNIMA	HCN/CTA-HCN	Mars 2022		Décret du HCN modifié et adopté
A1.2	Créer le Sous-Comité du Comité Technique d'Appui du Haut Conseil du Numérique dédié à la sécurité numérique (CTA-HCN-SCSN)	P1	MTNIMA	HCN/CTA-HCN	Mars 2022		CTA-HCN-SCSN créé
A1.3	Créer une préfiguration de l'Agence nationale de la cybersécurité au sein du MTNIMA	P1	MTNIMA	HCN/CTA-HCN	Mars 2022	2	Préfiguration créée
A1.4	Créer et opérationnaliser l'Agence nationale de la cybersécurité	P1	HCN/CTA-HCN	MTNIMA	Décembre 2022	10	Agence créée et opérationnelle
A1.5	Créer et opérationnaliser le CSIRT national au sein de l'Agence nationale de la cybersécurité	P1	HCN/CTA-HCN	MTNIMA	Juin 2023	10	CSIRT national créé
A1.6	Promouvoir la création de CSIRT sectoriels	P3	MTNIMA	Agence CS	2025	3	Étude d'opportunité réalisée et validée

N°	Objectifs stratégiques et actions	Priorité	Responsable	Autres participants	Échéance	Budget (Millions de MRU)	Indicateurs de performance
A1.7	Confier à l'Agence nationale de la cybersécurité la responsabilité d'Autorité nationale de certification électronique	P2	MTNIMA	Agence CS	Décembre 2023	6	Décrets promulgués
A1.8	Étudier l'opportunité de rédiger une loi spécifique sur la cybersécurité	P1	HCN	MTNIMA	Décembre 2022	1	Étude d'opportunité réalisée et validée
OS2	RENFORCER LA SÉCURITÉ DU CYBERESPACE MAURITANIEN ET DES INFRASTRUCTURES CRITIQUES						
A2.1	Élaborer et diffuser un guide d'hygiène informatique et des recommandations pour les usagers et pour les responsables informatiques	P1	Agence CS		2022	2	Première version diffusée
A2.2	Élaborer et diffuser un guide méthodologique sur les démarches d'analyse de risque	P1	Agence CS		2022	1	Première version diffusée
A2.3	Établir un Référentiel général de sécurité des systèmes d'information (RGSSI)	P1	Agence CS		2022	1	Première version diffusée
A2.4	Désigner un Fonctionnaires de la sécurité des systèmes d'information dans chaque ministère et lui donner des premiers éléments de formation	P1	Ministères	Agence CS	2022	1	Un FSSI désigné et formé dans chaque ministère
A2.5	Désigner des RSSI dans les DSI de l'État et les former	P1	Ministères	Agence CS	2022	2	Un RSSI désigné et formé dans chaque DSI de l'État
A2.6	Créer et opérationnaliser des SOC dans les grands réseaux de l'État	P2	Ministères	Agence CS	2023	40	Étude de faisabilité achevée fin 2022, SOC en place dans les réseaux fin 2023
A2.7	Élaborer une Politique de sécurité des systèmes d'information de l'État (PSSIE)	P2	Agence CS		2023	1	Première version diffusée
A2.8	Établir une PSSI générique	P1	Agence CS		2022	1	Première version diffusée
A2.9	Rendre obligatoire l'établissement d'une Politique de sécurité des systèmes d'information par les services de l'État et les opérateurs d'infrastructure critique nationale (ICN)	P2	Agence CS		2023		Textes nécessaires promulgués

N°	Objectifs stratégiques et actions	Priorité	Responsable	Autres participants	Échéance	Budget (Millions de MRU)	Indicateurs de performance
A2.10	Établir un document fixant les exigences minimales des audits de cybersécurité	P2	Agence CS	MTNIMA	2023	1	Première version diffusée
A2.11	Aménager les modalités de définition et de gouvernance des grands projets technologiques de l'État pour y intégrer la cybersécurité	P1	HCN	Agence CS	2022	2	Nouvelles modalités diffusées
A2.12	Créer le cadre institutionnel et juridique de protection des ICN	P1	MTNIMA		2023	2	Commission des ICN créée Textes promulgués
A2.13	Élaborer une procédure interministérielle d'identification et de désignation des ICN	P1	MTNIMA		2023	1	Procédure interministérielle élaborée et validée
A2.14	Identifier et désigner les ICN	P1	MTNIMA	Agence CS	2023	1	Nombre d'ICN identifiées et désignées
A2.15	Établir les règles de sécurité s'imposant aux diverses ICN	P2	MTNIMA	Agence CS	2023	2	Nombre de règles de sécurité établies
A2.16	Établir les règles de cybersécurité spécifiques à certains secteurs d'activité en liaison avec les organismes chargés d'assurer la régulation et la coordination de ces secteurs	P2	Agence CS	Autorités sectorielles	2024	2	Nombre de règles de cybersécurité spécifiques établies et validées
A2.17	Développer l'usage des certificats électroniques en Mauritanie, notamment dans les services de l'État	P1	MTNIMA	Agence CS	2023	10	50% des sites de l'État en https
A2.18	Étudier les conditions de création d'une IGC /PKI nationale	P3	MTNIMA	Agence CS	2025	5	Étude réalisée et validée

OS3	RENFORCER LE DISPOSITIF NATIONAL DE LUTTE CONTRE LA CYBERCRIMINALITÉ						
A3.1	Renforcer le cadre institutionnel de la lutte contre la cybercriminalité (gouvernance, organisation, unités opérationnelles, synergies entre services, etc.)	P1	Min Intérieur	Min Justice / MTNIMA	2024	4	Nombre de textes législatifs et réglementaires établis et approuvés
A3.2	Renforcer les capacités des unités opérationnelles de lutte contre la cybercriminalité	P1	Min Intérieur		2023/2024/2025	10	Nombre de ressources formées

N°	Objectifs stratégiques et actions	Priorité	Responsable	Autres participants	Échéance	Budget (Millions de MRU)	Indicateurs de performance
A3.3	Créer un laboratoire central d'investigation numérique	P1	Min Intérieur	Agence CS	2024	15	Laboratoire créé et opérationnel
A3.4	Mettre en œuvre un plan de formation sur la cybercriminalité et sur les preuves numériques pour les magistrats et les enquêteurs	P1	Min Justice et Intérieur	Agence CS	2023	15	Nombre de magistrats et enquêteurs formés
A3.5	Adhérer aux Conventions internationales relatives à la cybercriminalité	P2	Min Affaires étrangères	Min Justice et Intérieur	2023/2024	5	Adhésion effective aux Conventions de Malabo et Budapest
A3.6	Mettre la législation pénale et de procédure pénale au niveau des standards internationaux	P2	Min Justice		2025	5	Analyse validée et textes nécessaires promulgués
A3.7	Renforcer la valeur probante des preuves électroniques	P1	Min Justice	Min Intérieur	2022	2	Dispositions législatives adoptées

OS4	DÉVELOPPER LA SENSIBILISATION ET LES COMPÉTENCES						
A4.1	Réaliser et mettre en ligne des outils pédagogiques de sensibilisation et de responsabilisation sur les risques et menaces, les bonnes pratiques de cybersécurité et les peines encourues par les cybercriminels	P1	Agence CS	Min Justice et Intérieur	2022	2	Premiers outils pédagogiques en ligne
A4.2	Conduire des campagnes de sensibilisation et de responsabilisation sur les risques et menaces, les bonnes pratiques de cybersécurité et les peines encourues par les cybercriminels	P1	Agence CS		Action permanente	5	1 campagne par an
A4.3	Favoriser le développement d'un écosystème national de cybersécurité	P2	Agence CS		Action permanente	5	Propositions faites au HCN en 2022
A4.4	Assurer la formation de formateurs en cybersécurité	P1	Agence CS	Min Enseignement supérieur	Action permanente	15	Nombre de formateurs formés
A4.5	Créer des cursus de formation à la cybersécurité (y compris RSSI)	P1	Min Enseignement supérieur	Agence CS	2023	2	Nombre de cursus créés

N°	Objectifs stratégiques et actions	Priorité	Responsable	Autres participants	Échéance	Budget (Millions de MRU)	Indicateurs de performance
A4.6	Intégrer des cours de cybersécurité dans la formation des informaticiens	P1	Min Enseignement supérieur	Agence CS	2023	5	Nombre de cours intégrés
A4.7	Créer des stages courts de formation pour les FSSI des ministères	P1	Agence CS		2023	3	Nombre de stages
A4.8	Créer des stages courts pour former les RSSI et les administrateurs de la sécurité des systèmes numérique en attendant de disposer d'experts formés en nombre suffisants	P1	Agence CS		2024	5	Nombre de stages
A4.9	Inscrire des thématiques de cybersécurité dans le plan de travail des organismes de recherche	P2	Min Recherche	Agence CS	2025	2	Nombre de thématiques inscrites
A4.10	Favoriser l'éclosion de start-up de cybersécurité	P2	Min Transformation numérique	Agence CS	Action permanente	15	Propositions faites au HCN en 2022
OS5	RENFORCER LA COLLABORATION NATIONALE						
A5.1	Créer un cadre de collaboration entre l'Agence nationale de la cybersécurité et les divers opérateurs ou institutions impliquées dans la sécurité numérique (voir le détail dans la Stratégie)	P2	Agence CS		2023	1	Cadre de collaboration mis en place
A5.2	Favoriser la création de cercles de partage d'expérience en cybersécurité	P1	Agence CS		Action permanente	2	Au moins une réunion par an
A5.3	Favoriser le partage d'expérience entre les institutions chargées de la lutte contre la cybercriminalité	P1	Min Justice et Intérieur		Action permanente	2	Au moins une réunion par an
OS6	RENFORCER LA COOPÉRATION RÉGIONALE ET INTERNATIONALE						
A6.1	Nouer des partenariats pour le développement des capacités en cybersécurité	P1	Agence CS		Action permanente	1	Nombre de partenariats noués
A6.2	Nouer des partenariats pour le développement des capacités de lutte contre la cybercriminalité	P1	Min Intérieur		Action permanente	2	Nombre de partenariats noués

N°	Objectifs stratégiques et actions	Priorité	Responsable	Autres participants	Échéance	Budget (Millions de MRU)	Indicateurs de performance
A6.3	Mettre en place un dialogue avec les pays voisins sur la cybersécurité des infrastructures critiques transnationales	P2	Agence CS		Action permanente	4	Nombre de réunions de dialogues tenues
A6.4	Mettre en place une coopération opérationnelle avec des Agences de cybersécurité et CSIRT, notamment dans la région	P1	Agence CS		Action permanente	2	Nombre de conventions mises en place
A6.5	Développer la participation de la Mauritanie à la coopération judiciaire internationale en matière de lutte contre la cybercriminalité et d'accès transnational aux preuves numériques	P2	Min Justice	Min Intérieur	Action permanente	1	Nombre de participations dans des affaires internationales

APPENDICE II :

DEFINITIONS

Technologies de l'information et de la communications (TIC) : technologies employées pour recueillir, stocker, traiter et transmettre des informations, incluant les technologies qui impliquent l'utilisation d'ordinateurs ou de tout système de communication ou de télécommunication ;

Cyberespace : le réseau interdépendant des infrastructures utilisant les technologies de l'information, comprenant notamment l'Internet, les réseaux de télécommunications, les systèmes d'information et les objets connectés ;

Système d'information : tout dispositif, isolé ou non, ou ensemble de dispositifs interconnectés assurant en tout ou partie un traitement automatisé de données en exécution d'un programme ;

Donnée numérique : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique ;

Réseaux : ensemble des moyens assurant l'alimentation d'une infrastructure en produits ou services nécessaires à son fonctionnement (communications, énergie, logistique, etc.) ;

Sécurité numérique : l'ensemble des mesures prises pour assurer la cybersécurité et la lutte contre la cybercriminalité ;

Cybersécurité : l'ensemble des mesures et des actions destinées à protéger les moyens numériques et à prévenir les dommages face aux cyber menaces. La cybersécurité vise à préserver la disponibilité et l'intégrité des réseaux et de l'infrastructure ainsi que la confidentialité des informations qui y sont contenues ;

Cybercriminalité : les activités criminelles dont les ordinateurs et systèmes informatiques constituent soit l'arme soit la cible. La cybercriminalité recouvre les délits habituels (fraude, contrefaçon et usurpation d'identité par exemple), les délits liés au contenu (distribution en ligne de matériel pédopornographique ou incitation à la haine raciale par exemple) et les délits spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service et logiciel malveillant par exemple) ;

Hygiène informatique : l'ensemble des bonnes pratiques que chaque acteur du numérique devrait respecter afin de préserver la sécurité du système d'information qu'il utilise ou pour lequel il assure une fonction d'administrateur ;

CSIRT (*Computer Security Incident Response Team*) : centre d'alerte et de réaction aux attaques informatiques. Chargé d'assister les organismes qui lui sont rattachés (son « audience ») à prévenir les risques et menaces pesant sur les systèmes d'information et à réagir en cas d'incidents de sécurité ;

Infrastructure critique : une infrastructure ou un processus public ou privé dont la destruction, l'arrêt, l'exploitation illégitime ou la perturbation pendant une période de temps définie pourrait entraîner soit des pertes de vies humaines, soit des pertes importantes pour l'économie, ou porter un préjudice considérable à la réputation de l'État ou de ses symboles de gouvernance. Dans cette définition, l'infrastructure comprend les réseaux et systèmes et les données physiques ou numériques indispensables pour fournir ce service. Cette

expression peut faire référence à un système ou processus dont le fonctionnement est critique au sein de l'organisation ;

Opérateur d'infrastructure critique : opérateur public ou privé qui opère une infrastructure critique ;

Protection des infrastructures critiques : l'ensemble des mesures et des actions destinées à protéger les infrastructures critiques de l'ensemble des risques et menaces susceptibles de provoquer l'interruption totale ou partielle des services essentiels qu'elles fournissent ;

Service essentiel : un service dont l'interruption totale ou partielle pourrait avoir un impact grave sur le fonctionnement de l'État, sur l'économie du pays ou sur la santé, la sûreté, la sécurité et le bien-être de la population, ou une combinaison d'impacts de cette nature qui, pris individuellement, ne suffiraient pas à classer essentiel le service considéré ;

Opérateur de service essentiel : opérateur public ou privé qui fournit un service essentiel ;

Protection des services essentiels : l'ensemble des mesures et des actions destinées à protéger les services essentiels de l'ensemble des risques et menaces susceptibles de provoquer leur interruption totale ou partielle.

APPENDICE III :

ACRONYMES

Agence CS	Agence nationale de la cybersécurité
CICN	Commission des infrastructures critiques nationales
CS	Cybersécurité
CSIRT	Centre d'alerte et de réaction aux attaques informatiques (en anglais : *Computer Security Incident Response Team*)
CTA-HCN-SCSN	Sous-Comité du Comité Technique d'Appui du Haut Conseil du Numérique dédié à la sécurité numérique
DGTIC	Direction générale des TIC du ministère mauritanien chargé de la transition numérique
ESCWA	The United Nations Economic and Social Commission for Western Asia
FSSI	Fonctionnaires de la sécurité des systèmes d'information
HCN	Haut Conseil du Numérique
ICN	Infrastructures critiques nationales
IGC/PKI	Infrastructure de gestion de clés (IGC) (en anglais : *Public Key Infrastructure* (PKI), infrastructure à clés publiques)
MTNIMA	Ministère de la Transition Numérique, de l'Innovation et de la Modernisation de l'Administration
OS	Objectifs stratégiques
PSSI	Politique de sécurité des systèmes d'information
PSSIE	Politique de sécurité des systèmes d'information de l'État
RGSSI	Référentiel général de sécurité des systèmes d'information
RSSI	Responsable de la sécurité des systèmes d'information
SOC	Centre opérationnel de la cybersécurité (en anglais : *Security Operations center*)
TIC	Technologies de l'Information et de la Communication