République Démocratique du Congo

présidence.cd

STRATÉGIE NATIONALE DE CYBERSÉCURITÉ

DE LA RÉPUBLIQUE DÉMOCRATIQUE DU CONGO

Rédigée par la Commission technique pour la cybersécurité (CTC)

KINSHASA-JUILLET, 2022

Pour un cyberespace de confiance, sécurisé et résilient.

République Démocratique du Congo

présidence.cd

STRATÉGIE NATIONALE DE CYBERSÉCURITÉ

DE LA RÉPUBLIQUE DÉMOCRATIQUE DU CONGO

Rédigée par la Commission technique pour la cybersécurité (CTC)

POUR UN CYBERESPACE DE CONFIANCE, SÉCURISÉ ET RÉSILIENT.

KINSHASA-JUILLET, 2022

TABLE DES MATIERES

La présente **« Stratégie nationale de cybersécurité 2022 - 2025 »** a été réalisée par les experts évoluant dans le secteur du Numérique et de la cybersécurité réunis au sein de la Commission Technique pour la Cybersécurité (CTC) mise en place par le Cabinet du Chef de l'État sous l'impulsion de **Son Excellence Monsieur le Président de la République Félix-Antoine TSHISEKEDI TSHILOMBO.**

Cette commission est présidée par le **Directeur de Cabinet du Chef de l'État**, le **Conseiller Spécial en charge de la Sécurité** et le **Conseiller Spécial en charge du Numérique** qui en assurent la coordination.

Elle est composée d'experts, de consultants et d'acteurs des nouvelles technologies, soit 32 personnes qui ont travaillé entre les mois de février et de juillet 2022.

RESUME ANALYTIQUE

Juste après son accession à la magistrature suprême, le Président de la République, Félix Antoine TSHISEKEDI TSHILOMBO s'est employé à traduire sa vision sectorielle de digitalisation de la RDC dans un document référentiel de programmation dénommé « le Plan National du Numérique » avec l'objectif avoué de faire du numérique congolais un levier d'intégration, de bonne gouvernance, de croissance économique et du progrès social.

Ce Plan National du Numérique, décliné en quatre piliers fondamentaux (Infrastructures, contenus, usages applicatifs, gouvernance – régulation) permet à l'État Congolais, tant au niveau national, provincial que local, d'aligner dans son agenda la nécessaire transformation numérique des institutions, des entreprises et des services publics, de refondre l'architecture pyramidale d'actions en privilégiant la transversalité et de se construire un écosystème gouvernemental digital afin d'atteindre ses objectifs qui sont ceux de bâtir une économie solide, prospère et résiliente à l'ère du Numérique.

C'est une révolution systémique et structurelle majeure qui va nécessiter un encadrement par des mécanismes et de dispositifs adaptés aux réalités du cyberespace. Avec l'ambition d'être le hub technologique au cœur de l'Afrique notamment par sa position géographique et ses potentielles en ressources naturelles, la République Démocratique du Congo se devait de se doter d'une stratégie nationale de cybersécurité afin de protéger ses actifs contre des menaces cyber qui gangrènent la toile mondiale.

Cette stratégie nationale de cybersécurité définit le cadre stratégique et structurel pour le développement de la confiance numérique, la protection de l'environnement cyber, la défense et la sécurité de systèmes d'information ainsi que la lutte contre la cybercriminalité.

INTRODUCTION

Le continent africain connaît actuellement une expansion fulgurante des technologies de l'information et de la communication. Cette expansion amène avec elle, une vulnérabilité des plus fortes faces aux cybermenaces.

Certains gouvernements africains ont, à l'instar d'autres nations du monde, trouvé une forte réponse à ces cybermenaces en privilégiant l'élaboration d'une stratégie de cybersécurité de manière à savoir faire à ce côté sombre des nouvelles technologies de l'information et de communication. L'absence d'une réponse appropriée s'appuyant sur une gouvernance structurelle à la taille des enjeux, sur une législation adaptée et évolutive en fonction de la mutation de la nature et de la forme des pratiques obscures, sur une collaboration synergique avec le secteur privé, un cadre de confiance entre les acteurs et de coopération à tous les niveaux, reste encore un défi immense à relever. Bien qu'ayant enregistré quelques avancées significatives jusqu'ici, la progression de la cybersécurité en Afrique reste encore faible et la cybercriminalité gagne du terrain.

Afin donc de faire face à cet éventail croissant de cybermenaces et de défis, les gouvernements africains doivent s'engager, comme beaucoup d'autres pays avant eux, dans la mise en place de stratégies de cybersécurité qui favorisent la collaboration et la confiance entre les acteurs étatiques et privés des secteurs de la sécurité face aux phénomènes en constante mutation de la cybercriminalité.

Eu égard à sa taille, deuxième pays africain en superficie entouré des 9 voisins, et à ses potentielles en ressources naturelles, **la République Démocratique du Congo,** qui vient d'amorcer sa transformation numérique, risque d'être le terrain prisé de bataille du cyberespace. La création d'un écosystème cyber-sécuritaire résilient, proactif, et adapté pour assurer la protection des citoyens, des institutions et entreprises publiques, des partenariats, de la diplomatie, des renseignements, etc. est donc essentiel.

Considérant les enjeux du côté obscur de la numérisation et de montée en flèche de la cybercriminalité et de la cyber-délinquance, afin de tirer parti de meilleures pratiques à capitaliser pour le salut numérique de notre pays qui a amorcé son train de numérisation de ses institutions et entreprises et services publics, il est impérieux de constituer et formaliser une stratégie nationale de cybersécurité.

OBJECTIFS

Objectif global

Tout en utilisant les opportunités offertes par l'évolution des nouvelles technologies, la stratégie vise entre autres à créer, réfléchir, partager dans un seul objectif : **Construire une R.D. Congo consciente, numérique et sécurisée.**

L'objectif de la stratégie nationale de cybersécurité est de prévenir les menaces et d'assurer la disponibilité, la confidentialité et l'intégrité du cyberespace de manière à donner à la République Démocratique du Congo l'assurance, la capacité et la résilience nécessaires pour s'affirmer dans un univers numérique en mutation rapide.

Objectifs spécifiques

La stratégie de cybersécurité répond à 7 objectifs :

1. Gouvernance et sécurisation des opérateurs d'infrastructures critiques
2. Protection des données et de l'information
3. Sensibilisation, développement des capacités et des compétences
4. Confiance numérique
5. Législation et réglementation
6. Gestion des risques et de crise
7. Coopération sous-régionale, régionale et internationale

1 CONTEXTE

1 CONTEXTE

Selon *Africa Cyber Security Market*, le marché de la cybersécurité en Afrique est estimé à 2,32 milliards de dollars US en 2020 contre 1,33 milliards de dollars US en 2017.

La numérisation ne cesse de se développer en Afrique et de ce fait présente non seulement des opportunités, mais aussi des risques.

Il y a encore quelques années, le mot « cybersécurité » semblait encore relever de l'imaginaire. Il était commun de penser que la sécurité de l'information ne concernait qu'un nombre très restreint de structures et d'individus. Aujourd'hui, tout le monde est touché, de près ou de loin, par ces enjeux de sécurité.

La cybersécurité est définie comme « l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace, susceptibles de compromettre **la disponibilité, l'intégrité, la confidentialité ou la traçabilité** des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles. »

Afin de minimiser les cyber-risques, il est primordial de mettre autour d'une seule table, les États, les experts et responsables de la sécurité et de la protection des données, les décideurs, les entreprises et la société civile afin d'échanger sur les réalités des environnements, sur les niveaux de risques et les mesures de mitigation pouvant être mises en place. Cela permettrait d'anticiper certaines attaques, d'éviter des failles de sécurité et de minimiser les vulnérabilités.

La cybersécurité en R.D. Congo est un véritable enjeu économique, institutionnel et sociétal.

Il est important de comprendre les enjeux que comportent l'écosystème cyber adaptés à la réalité du pays, d'apporter des éléments de réponse, de décision pour les prochaines années et ainsi influencer le futur, celui de nos enfants et de nos concitoyens.

Il faut aborder la cybersécurité selon l'angle organisationnel et réglementaire et traiter ensuite l'ensemble des disciplines aussi bien techniques, fonctionnelles qu'humaines qui en dépend, gravite autour et l'influence.

La première action est de définir collectivement les exigences sécuritaires minimales par des analyses de risques correspondant aux réalités de la R.D. Congo afin de le prévenir d'un bon nombre de cyberattaques de masse dont le pays et les entreprises peuvent être victimes.

La sécurité de l'information doit occuper la place qu'elle mérite au sein de la société, comme réel outil de gestion, de création et comme un moyen de protection du capital informationnel et économique.

Notre pays la RD Congo, qui a amorcé sa transformation numérique, en se dotant d'un plan National du Numérique, a d'importantes infrastructures critiques à protéger. Il s'agit notamment des services publics en ligne, les infrastructures nucléaires, l'intranet gouvernemental, les sites e-Gouv, le réseau électrique, les banques et assurances, les régies des eaux, etc.

Notre économie se dématérialise, nos institutions également. Plusieurs initiatives sectorielles et multisectorielles, telles qu'inscrites dans le Plan National du Numérique, sont en train d'être mises en place pour construire un espace numérique congolais propices aux échanges et transactions électroniques. Cette construction nécessite sans l'ombre d'aucun doute d'être surveillée et protégée en temps réel contre les cyberattaques qui gangrènent l'espace.

C'est dans ce contexte que la **« Stratégie Nationale de Cybersécurité** » est élaborée en vue d'assurer la gouvernance étatique numérique en République Démocratique du Congo.

2

ETAT DES LIEUX

2 ETAT DES LIEUX

Si dans certains secteurs d'activité (les banques, les télécoms), la cybersécurité est plus ou moins régulée, la grande majorité des activités, y compris les secteurs du service public, bien qu'ayant une visibilité sur le cyberespace dans certains cas, ne sont pas soumises à des règles de sécurité, même minimales.

La première étape pour protéger efficacement la République Démocratique du Congo contre les cyber-risques et les futures menaces consiste à évaluer la situation actuelle et les éventuelles menaces. Il ne s'agit pas de circonscrire avec précision les risques encourus par le pays, mais d'intégrer de manière stratégique l'importance des différentes menaces et d'anticiper leurs évolutions possibles. Outre la situation de menace, un autre facteur clé affectant le statu quo est le niveau actuel de protection de la République Démocratique du Congo contre les cyber-risques.

2.1. Cybermenaces

C'est en identifiant clairement les principales menaces pour la République Démocratique du Congo que l'on peut établir avec précision d'où viennent les cyber risques. Il convient de relever que les menaces évoluent de façon très constante. Les principaux moteurs en sont le numérique, qui rend notre société de plus en plus vulnérable face aux perturbations des systèmes d'information, ainsi que le professionnalisme dont font preuve les auteurs des attaques. Comme tout porte à croire que ces tendances vont se poursuivre, il faut s'attendre à ce que les menaces s'intensifient encore davantage en se complexifiant.

Pour analyser la situation, il est important de différencier les menaces dues à des actes illicites délibérés (telles que les cyberattaques) et les dangers dus à des événements provoqués de façon non intentionnelle (telles que les erreurs humaines et/ou pannes techniques). Ces deux catégories seront donc décrites dans des sections distinctes.

2.2. Cyberattaques

Ces dernières années, on a pu constater une forte augmentation des menaces dues aux cyberattaques. En République Démocratique du Congo, dans la sous-région et dans toute l'Afrique, des attaques réussies, aux conséquences parfois graves, ont montré que non seulement la fréquence et la complexité des cyberattaques augmentaient, mais encore que celles-ci étaient de plus en plus dirigées contre des États ou des entreprises.

Vu la diversité des cyberattaques possibles, il faut établir une distinction entre plusieurs phénomènes, en fonction du but poursuivi par les attaques, des acteurs impliqués et des cibles visées. Sur cette base, on distingue six types de cyberattaques.

1. Cybercriminalité
2. Cyber espionnage
3. Cyber terrorisme
4. Désinformation et propagande
5. Cyber conflits
6. Cyber hacktivisme

Bien que non exhaustif, l'état des lieux que nous venons de dresser ci-haut ne devra pas ignorer de prendre en compte les faits ci-dessous :

2.3. L'humain reste le maillon faible

Outre les cyberattaques ciblées et délibérées, il est également possible que des actes involontaires ou des événements liés aux conditions naturelles et techniques provoquent des dégâts touchant le cyberespace ou l'environnement physique. Ceux-ci sont dus à des erreurs humaines dans la préparation et l'utilisation de l'informatique (p. ex. utilisation inappropriée ou négligente des systèmes informatiques, mauvaises administration ou configuration, perte de supports de données, etc.) ou à des défaillances techniques dont les causes peuvent être multiples (par ex. vieillissement des infrastructures, phénomènes naturels, surcharge, défaut de conception ou entretien insuffisant).

De tels événements d'ampleur variable surviennent fréquemment et font partie du quotidien des départements informatiques des entreprises et des pouvoirs publics. En conséquence, les répercussions de ces erreurs et de ces défaillances sont généralement faciles à maîtriser. Néanmoins, l'expérience montre que derrière bon nombre de ces cybers incidents se cachent non pas des attaques ciblées, mais un enchaînement de diverses circonstances, telles qu'erreurs humaines ou pannes techniques, liées à une préparation insuffisante. Il est donc essentiel de ne pas négliger les mesures de prévention et de sensibilisation contre de tels événements lors la planification et de la mise en œuvre de la stratégie.

2.4. Risques des évolutions technologiques

Les organisations publiques et privées utilisent les nouvelles technologies notamment pour créer de nouvelles possibilités et accroître leur développement et leur efficacité. En utilisant ces technologies, elles deviennent, de facto, de plus en plus dépendantes des nouvelles technologies et sont par conséquence, de plus en plus exposées aux cybermenaces.

L'utilisation de ces nouvelles technologies permet de maintenir la compétitivité et de développer de nouvelles opportunités. Toutefois, ces évolutions technologiques (Cloud Computing, Intelligence Artificielle, Blockchain, NFTs, Internet des Objets) comportent des risques, notamment parce qu'elles contribuent à développer de nouvelles chances pour les acteurs de la cybercriminalité. Il est donc essentiel que la République Démocratique du Congo soit toujours au courant de l'évolution des technologies et soit consciente des risques associés.

3

ORIENTATION STRATEGIQUE

3 ORIENTATION STRATEGIQUE

L'orientation stratégique de la stratégie nationale de cybersécurité découle des champs d'action identifiés. La vision et les objectifs stratégiques prescrivent ce qui doit être atteint, les principes stratégiques décrivent comment procéder et la section « parties prenantes » définit à quels groupes la stratégie s'applique.

3.1 Vision et objectifs stratégiques

Du fait que les cyber risques touchent simultanément divers domaines de l'économie, de la politique et de la société, des mesures doivent être prises dans différents domaines.

La vision

Tout en utilisant les opportunités offertes par l'évolution des nouvelles technologies, la stratégie vise entre autres à créer, réfléchir, partager dans un seul objectif : **Construire une R.D. Congo consciente, numérique et sécurisée.**

Les objectifs stratégiques

Répartis en sept champs d'actions, les objectifs stratégiques répondent à de grandes gammes de politiques publiques qui s'articulent autour :

- de la sécurité nationale
- de l'anticipation
- des questions opérationnelles de détection et de réponse aux cyberattaques, ainsi que l'alerte et l'accompagnement des victimes
- du renforcement de capacités scientifiques, techniques, industrielles et humaines
- de la protection des systèmes d'information de l'État et des opérateurs économiques
- de l'adaptation du législatif
- du développement des coopérations
- des enjeux de communication et de sensibilisation

La vision ne pourra se réaliser que lors que **les sept champs d'action** auront été mis en œuvre.

GOUVERNANCE ET SÉCURISATION DES OPÉRATEURS D'INFRASTRUCTURES CRITIQUES
Une bonne organisation est un facteur clé de réussite d'un plan national pour la cybersécurité. Cette organisation passe par la mise en place d'organes institutionnels et structurels en charge de la cybersécurité. De plus, des cyberattaques à grande échelle ou ciblant des infrastructures critiques peuvent mettre en danger la sécurité de la population et de la nation. En cas d'attaques, il faut pouvoir mettre en œuvre, si nécessaire, des contremesures actives, afin d'en garantir la résilience.
PROTECTION DES DONNEES ET DE L'INFORMATION
La protection des données personnelles ou d'autres données sensibles, est une priorité lors de la mise en place d'une stratégie de gouvernance. Mais pour réellement protéger des données, il faut des règles régissant cette protection.
SENSIBILISATION, DÉVELOPPEMENT DES CAPACITÉS ET DES COMPÉTENCES
Les institutions académiques et de formation accordent à la cybersécurité l'importance qu'elle mérite, et fourniront à la société, les connaissances et compétences dont elle a besoin dans la lutte contre les cyber-risques. De même, la sensibilisation au sein de la société doit devenir culturelle.
CONSTRUCTION DE LA CONFIANCE NUMÉRIQUE
Les attaques ciblées existent. Afin de protéger la République Démocratique de Congo, il faut continuellement surveiller, analyser et répondre aux différentes alertes de failles, d'attaques et de vulnérabilités. Une vue d'ensemble des situations doit être dressée et suivie.
LEGISLATION ET REGLEMENTATION
La législation et la réglementation représentent des outils importants de protection contre les cyber-risques. La lutte contre la cybercriminalité et les menaces associées est renforcée grâce à des exigences minimales de sécurité et de protection mises en place.
GESTION DES RISQUES ET DE CRISE
Les cybers incidents peuvent être lourds de conséquence et s'aggraver au point d'exiger une gestion de crise au niveau national. Il est essentiel, pour maîtriser les crises, de brosser un tableau actuel, uniforme et complet de la situation, de définir des processus de prise de décision efficaces et d'adopter une stratégie de communication.
AMELIORATION DE LA COOPERATION SOUS-RÉGIONALE, RÉGIONALE ET INTERNATIONALE
La défense des intérêts de la politique extérieure et de la politique de sécurité de la RDC doit aussi être assurée dans le cyberespace. Le pays s'engage donc, au niveau diplomatique comme sur le plan technique et opérationnel, en vue du renforcement de la coopération internationale pour réduire les cyber-risques.

3.2 Les principes

Les principes définissent de quelle manière il convient de procéder.

- La stratégie nationale de cybersécurité s'appuie sur une approche basée sur les risques qui a pour but d'améliorer la résilience de la République Démocratique de Congo en matière de cyber risques. Cela implique l'hypothèse qu'aucune protection intégrale contre les cyber-risques n'est possible, mais que les risques peuvent être traités de manière à ce que le risque résiduel soit tolérable ou accepté. Dans une approche exhaustive, toutes les vulnérabilités pertinentes et toutes les menaces sont prises en compte. Cependant, l'approche par la maturité, sera aussi considérée afin d'améliorer certains indicateurs et donner une meilleure visibilité au niveau internationale du niveau de la cybersécurité en RDC.

- La cybersécurité concerne tous les domaines de la vie, de l'économie et de l'administration. Tous doivent agir et assumer ensemble la responsabilité de la protection de la République Démocratique de Congo contre les cyber-risques. La stratégie nationale de cybersécurité renforce cette responsabilité commune en exigeant des efforts aux acteurs ayant les compétences requises et en utilisant les structures existantes. Il en découle une mise en œuvre décentralisée, mais pilotée de façon centrale par le Conseil National de Sécurité et présentant une répartition claire des tâches et des rôles.

- La stratégie nationale de cybersécurité s'appuie sur une approche accordant un rôle central à l'État, ce qui signifie que l'État peut agir, fixer des incitations ou intervenir sur le plan réglementaire et autres de manière régalienne.

- La stratégie nationale de cybersécurité poursuit une approche coopérative. Elle renforce et coordonne au niveau national le partenariat public-privé existant.

- Au niveau international, la stratégie nationale de cybersécurité encourage la collaboration avec des partenaires régionaux et internationaux.

- La stratégie nationale de cybersécurité est mise en œuvre de manière transparente dans la mesure où cela ne porte pas atteinte à l'efficacité des mesures. Ce résultat est obtenu par le biais d'une communication active de la stratégie nationale de cybersécurité vis-à-vis de la société ainsi que des milieux économiques et politiques.

3.3 Les parties prenantes

L'État congolais s'engage à appliquer les mesures définies dans la stratégie nationale de cybersécurité en collaboration avec les institutions gouvernementales, les entreprises et la société. L'effet recherché par la stratégie nationale de cybersécurité concerne ainsi tout le territoire de la République Démocratique du Congo. La stratégie nationale de cybersécurité s'adresse aux parties prenantes suivantes :

- **L'État congolais** au travers de ses institutions régaliennes et les organismes publics : Parties prenantes essentielles de cette stratégie, leur implication est nécessaire car la cybersécurité a un aspect transverse et impliquant que toutes les forces de l'état travaillent ensemble pour la réussite de cette stratégie.

- **Les Opérateurs d'importances vitales et Infrastructures critiques.** La principale partie prenante est celle des exploitants d'infrastructures critiques. Ceux-ci garantissent la disponibilité des biens et services essentiels. C'est pour quoi leur fonctionnement est indispensable pour la population et pour les milieux économiques congolais. Leur protection requiert une priorité maximale et est le point central de toutes les mesures de la stratégie.

- **La Population :** La protection de la population est, en définitive, le but ultime de toutes les mesures de la stratégie nationale de cybersécurité. Mais elle est notamment au centre des efforts de lutte contre la cybercriminalité. Par ailleurs, la stratégie nationale de cybersécurité contribue, par une information transparente, à ce que la population bénéficie d'une gestion de l'informatique sûre, informée et fiable.

- **L'Économie nationale :** Pour l'économie, un contexte sûr et fiable constitue une base importante et un facteur de compétitivité. Les cyber-risques posent de grands défis non seulement aux infrastructures critiques, mais aussi à toutes les autres entreprises et en particulier aux PME. La stratégie nationale de cybersécurité crée des conditions aussi sûres que possible pour les entreprises congolaises et met à leur disposition un soutien ciblé pour la gestion des cyber-risques.

4

CHAMPS D'ACTIONS ET MESURES ASSOCIEES

4 CHAMPS D'ACTIONS ET MESURES ASSOCIEES

Pour construire un « cyberespace de confiance, sécurisé et résilient », la République Démocratique du Congo identifie 7 piliers stratégiques qui déclinent des objectifs généraux et spécifiques, des mesures d'applications et des reformes à amorcer ainsi que des actions à mener dans une approche transversale et complémentaire afin de redresser la question de cybersécurité et de répondre efficacement contre des risques et menaces cyber.

4.1 Gouvernance et Sécurisation des opérateurs d'infrastructures critiques

4.1.1 Enjeux

La République Démocratique du Congo est la cible d'attaques informatiques qui portent atteinte à ses intérêts fondamentaux.

Au sens de la présente stratégie, les infrastructures critiques sont définies comme l'ensemble des systèmes, actifs, installations ou réseaux qui fournissent des services essentiels au fonctionnement de l'économie et au bien-être de la population.

Les infrastructures critiques représentent la logistique vitale. Selon l'Union Internationale des Télécommunications (UIT), la faible préparation des pays africains à la transition numérique et aux menaces cyber (sabotage des infrastructures publiques, fraude digitale, espionnage et vol des stratégiques, vol de renseignement et intrusion militaire, etc.) aurait le potentiel de fragiliser les systèmes d'information et de nuire aux ambitions du continent d'être le premier marché mondial de l'économie numérique.

Lorsqu'un attaquant cible des institutions, des infrastructures critiques, des services essentiels ou encore des entreprises stratégiques ou des organismes à importance vitale (OIV), il cherche à s'installer durablement dans les systèmes d'information visés pour y voler des données confidentielles (politiques,

diplomaties, technologies, économies, etc.) ou interrompre à distance des activités à impact social ou mener une guerre cyber contre les entités ou des institutions ciblées.

La numérisation des activités et les téléservices identifiés comme solution salvatrice lors de la grande pandémie de la covid-19, s'avèrent aujourd'hui objet des cyberattaques sophistiquées. Il y a donc urgence pour se doter des moyens appropriés pour faire face à ce côté obscur du Numérique.

La République Démocratique du Congo, qui a amorcé sa transition vers une économie numérique à travers le Plan National du Numérique dont l'ambition affirmée est de devenir le hub technologique au cœur de l'Afrique à l'horizon 2025, risquerait d'être une cible potentielle privilégiée compte tenu des failles, dont certaines sont structurelles, si la mesure de la question de la Cybersécurité et des menaces cybernétiques dans la conception et modélisation stratégique des politiques publiques sectorielles n'est pas prise. Classée en 48ème position avec un score de 5.3 sur 100 et avec un actif important en infrastructures critiques ainsi que l'amorçage de plusieurs chantiers structurants notamment la construction de l'intranet gouvernemental (eGov), la mise en ligne des services publics, des installations nucléaires, le développement du réseau électrique, la digitalisation de l'économie en passant par des banques numériques et des services d'assurances en ligne, des chaînes de dépense et de recettes, etc., la République Démocratique du Congo a l'impérieuse tâche de protéger et de veiller à la disponibilité 24h/24 de ses actifs.

Ceci implique la responsabilité de mettre en place un organe de gouvernance qui, d'une part, va décliner des directives claires sur la protection et la résilience des infrastructures critiques et des services essentiels afin de garantir leur disponibilité et leur efficience pour sécuriser le cyberespace congolais, et, d'autre part, permettre de construire une économie numérique utile pour des planifications futures dans une approche cohérente, complémentaire et transversale et qui inspire confiance. Cet organe devra regrouper en son sein les compétences et fonctionnalités suivantes :

1. d'être une autorité de régulation de la cybersécurité qui définira les standards, les règles ainsi que les politiques et les procédures en matière de cybersécurité au niveau nationale et d'interface avec les autres autorités de régulations nationales. L'autorité produira également les indicateurs de performance de la cybersécurité au niveau national ;
2. d'être une entité en charge de la gestion des risques, des audits et de la conformité qui s'assurera que les standards, règles et politiques définis sont implémentés aux niveaux des organismes et des infrastructures publiques ainsi que les partenaires des organismes publics ;
3. d'être une entité en charge de la sécurité opérationnelle (CERT/SOC) qui assurera la supervision de la cybersécurité des organismes publiques, de la formation et sensibilisation à la cybersécurité, de la cyber résilience qui comprend la gestion des incidents, la gestion de crise et la continuité des activités. Elle disposera en plus d'un centre opérationnel de cybersécurité ainsi que d'un office dédié à la supervision de la cybersécurité des organismes d'importance vitale (OIV) ;
4. d'être une entité en charge de lutte contre la cybercriminalité qui sera chargée d'accompagner la justice dans l'expertise cyber pour l'établissement des faits, des délits et des crimes commis au moyen des systèmes d'informations ou des communications électroniques.

Au vu de la complexité de l'environnement et des enjeux liés au développement explosif des technologies de l'information et de la communication, cet organe sera créé par décret du Premier Ministre et relèvera directement de l'autorité du Président de la République, Chef de l'État.

4.1.2 Objectifs

Objectif Général I : Protéger et défendre les cyber intérêts fondamentaux de la République Démocratique du Congo dans le cyberespace
Objectif spécifique I.1 : Doter le pays d'un organe de gouvernance et de pilotage de la Cybersécurité
Objectif spécifique I.2 : Assurer la veille des entités publiques et des services essentiels
Objectif spécifique I.3 : Accélérer le renforcement de la sécurité des systèmes d'information des institutions officielles du pays

4.1.3 Mise en œuvre

Créer l'organe de gouvernance dénommé «Agence Nationale de Cybersécurité»

L'Agence Nationale de Cybersécurité sera l'autorité nationale de régulation en charge de Cybersécurité et de sécurité des systèmes d'information en République Démocratique du Congo. Elle va assurer la certification électronique, le suivi de la conformité aux normes et principes qui seront édictées, l'audit des systèmes d'informations de l'État et des organismes à importance vitale, l'homologation des prestataires de services de confiance, des vendeurs de produits de cybersécurité et, enfin, l'expertise en matière de cybercriminalité.
Elle collaborera de manière transversale notamment avec les Ministres ayant dans leurs attributions l'intérieur et la sécurité, la justice, la défense, les droits humains, la poste et les télécommunications, le numérique ainsi que la recherche scientifique et l'innovation technologique.

Enfin, elle guidera la politique de sécurité des systèmes d'information de l'État et orientera et coordonnera l'élaboration des futures stratégies de Cybersécurité de la RD Congo.

L'Agence Nationale de Cybersécurité aura entre autres pour missions de :

- Piloter, coordonner et suivre la mise en œuvre de la stratégie nationale de Cybersécurité ;
- Assurer la réglementation nationale en matière de cybersécurité, de laquelle découlera les règlementations sectorielles ;
- Mettre en place des mesures de prévention, de protection et de défense des données des Congolais ainsi que des infrastructures critiques et essentielles face aux risques de cybermenaces ;
- Piloter la gestion des risques au niveau national ;
- Piloter les mesures de cyber-résilience, de gestion des cyber-incidents, de continuité d'activités, de gestion des crise cyber, etc. ;
- Élaborer la politique de sécurité des systèmes d'information de l'État et assurer la conformité des procédures de Cybersécurité pour les organismes et institutions publiques ;
- S'assurer du mécanisme d'inclusion nationale des différentes parties prenantes à la mise en œuvre de la stratégie nationale de la Cybersécurité ;
- Identifier, en collaboration avec les Ministères et les régulateurs sectoriels, les organismes à importance vitale et les services essentiels, et s'assurer de leur mise à jour ;
- Suivre les indicateurs de performances en matière de Cybersécurité et sécurité des systèmes d'informations ;
- Établir et maintenir des bases de données des cyber-vulnérabilités ;
- Participer au développement de la confiance numérique ;
- Assurer l'audit et la veille technologique des systèmes d'information et des réseaux de communications électroniques en République Démocratique du Congo ;
- Certifier et homologuer les produits et services de Cybersécurité et de cryptologie en République Démocratique du Congo ;
- Accompagner les organismes et institutions publiques dans la lutte contre la Cybercriminalité ;
- Collaborer et participer à la sensibilisation, à la formation ainsi qu'aux investigations en matière de Cybersécurité.

En plus, l'Agence Nationale de Cybersécurité coopérera avec les structures de protection de données à caractère personnel, de lutte contre la cybercriminalité ainsi que celles de cyberdéfense militaro-sécuritaires afin d'assurer une synergie dans les efforts de protection du cyberespace congolais.

Mettre en place un dispositif sécuritaire de veille technologique des systèmes d'informations, des technologies et des usages numériques.

Des mesures seront prises pour assurer au profit des institutions officielles du pays, des entreprises et du grand public une veille active en matière de sécurité des technologies et des usages numériques. Ceci couvrira le secteur public et privé, les particuliers ainsi que les citoyens.

Mettre en place la politique de sécurité des systèmes d'information de l'État

Afin de garantir la disponibilité et l'efficience des infrastructures informationnelles publiques, un document de politique de sécurité des systèmes d'information de l'État sera élaboré et mis en exécution afin d'accompagner le processus de veille et de protection du cyberespace congolais. Ceci va nécessiter de mobiliser des ressources humaines et budgétaires afin d'assurer l'efficacité des mesures qui seront adoptées.

4.2 Protection des données et de l'information

4.2.1 Enjeux

Le vol de données digitales est devenu, depuis des décennies, sujet au cœur de débats sur la transformation numérique des économies mondiales. Les données tant privées que publiques sont visées par des cybercriminels. Si dans l'effort fourni, l'usager développe peu à peu la confiance dans la culture du numérique et dans ses outils, cependant, il redoute encore profondément on impact sur sa vie privée et ses activités.

Le mode opératoire constaté lors de certaines attaques informatiques contre des entreprises ou des administrations montre une réelle difficulté à dissocier vie privée et vie professionnelle dans l'utilisation des équipements comme des services. La prise de contrôle de l'équipement personnel utilisé — ordinateurs, tablettes — l'usurpation d'identité et le vol d'identifiants à des comptes bancaires ou à des sites commerciaux, par l'engagement d'une relation affective virtuelle débouchant sur une demande de transfert d'argent, par le vol ou chiffrement de données à l'insu de l'utilisateur conduisant au paiement d'une rançon, la cyber-escroquerie est aujourd'hui pratiquée à grande échelle par une criminalité qui s'est organisée et a gagné en efficacité.

D'où, la nécessité de protéger les données de citoyens et des particuliers. Pour accompagner sa stratégie cyber, la République Démocratique du Congo se dotera

d'une autorité de protection de données à caractère personnel avec des principes tels que consacrés dans la convention de l'Union Africaine sur la cybersécurité et la protection de données à caractère et qui sont repris dans la loi portant code du Numérique. A cet effet, l'Agence Nationale de Cybersécurité sera l'interlocuteur étatique opérationnel identifié pour protéger les données des citoyens et intervenir en cas d'incident informatique grave affectant les administrations et les infrastructures critiques. Les victimes de cyber malveillance seront prises en charge et orientées vers un service d'assistance dynamique.

4.2.2 Objectifs

Objectif Général II : Développer la culture, l'usage et la protection des données des citoyens congolais dans le cyberespace
Objectif spécifique II.1 : Protéger la vie numérique de la population
Objectif spécifique II.2 : Accroître la lutte contre la cybercriminalité
Objectif spécifique II.3 : Assister les victimes d'actes de cyber malveillance

La République Démocratique du Congo développera un usage du cyberespace conforme à ses besoins, à ses valeurs et y protègera la vie numérique de sa population. Elle accroîtra sa lutte contre la cybercriminalité et l'assistance aux victimes d'actes de cyber malveillance.

4.2.3 Mise en œuvre

Protéger la vie numérique, la vie privée et les données personnelles
La République Démocratique du Congo se dotera d'une feuille de route claire en matière d'identité numérique avec système d'authentification et de signature électronique afin de protéger la vie privée et les données personnelles ses citoyens. Les droits à la vie privée et à la maîtrise individuelle et collective des données personnelles seront réaffirmés chaque fois que nécessaire et notamment à l'occasion des négociations commerciales entre entreprises étrangères et locales, entre États qu'elles soient bilatérales ou multilatérales.

Mesurer la cybercriminalité
L'Agence Nationale de Cybersécurité mettra en œuvre un dispositif de suivi de l'évolution de la cybercriminalité en Afrique et dans le monde afin de produire des statistiques sur les types et les activités de la criminalité en ligne afin d'orienter les pouvoirs publics à prendre des dispositions idoines.

Apporter une assistance de proximité aux victimes d'actes de cyber malveillance

L'Agence Nationale de la Cybersécurité mettra en place un dispositif destiné à porter assistance aux victimes d'acte de cyber malveillance. Ce dispositif aura également la mission de sensibilisation aux enjeux et défis liés à la protection de la vie privée et de prévenir contre des potentielles menaces cyber. Il offrira un portail pour accompagner les victimes de cyber malveillance à utiliser des solutions s'appuyant sur des acteurs de proximité et faciliter les démarches administratives, notamment afin de favoriser le dépôt de plainte.

4.3 Sensibilisation, développement des capacités et des compétences

4.3.1 Enjeux

La République Démocratique du Congo a besoin de sensibiliser sa population aux risques associés aux usages du numérique et de la former à la cybersécurité.

Les considérations technologiques et politiques peuvent dominer les discussions sur la cybersécurité, en négligeant l'élément humain fondamental qui est au cœur de celle-ci. Ce domaine d'intervention aborde les défis liés à la promotion du renforcement des capacités en matière de cybersécurité et à la sensibilisation des entités gouvernementales, des citoyens, des entreprises et d'autres organisations, ce qui est essentiel pour permettre l'économie numérique d'un pays.

Les bonnes pratiques prises en compte dans cette section comprennent la mise en place de programmes d'enseignement et de sensibilisation dédiés à la cybersécurité, l'expansion des programmes de formation et de développement de la main d'œuvre, l'adoption de systèmes de certification internationaux, et la promotion de l'innovation et du développement durable, l'adoption de systèmes de certification internationaux et la promotion de pôles d'innovation et de recherche et développement (R&D).

La société civile néglige en général les bonnes pratiques lors de l'utilisation des réseaux de communications électroniques. Dans l'usage privé des réseaux de communications électroniques, les enfants et adolescents, confrontés à des contenus inadaptés, exposés au harcèlement ou à la prédation, sont les premières victimes. Afin de rompre le silence et de permettre les poursuites, les plus jeunes devront être initiés à la conduite à tenir lorsqu'ils sont victimes de malveillance numérique.

La sensibilisation de tous est un préalable nécessaire pour que le gouvernement, l'administration ou les entreprises puissent prendre en compte le « risque cyber » à son juste niveau et décider des mesures susceptibles de protéger les personnes qu'ils représentent ou les organismes qu'ils dirigent, face à des menaces de vol d'informations ou de propriété intellectuelle, d'atteinte aux données personnelles, voire l'exposition à des ruptures d'activité, d'accidents de production, avec des impacts technologiques ou environnementaux auxquels ils sont potentiellement exposés.

Outre la sensibilisation des plus jeunes, toutes les formations à tous les métiers doivent permettre aux futurs professionnels de bénéficier d'une sensibilisation plus ou moins importante en cybersécurité. Le gouvernement devrait également envisager de mettre en place divers systèmes d'incitation, tels que des bourses pour les programmes d'enseignement privés et des subventions pour les apprentissages correspondants.

4.3.2 Objectif

Objectif Général III : Développer des cursus dédiés à la cybersécurité et produire une main d'œuvre locale qualifiée.
Objectif spécifique III.1 : Sensibiliser l'ensemble de la population sur les risques cyber et les politiques publiques existantes en matière de Cybersécurité
Objectif spécifique III.2 : Développer des capacités et des compétences locales en Cybersécurité
Objectif spécifique III.3 : Favoriser l'innovation et la Recherche et Développement en matière de cybersécurité

La République Démocratique du Congo devra mettre en place, dès l'école primaire, une sensibilisation à la sécurité de l'information et aux comportements responsables dans le cyberespace. Les formations initiales supérieures et continues intégreront un volet consacré à la cybersécurité adapté à la filière considérée.

Il s'agira ici de sensibiliser toutes les branches de la population (gouvernement, citoyens, entreprises et autres organisations) essentielles à l'économie numérique.

Encourager le civisme cyber, en dotant les citoyens du bagage nécessaire pour une bonne attitude dans le cyberespace, à la gestion de la confidentialité et aux cyber risques. Améliorer la cyber hygiène de toutes les franges de la population.

Accompagner la transformation numérique de la sensibilisation nécessaire afin de protéger la souveraineté numérique, l'économie et les citoyens.

4.3.3 Mise en œuvre

Élaborer des programmes de sensibilisation en matière de Cybersécurité

Tel qu'inscrit dans le Plan National du Numérique, un programme ambitieux de sensibilisation de l'ensemble de la population résidant ou travaillant en République Démocratique du Congo doit être engagé. Sous la conduite de l'Agence Nationale de Cybersécurité et avec l'appui des Ministères concernés un appel à manifestation d'intérêt pour la réalisation de contenus de sensibilisation à destination du grand public sera lancé.

Encourager la création d'un Institut National et la promotion des Instituts privés en Cybersécurité

Dans le cadre de la mise en œuvre de la Stratégie Nationale de Cybersécurité, la République Démocratique du Congo ouvrira un Institut panafricain de cybersécurité et mettra en place une politique pour encourager l'ouverture des centres et des instituts en cybersécurité pour combler le besoin et faire du secteur un atout majeur dans le cadre de l'ambition d'être un hub technologique au cœur de l'Afrique.

Financer l'innovation et la R&D en matière de Cybersécurité

Le gouvernement favorisera un environnement qui stimule la recherche fondamentale et appliquée en matière de cybersécurité dans tous les secteurs et les différents groupes d'acteurs. Ces initiatives consistent, par exemple, à veiller à ce que les efforts de recherche nationaux soutiennent les objectifs de la stratégie nationale en matière de cybersécurité, à développer des programmes de R&D axés sur la cybersécurité dans les organismes de recherche publics ; la diffusion efficace des nouvelles découvertes, des technologies de base, des techniques, des processus et des outils.

Le gouvernement devra également chercher à établir des liens avec la communauté internationale de la recherche dans les domaines scientifiques liés à la cybersécurité, tels que l'informatique, l'ingénierie électrique, les

mathématiques appliquées et la cryptographie, mais aussi des domaines non techniques tels que les sciences sociales et politiques, les études commerciales et de gestion et la psychologie, pour n'en citer que quelques-unes.

Enfin, le gouvernement examinera les mécanismes d'incitation disponibles sous forme de subventions, les marchés publics, les crédits d'impôt, les concours et autres initiatives qui encouragent le développement de solutions, produits et services innovants en matière de cybersécurité.

4.4 La confiance numérique

4.4.1 Enjeux

Le cyberespace est en construction rapide. Les grands équipements qui assurent le fonctionnement des réseaux de communications électroniques dont les infrastructures sont situées en République Démocratique du Congo, sont souvent conçus, développés et parfois administrés depuis des centres situés hors du pays voire hors du continent. Il en est de même pour l'essentiel des équipements de communications et de sécurité informatique de nos infrastructures. Le fonctionnement d'un nombre croissant d'entreprises repose sur l'utilisation d'applications et le traitement de données hébergés dans des espaces immatériels non maîtrisés, portés par des infrastructures physiques situées hors du territoire et non soumises au droit congolais.

Les évolutions en cours tant au niveau des technologies que dans les modèles économiques, avec par exemple la multiplication des objets connectés ou la concentration des plateformes de service en ligne entre les mains de quelques acteurs seulement, sont de nature à amplifier cette perte de maîtrise du cyberespace national. En cas de crise internationale, l'accès à des pans entiers du cyberespace pourrait nous être refusé.

4.4.2 Objectif

Objectif Général IV : Assurer la disponibilité pour le grand public, les entreprises et les institutions officielles du pays des produits et services numériques présentant des niveaux d'ergonomie, de confiance et de sécurité adaptés aux usages et aux cyber menaces

Objectif spécifique IV.1 : Faire connaître et valoriser l'offre de produits et services de sécurité nationale

Objectif spécifique IV.2 : Assurer la capacité de prévenir, détecter et traiter les attaques informatiques sur les produits et services de confiance
Objectif spécifique IV.3 : Développer la sureté et la certification de produits de marque made in DRC

La République Démocratique du Congo fera de la sécurité du cyberespace un facteur de compétitivité. Elle s'assurera de la disponibilité pour le grand public, les entreprises et les institutions officielles du pays de produits et services numériques présentant des niveaux d'ergonomie, de confiance et de sécurité adaptés aux usages et aux cybermenaces.

4.4.3 Mise en œuvre

Établir et publier la liste des matériels, produits et services de confiance
L'Agence Nationale de Cybersécurité établira une liste de matériel et de services de confiance puis accentuera ses efforts en matière de qualification et de suivi de produits et de services de sécurité informatique. En lien avec les administrations compétentes, l'Agence Nationale de Cybersécurité engagera une étude sur les produits et services de sécurité informatique de confiance.

Mettre en place un Centre Opérationnel des Opérations (SOC)
La République Démocratique du Congo se dotera d'une capacité de détection et de traitement des attaques informatiques par le biais de l'Agence Nationale de Cybersécurité. Cet effort devra être poursuivi, mais il appartient aux infrastructures critiques d'assurer leur propre sécurité dans le domaine informatique, l'Agence Nationale de Cybersécurité ne devant intervenir que pour du conseil, du contrôle ou en cas de crise. Toutefois, comme tenu de la question sur la souveraineté numérique, le SOC national pourrait ouvrir les services de surveillance en temps réel et de riposte aux OIV et services essentiels.

Action 3 : Développer la sûreté et la certification de produits made in DRC
La République Démocratique du Congo mettra en place une politique prioritaire sur l'anticipation et la prévention. Il s'agira d'obtenir que les produits et services numériques ou intégrant du numérique, conçus, développés et mis en place localement soient parmi les plus sûrs du continent.

4.5 Législation et règlementation

Les nouvelles technologies de l'information et de la communication, au-delà du service qu'elles fournissent à la société, constituent un espace virtuel qui attire une délinquance particulière.

Face à cette situation, la législation congolaise se trouve limitée parce que, initialement conçue pour régir un espace territorialement bien défini ou déterminé.

Dans l'élaboration de la Stratégie Nationale de Cybersécurité, il est notamment question d'analyser les déficits du cadre législatif et règlementaire des TIC en République Démocratique du Congo et concevoir des instruments adéquats pour améliorer le cyber environnement et lutter contre la cybercriminalité.

Cette démarche passe par l'inventaire du cadre normatif existant avant de voir la législation actuellement en gestation.

4.5.1 Cadre normatif des TIC existants

Pour assurer la mise en œuvre cohérente et pérenne de la Stratégie Nationale de Cybersécurité, la République Démocratique du Congo va construire un écosystème législatif cyber en comblant les déficits du cadre législatif et règlementaire existants tout en se projetant sur des instruments adéquats afin d'améliorer son cyber environnement et lutter contre la cybercriminalité.

Cette démarche passe par l'inventaire du cadre normatif existant avant de voir la législation actuellement en gestation.

L'Ordonnance n°87-243 du 22 juillet 1987 portant réglementation de l'activité informatique au Zaïre.

L'article 9 de cette Ordonnance stipule que : « *Tout acte accompli à l'occasion d'une application informatique et qui porte atteinte à la sécurité de l'État, à l'ordre public ou aux bonnes mœurs, est punissable conformément aux lois en vigueur* ».

Il y a un déficit dans cette unique disposition à caractère répressif, car elle ne définit pas les actes infractionnels que peut accomplir une personne et les lois en vigueur qui les répriment. Elle ne définit pas non plus les applications informatiques susceptibles de porter atteinte à la sécurité de l'État, à l'ordre public ou aux bonnes mœurs.

Aussi, étant un acte règlementaire, cette Ordonnance ne pouvait contenir des incriminations et des peines au risque d'énerver le principe de la légalité et des peines.

La loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication

La présente loi abroge la loi-cadre n°013/2002 du 16 octobre 2002 sur les télécommunications en République Démocratique du Congo.

A l'instar de celle qu'elle a abrogée, cette loi a mis l'accent sur le secteur des télécommunications et n'a pris en compte que très partiellement les situations complétement inédites, notamment la protection des données à caractère personnel, la Cybersécurité et la cybercriminalité.

A titre indicatif, elle n'a pas règlementé certaines matières relevant du numérique telles les nouvelles activités ou les services numériques non identifiés, le commerce électronique, la valeur juridique des écrits et outils électroniques ainsi que leur création, certification et archivage , d'une part, et n'a pas prévu la création d'un organisme indépendant chargé de la protection des données à caractère personnel et d'autres structures notamment celles chargées de sécuriser les systèmes d'informations ainsi que de la lutte contre la cybercriminalité, d'autre part.

Au regard de l'expansion fulgurante des technologies de l'information et de la communication, l'adoption d'un nouveau cadre juridique dans le meilleur délai aiderait à combler les déficits du cadre normatif existant.

4.5.2 Législation en gestation

La loi portant Code du numérique dont le projet est actuellement sous examen au niveau du Gouvernement s'annonce être le nouveau cadre juridique qui aura pour but de combler les lacunes de la loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.

Dans sa substance, la nouvelle loi n'abrogera la précédente que dans certaines dispositions, à savoir celles de son titre III relatif à la protection de la vie privée et des données à caractère personnel des utilisateurs de réseaux et de services ainsi que celles du titre IV relatif à la cybersécurité, la cryptologie, la cybercriminalité et la fraude.

Elle mettra en place de nouvelles règles sur les activités et services numériques non identifiés, les régimes juridiques s'y rapportant, le régime de sanctions, la création des entités publiques ou organes indépendants chargés de la régulation ou du contrôle.

Ces instruments normatifs et institutionnels paraissent adéquats pour améliorer le cyber environnement et lutter contre la cybercriminalité en République Démocratique du Congo.

Dans son volet protection des données personnelles, le Code du numérique consacre tout un Livre qui est l'un des plus importants.

Ce livre institue l'Autorité de protection des données à caractère personnel, fixe les conditions et principes de traitement, de transmission et de transfert des données à caractère personnel ainsi que des activités du registre public des données. Il édicte les mesures administratives et des sanctions.

Dans son volet cybersécurité et cybercriminalité, le Code du numérique détermine les règles applicables aux moyens permettant d'assurer la protection et l'intégrité des données numériques, aux infractions spécifiques liées aux technologies de l'information et de communication et autres.

En traitant de la cybersécurité, il aborde les obligations générales et spécifiques inhérentes à la cybersécurité en même temps, précise les dispositions ainsi que les régimes juridiques applicables à l'exercice des activités et services de cryptologie. L'obligation la plus importante est celle de coopérer dans la détection des cyberattaques conformément aux dispositions légales et règlementaires applicables en République Démocratique du Congo. Cette obligation est imposée à toute personne physique ou morale opérant et/ou ayant des connaissances dans le secteur du numérique.

S'agissant de la cybercriminalité, le Code la définit comme étant l'ensemble d'infractions pénales spécifiques liées aux technologies de l'information et de la communication ainsi que celles dont la commission est facilitée ou liée à l'utilisation de ces technologies.

Le Code pose les principes de la responsabilité pénale conformément à la constitution, aux Codes pénal et de procédure pénale. Il s'agit de la responsabilité de personnes physiques et morales de droit privé responsables des infractions dans l'espace cybernétique.

Il réaffirme les peines applicables, à l'instar du Code pénal, à savoir : la servitude pénale, l'amende et la confiscation spéciale. Il réaffirme aussi les règles relatives à la participation criminelle, la tentative punissable, la récidive et les circonstances aggravantes.

Somme toute, la loi portant Code du numérique, une fois adoptée par le Parlement et promulguée par le Président de la République permettra à la République Démocratique du Congo de faire un grand pas dans l'amélioration du cyber environnement et la lutte contre la cybercriminalité.

Aussi, pour avoir un arsenal juridique consolidé en la matière et la mise en place de nouveaux mécanismes et moyens plus adaptés à la mutation du phénomène de la cybercriminalité, il est avantageux que la République Démocratique du Congo ratifie les conventions internationales et régionales qui existent. La première c'est la Convention de l'Union Africaine sur la Cybersécurité et la protection des données à caractère personnel, dite Convention de Malabo, adoptée le 27 juin 2014.

4.5.3 Enjeux

Au fur et à mesure que la République Démocratique du Congo continue sa transformation en une société numérique, elle devra à la fois lutter contre divers types de cyber crimes et cyber délits et protéger ses cyber intérêts. En outre, vu l'évolution rapide et continue du paysage cybernétique, la République Démocratique du Congo aura besoin de mettre en place et revoir régulièrement ses dispositifs législatifs et réglementaires.

4.5.4 Objectif

Objectif Général V : Mettre en place une législation cyber adaptée permettant de maitriser et de contrôler les activités et services numériques face aux nouveaux phénomènes du côté obscur de la digitalisation

Objectif spécifique V.1 : Combler les déficits du cadre législatif et réglementaire des TIC

Objectif spécifique V.2 : Élaborer des instruments adéquats pour améliorer le cyber environnement

Objectif spécifique V.3 : Réprimer et lutter contre la cybercriminalité

La République Démocratique du Congo ne dispose pas d'un cadre législatif et règlementaire à jour, à la fois aligné sur les développements du cyberespace et sur les normes régionales et internationales, permettant au pays de combattre effectivement les cyber-activités malveillantes visant le pays ou qui sont perpétrées depuis son territoire. Le cadre législatif et réglementaire congolais ne prévoit pas, à ce jour, d'unités judiciaires et de sécurité disposant des outils et des technologies appropriés pour mener à bien les missions de lutte contre la cybercriminalité.

4.5.5 Mise en œuvre

Effectuer une analyse des déficits du cadre législatif et réglementaire des TIC, et élaborer des instruments adéquats pour améliorer le cyber environnement et lutter contre la cybercriminalité.

Adopter, voter et promulguer le Code du Numérique
Dans son Livre relatif à la Cybersécurité et cybercriminalité, le Code du numérique détermine les règles applicables aux moyens permettant d'assurer la protection et l'intégrité des données numériques, aux infractions spécifiques liées aux technologies de l'information et de communication.

- Ratifier **les** conventions internationales et régionales relatives à la cybercriminalité et la cybersécurité

Pour avoir un arsenal juridique consolidé en la matière et la mise en place de nouveaux mécanismes et moyens plus adaptés à la mutation du phénomène de la cybercriminalité, la République Démocratique du Congo devra ratifier les conventions internationales et régionales qui existent. La première c'est la Convention de l'Union Africaine sur la Cybersécurité et la protection des données à caractère personnel, dite Convention de Malabo, adoptée le 27 juin 2014.

- **Créer un cadre institutionnel et renforcer** le cadre législatif et réglementaire en matière de protection **de** données et l'aligner aux normes internationales

Conformément aux recommandations de l'UIT, de l'UA et des autres organismes, la République Démocratique du Congo optera pour la création d'une autorité nationale de protection de données à caractère personnel qui collaborera étroitement avec l'Agence Nationale de Cybersécurité qui lui prêtera bras opérationnel dans le cadre de réalisation de ses missions notamment la définition des politiques sur la protection de données à caractère personnel et la procédure d'accès à tous les niveaux pour son traitement.

4.6 Gestion des risques et de crise

4.6.1 Enjeux

Le risque cyber constitue un risque à part entière. Il est d'ailleurs considéré par plusieurs États comme un risque systémique. Afin de se protéger correctement de la menace d'origine cyber, l'État congolais doit mettre en place un certain nombre de mesures de sécurité. Cette mise en place doit être menée de façon éclairée et raisonnée, en cohérence avec la menace qui pèse sur le cadre de protection.

Adopter une approche basée sur la gestion des risques permet d'appréhender la question en aval, en étudiant la menace, les évènements redoutés qui pourraient subvenir, afin d'anticiper et d'adapter au mieux les mesures de sécurité à mettre en place.

Par ailleurs, l"actualité nous présente chaque jour des États et des organisations mis en difficulté par une situation critique non anticipée.

Un tel événement porte atteinte à la réputation de l'État ou de l'organisation mais aussi à leur souveraineté mettant en cause leur stratégie, leur capacité d'anticipation et leur mode de gestion.

En revanche, un État ou une organisation proactive peut établir par avance un plan de gestion de crise et bénéficier ainsi, le moment venu, d'un avantage décisif qui les aide à réagir avec efficacité et à communiquer opportunément.

4.6.2 Objectif

Objectif Général VI : Mettre en place un Plan de continuité des activités pour l'ensemble des institutions, entreprises et services publics de l'État et des Organismes d'importance vitale et services essentiels
Objectif spécifique VI.1 : Se préparer à la crise de cyberattaque
Objectif spécifique VI.2 : Renforcer les capacités locales d'intervention par des partenariats de proximité en matière de gestion des incidents
Objectif spécifique VI.3 : Définir une politique de résilience pour les infrastructures critiques et les services essentiels

La République Démocratique du Congo doit anticiper et se préparer au pire plutôt que courir le risque de le subir. L'ANCY devra s'assurer d'une implémentation

obligatoire d'une cartographie des risques cyber au niveau national ainsi que d'un plan de continuité des activités pour l'ensemble de l'État congolais et des organismes économiques notamment ceux identifiés en tant que OIV.

4.6.3 Mise en œuvre

Préparer la République Démocratique du Congo à faire face à différents scénarios de risques.
Le risque cyber est aujourd'hui stratégique. Une menace exploitant une ou plusieurs vulnérabilités est un risque à part entière. La gestion des risques nécessite de s'appuyer sur un socle de compétences relativement variées et spécifiques qui permettront de mettre en œuvre des outils méthodologiques appropriés (Méthode EBIOS, Risk Manager ou In-House).

Préparer la République Démocratique du Congo à faire face à une crise informatique majeure.
Le renforcement de la sécurité de l'information des infrastructures critiques devra faire l'objet de mesures législatives.

La République Démocratique du Congo mettra en place un **CSIRT (Computer Security Incident Response Team)/CERT (Computer Emergency Response Team).** Ce centre de veille, d'alerte et de réponse, le CSIRT/CERT évoluera au sein de L'Agence Nationale de Cybersécurité (ANCY) , responsable de la prévention, de la détection et du traitement des cyberattaques sur les systèmes d'information.

Des exercices de gestion de crise cybernétique devront être menés et concerneront progressivement l'ensemble des infrastructures critiques.

La tenue régulière d'exercices revêt dès lors une importance non négligeable si l'on entend renforcer la résilience face aux incidents et tester l'efficacité du plan d'urgence. Les leçons tirées de ces exercices peuvent ensuite alimenter les évaluations annuelles de ce plan.

La participation des services de sécurité congolais, de l'Administration publique et des opérateurs d'infrastructures critiques aux exercices est essentielle.

L'ANCY devra faire adopter par chaque opérateur concerné une approche de gestion des risques, tant au niveau stratégique qu'au sein des organismes publics et privés, afin d'assurer au juste niveau nécessaire la sécurité des réseaux, systèmes d'information et données numériques.

L'ANCY devrait veiller à ce que les responsables de la cybersécurité, quel qu'en soit le niveau, bénéficient du soutien hiérarchique.

4.7 Coopération sous-régionale, régionale et internationale

La production et la délivrance des services essentiels par voie électronique ouvre la porte aux menaces cyber multi-protéiformes. Les risques naturels et les attaques malveillantes contre les systèmes d'infrastructures critiques peuvent causer de graves menaces sur notre société et sur notre économie. Les chocs récents, tels que les cyberattaques des banques ouest-africaines (3,5 milliards d'euros) ou les menaces de débrancher les câbles sous-marins reliant l'Europe et l'Afrique par fibre optique démontrent les effets en cascade que peut entraîner un arrêt des infrastructures critiques, susceptible de causer d'importants dommages économiques ainsi que des pertes en vies humaines.

4.7.1 Enjeux

Le cyberespace est devenu un sujet majeur de négociation au sein des organisations internationales dont les travaux portent désormais sur l'ensemble du champ du numérique.
Le cyberespace est devenu un sujet majeur de négociation au sein des organisations internationales dont les travaux portent désormais sur l'ensemble du champ du numérique.

Les États ont reconnu que loin d'être d'un espace sans règle, le cyberespace était régi par le droit international existant. Pour autant, le cadre normatif international est encore en débat, ce qui, en l'absence d'avancée des négociations, pourrait nuire à la préservation d'un cyberespace stable et sûr, respectueux des droits fondamentaux et propice au développement d'une économie prospère et de confiance à l'ère numérique. Tandis qu'un nombre croissant de pays africains déclarent se doter de capacités offensives, la conflictualité entre États trouve à s'exprimer de manière croissante dans le cyberespace.

Par ailleurs, les révélations de pratiques massives et de techniques d'espionnage menées par de grands États ou des alliances d'États contre d'autres — parfois alliés —, des personnes et des entreprises, ont accru la défiance politique contre les pays à l'origine de ces pratiques et la méfiance technique vis-à-vis de leurs produits et services.

Parallèlement, des groupes d'individus aux motivations et soutiens divers, mercenaires recrutés mondialement et associés au gré des circonstances, recourent régulièrement à des attaques informatiques dans le cyberespace pour tenter de déstabiliser les autorités gouvernementales de nombreux pays ou des entreprises qui les incarnent symboliquement. Des organisations terroristes profitent par ailleurs de l'audience portée par les réseaux sociaux pour diffuser une propagande destinée à attirer des volontaires et terroriser des populations. Ces différents groupes bénéficient d'un impact médiatique constant.

La République Démocratique du Congo doit participer à la transformation numérique du continent africain. L'Afrique numérique se construira sur des alliances, de la confiance et la maîtrise des données, matières premières des prochaines décennies. A ce titre, la République Démocratique du Congo fournira tous ses efforts pour promouvoir un cyberespace sûr, stable et ouvert entre des États sincères et crédibles.

4.7.2 Objectif

Objectif Général VI : Développer des relations étatiques pour renforcer la sureté, la stabilité et la sécurité du cyberespace
Objectif spécifique VI.1 : Signer des partenariats cyber avec des organismes et des États désireux de développer des cyberespaces stables
Objectif spécifique VI.2 : Établir avec des États crédibles et sincères des feuilles de route pour la promotion d'un cyberespace sûr et stable
Objectif spécifique VI.3 : Renforcer la présence et l'influence de la République Démocratique du Congo dans les discussions à toute échelle sur la Cybersécurité

La République Démocratique du Congo, dans quelques années, lorsqu'elle aura atteint un niveau de maturité suffisant, sera un acteur principal pour la promotion d'un cyberespace sûr, stable et ouvert en Afrique.

4.7.3 Mise en œuvre

Signer des conventions bilatérales et multilatérales existantes en matière de Cybersécurité
Afin de renforcer son cyberespace et échanger les bonnes pratiques, la République Démocratique du Congo signera des conventions en matière de Cybersécurité **avec** des États stables, crédibles et sincères.

Créer un nouveau partenariat cyber pour la coopération avec des États crédibles et sincères en matière de cybersécurité et de sécurisation du cyberespace commun

Avec des **États volontaires**, crédibles et sincères, des feuilles **de route** seront conjointement élaborées afin de déterminer les facteurs-clés de succès dans la mise en place des politiques propices à l'émergence d'un cyberespace stable et compréhensible par tous notamment en matière de réglementation, de normalisation et de certification, de confiance et sécurité dans le numérique - en veillant au respect de la souveraineté des États-membres, de protection de la vie privée et des données personnelles conçues comme un bien d'intérêt public.

Participer à des initiatives à toute échelle sur la Cybersécurité et encourager le retour sur l'expérience

Afin de renforcer la confiance à l'échelle internationale et d'explorer de nouveaux mécanismes de régulation visant à prévenir les conflits dans le cyberespace, la République Démocratique du Congo, dès qu'elle aura atteint le niveau de maturité satisfaisant, renforcera ses contacts avec toutes les parties prenantes disposées à engager le dialogue sur les enjeux de cybersécurité.

5

MISE EN OEUVRE DE LA STRATEGIE

5 MISE EN OEUVRE DE LA STRATEGIE

Les mesures décrites dans les sept champs d'action seront mises en œuvre d'ici 2025. Pour ce faire, il est nécessaire de définir clairement qui est responsable de quelles mesures, sur quelles bases légales s'appuie la mise en œuvre des mesures et jusqu'à quand les objectifs doivent être atteints.

1. Il convient de clarifier les bases légales.
2. Il est important de définir comment la République Démocratique du Congo collabore avec les institutions gouvernementales, les entreprises et la société civile et quel rôle ces acteurs jouent dans la mise en œuvre de chacune de ces mesures.
3. Les progrès réalisés dans la mise en œuvre de la stratégie nationale de cybersécurité doivent être transparents. Pour chaque mesure, il s'agit donc de définir des objectifs de prestations mesurables et jusqu'à quand ceux-ci doivent être remplis.
4. Il convient de définir qui mettra la stratégie nationale de cybersécurité à jour et comment, dans l'éventualité où des ajouts ou des modifications s'avèrent nécessaires avant fin 2025.

Afin de mettre en œuvre la vision et les sept objectifs stratégiques de cette stratégie ambitieuse, des investissements supplémentaires importants, mais essentiels, sont nécessaires.

Un engagement clair du gouvernement congolais en faveur de ces ressources est donc l'élément final élémentaire de cette stratégie nationale de cybersécurité.

Les investissements dans la cybersécurité ont indéniablement un impact économique, sociétal et économique direct. Si le gouvernement parvient à inspirer et à garantir la confiance numérique les entreprises et les citoyens seront également plus confiants pour investir dans davantage d'applications numériques. Cela stimulera la productivité et la croissance économique dans notre pays, et les cyberattaques pourront plus facilement être prévenues. L'objectif est de faire de la République Démocratique du Congo l'un des pays les moins vulnérables d'Afrique dans le domaine de la cybersécurité et des nouvelles technologies d'ici à 2025.

6
CONCLUSION

6 CONCLUSION

La RD Congo mettra en place des synergies pour protéger et assurer la veille en temps réel de l'efficience et de la production des services essentiels, en raison notamment des avancées technologiques, des exigences de la population ainsi que des effets de la nécessité du libre-échange, de l'interconnexion des systèmes et de la fluidité des transactions financières sur des plateformes électroniques.

Les risques naturels et les attaques malveillantes contre les systèmes d'infrastructures critiques peuvent causer de graves menaces sur notre société et sur notre économie. Les chocs récents, tels que les cyberattaques des banques ouest-africaines (3,5 milliards d'euros) ou les menaces de débrancher les câbles sous-marins reliant l'Europe et l'Afrique par fibre optique démontrent les effets en cascade que peut entraîner un arrêt des infrastructures critiques, susceptible de causer d'importants dommages économiques ainsi que des pertes en vies humaines.

De ce fait, il est donc nécessaire de mettre en place une politique de protection et sécurisation des infrastructures critiques et d'assurer la veille de ces infrastructures afin de parer contre ces attaques cyber qui deviennent de plus en plus imminentes.

Par ailleurs, étant donné qu'une grande partie des infrastructures critiques sont détenues et exploitées par le secteur privé, la stratégie nationale de Cybersécurité doit servir d'incitatif à l'État et aux exploitants d'infrastructures critiques à investir dans la protection et la résilience de ces dernières. Les mesures de résilience s'étendent de la mise en place de systèmes redondants à la diversification des fournisseurs clés, en passant par le renforcement des actifs et l'établissement de capacités de production de secours, de récupération rapide après incident et d'adaptation appropriées.

Cette stratégie permet de mettre en avant des défenses imparables, des compétences puissantes, dans le but de faire d'une attaque quelconque sur le territoire de la République Démocratique du Congo, une tentative se résultant par un échec. Mais surtout assurer au pays un niveau de maturité suffisant.

Nous savons que le risque zéro n'existe pas. La technologie numérique fonctionne notamment parce qu'elle est ouverte (ex : le cloud), cette ouverture est inévitablement porteuse de risques.

Il est donc nécessaire de mettre en lumière le côté législatif, une étape importante dans la mise en œuvre de cette stratégie. La vision à l'horizon 2025 envisage une

République Démocratique du Congo sécurisée et résiliente face aux cybermenaces ainsi que prospère et confiante dans le monde numérique.

7

GLOSSAIRE

7 GLOSSAIRE

Activité d'importance vitale ou AIV (Cybersécurité) : Activité digitalisée qui concourt à la production et la distribution des services indispensables à l'exercice de l'autorité de l'État et des services publics, au fonctionnement de l'économie et des finances publiques, au maintien de l'ordre publique, au potentiel de défense et de sécurité national et qui est difficilement substituable. Activité non digitalisée mais nécessaire au bon déroutement d'une activité digitale d'importance vitale (ex. fourniture en énergie).

CSIRT (Computer Security Incident Response Team) : équipe chargée d'alerter sur les menaces, de prévenir les risques sur les systèmes d'information, de réagir en cas d'incident de sécurité et d'aider à en atténuer les effets.

Cyber conflits : Si le scénario d'une guerre menée exclusivement dans le cyberespace (cyberguerre) est actuellement considéré comme peu réaliste, il est avéré en revanche que des cyberattaques de toutes sortes sont utilisées comme des moyens de guerre dans divers conflits.

Cyber espionnage : Le cyber espionnage est une activité visant à obtenir des informations de manière non autorisée à des fins politiques, militaires ou économiques. Elle est pratiquée par des acteurs étatiques aussi bien que non étatiques. Ses auteurs se concentrent à la fois sur des entreprises et sur des institutions étatiques, sociales ou internationales. L'économie congolaise est l'une des plus sollicitée au monde, et de nombreux groupes régionaux et internationaux y ont installé leur bureau. Cela fait de notre pays une cible attrayante pour le cyber espionnage, dont les conséquences peuvent être néfastes.

Cyber hacktivisme : Les hacktivistes exploitent les réseaux informatique dans le but de militer pour cause politique ou sociale (défiguration de sites Internet, exfiltration de données, etc...).

Cyber terrorisme : Ensemble des attaques graves (virus, piratage, etc.) et à grande échelle des ordinateurs, des réseaux et des systèmes informatiques d'une entreprise, d'une institution ou d'un État, commises dans le but d'entraîner une désorganisation générale susceptible de créer la panique.

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

Cybersécurité : l'ensemble des mesures et des actions destinées à protéger le cyberespace des menaces associées à ses réseaux et à son infrastructure informatique ou susceptibles de leur porter atteinte. 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.

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

Désinformation et propagande : La menace due à la diffusion ciblée d'informations erronées ou obtenues illégalement par des cyberattaques ou non dans le but de discréditer des acteurs politiques, militaires ou civils a beaucoup gagné en importance. Dans certains pays, on observe des activités de ce genre avant des élections importantes.

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.

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.

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

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.

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.

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

Risque : L'exploitation d'une vulnérabilité d'un système donné, qui engendre un impact néfaste ave une certaine vraisemblance.

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.

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

Système d'Information d'Importance Vitale ou SIIV : Système d'information hébergeant ou transportant une activité ou des données d'importance vitales.

Technologies de l'Information et de la Communications (TIC): technologies employées pour recueillir, stocker, utiliser et envoyer des informations et incluant celles qui impliquent l'utilisation des ordinateurs ou de tout système de communication y compris de télécommunication.

8

BIBLIOGRAPHIE

8 3. BIBLIOGRAPHIE

8.1 3.1 CONSTITUTION, LOIS, REGLEMENT ET DECISION

1. Constitution de la République Démocratique du Congo, JORDC, février 2006.
2. Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication, JORDC, numéro spécial, septembre 2021.
3. Décision n°22/013 du 23 mai 2022 portant création et organisation, au sein du Cabinet du Président de la République, d'une commission technique chargée de la mise en œuvre de la Cybersécurité en République Démocratique du Congo (CTC).
4. Décision n°22/014 du 23 mai 2022 portant désignation des membres de la commission technique chargée de la mise en œuvre de la cybersécurité en République Démocratique du Congo (CTC).

8.2 RAPPORTS, DECLARATIONS ET DOCUMENTS OFFICIELS

1. L'Union internationale des télécommunications (UIT), la Banque mondiale, le Secrétariat du Commonwealth (Comsec), l'Organisation des télécommunications du Commonwealth (OTC), et le Centre d'excellence de l'OTAN pour la cyberdéfense en coopération (CE-CDC OTA). Guide pour l'élaboration d'une stratégie nationale de la cybersécurité - Engagement stratégique pour la cybersécurité », Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).
2. Déclaration de Lomé sur la cybersécurité et la lutte contre la cybercriminalité, sommet de la cybersécurité-Lomé 2022, mars 2022.
3. Stratégie nationale de cybersécurité du Sénégal, République du Sénégal, novembre 2022.
4. Projet de loi portant code du numérique de la République Démocratique du Congo, RD Congo, 2022.
5. Africa Cyber Security Market report
6. La Résolution 58/199 de l'Assemblée Générale des Nations Unies relative à la création d'une culture mondiale de la Cybersécurité et de la protection des infrastructures essentielles de l'information, adoptée le 30 janvier 2014.

7. La Convention de l'Union Africaine sur la Cybersécurité et la protection de données à caractère personnel, adoptée à Malabo en Guinée Équatoriale le 27 juin 2014.
8. La résolution 2341 du Conseil de sécurité des Nations Unies sur la protection des infrastructures critiques et le renforcement de la capacité des États de prévenir les attaques contre ces infrastructures, adoptée à l'unanimité le 17 février 2017.

8.3 OUVRAGES

1. NDUKUMA ADJAYI K., Droits de télécoms et du Numérique : profil africain et congolais, prospective comparée d'Europe et de France, éd. Le Harmattan, Paris, 2019.

9 ANNEXES

ANNEXE 1

Critères de sélection des OIV (liste non exhaustive)

1. Organisme exerçant une activité d'importance vitale digitalisée, en cours de digitalisation ou à digitaliser dans les 3 prochaines années	2. Organisme exerçant une activité nécessaire au bon déroulement d'une activité d'importance vitale digitalisée, en cours de digitalisation ou à digitaliser dans les 3 prochaines années.
3. Organisme ayant un poids considérable sur sa contribution au PIB du pays	4. Organisme qui dessert un nombre significatif d'abonnés pour un service essentiel

ANNEXE 2

Liste des activités d'importance vitale en RDC

SECTEUR Sous – secteur	ACTIVITÉS D'IMPORTANCE VITALE EN RDC
REGALIEN Administration publique	Activités civiles de l'État
	Activités fiscales de l'État
	Activités judiciaires
	Activités militaires de l'État
	Réseau e-gouvernement
	Messagerie professionnelle de l'administration publique
	Identification biométrique
ENERGIE Électricité	Vente ou revente d'électricité aux particuliers et entreprises (vente d'électricité aux consommateurs finaux, vente d'électricité aux fournisseurs d'électricité, exploitation d'une bourse de l'électricité)
	Distribution d'électricité (conduite et supervision du réseau de distribution, gestion des raccordement des consommateurs, pilotage des compteurs des consommateurs)

	Transport d'électricité (conduite et supervision du réseau de transport, équilibrage de l'offre et de la demande, gestion des interconnexions)
ENERGIE – Pétrole	Exploitation d'oléoducs (conduite et supervision d'oléoducs)
	Production (conduite et supervision d'installations de productions) Raffinage (conduite et supervision de raffineries) Stockage (conduite et supervision d'installations de stockage) Transport hors oléoducs (planification des transports, exploration d'une flotte de navires ou camions)
	Service de transfert de données logistiques numérisées entre opérateurs pétroliers, et entre les opérateurs pétroliers et les autorités publiques
ENERGIE – GAZ	Vente ou revente de gaz aux particuliers et entreprises (vente de gaz aux consommateurs finaux de gaz, exploitation d'une bourse du gaz)
	Distribution de gaz (conduite et supervision du réseau de distribution, gestion des raccordements des consommateurs, pilotage des compteurs des consommateurs)
	Transport de gaz (conduite et supervision du réseau de transport, équilibrage de l'offre et de la demande, gestion des interconnexions)
	Stockage de gaz (conduite et supervision d'installations de stockage)
	Liquéfaction de gaz (conduite et supervision d'installations de liquéfaction) Déchargement de regazéification (conduite et supervision d'installation de déchargement, conduite et supervision d'installation de regazéification)
	Fourniture, distribution, transport, stockage et traitement de gaz
	Raffinage (conduite et supervision d'installations de raffinage) Traitement (conduite et supervision d'installations de traitement)
TRANSPORTS – Transport aérien	Transport de passagers (enregistrement et embarquement des passagers, exploitation des aéronefs) Transport de fret (enregistrement et embarquement du fret, exploitations des aéronefs)
	Exploitation d'installations aéroportuaires (inspection-filtrage, enregistrement et embarquement du fret, gestion des passagers et des bagages-

	Avitaillement et armement des aéronefs
	Contrôle et régulation de la navigation aérienne en route Contrôle et régulation des aérodromes
	Maintenance et réparation aéronautiques
	Gestion des flux de passagers
TRANSPORTS – Transport guidé	Transport de passagers (exploitation des matériels de transports guidés, information et accueil des passagers)
TRANSPORTS – Transport par voie d'eau	Service aux marchandises (chargement, déchargement, entreposage, gardiennage, gestion de conteneurs) Accueil des navires (pilotage, remorquage, lamanage, ravitaillement) Information, accueil, inspection-filtrage, embarquement-débarquement des passagers Gestion des ouvrages portuaires
	Service de trafic maritime
	Service de trafic fluvial
TRANSPORTS – Transport routier	Gestion de routes (entretien, signalisation, gestion des infrastructures, régulation et surveillance du trafic)
	Gestion des routes (entretien, signalisation, gestion des infrastructures, régulation et surveillance du trafic)
	Gestion centralisée d'une flotte de véhicules Aide à la gestion du trafic Information aux passagers Aide à l'exploitation
	Transport de marchandises et de matières dangereuses
	Gestion des flux de passagers Exploitation
TRANSPORTS	Organisation de transports Affrètement de transporteurs
TRANSPORT AÉRIEN	Protection des installations aéroportuaires (Systèmes de surveillance de contrôle d'accès et d'alarme de gestion de la riposte, systèmes de surveillance par télévision en circuit fermé) Transport de fret (gestion des bases de données d'agents habilités et/ou d'expéditeurs connus) Coordination des activités de sûreté (systèmes de commandement, de contrôle et de répartition de la sûreté)
LOGISITIQUE	Gestion de plateforme logistique
BANQUES	Gestion des dépôts Octroi de crédits Service de paiement

	Service d'investissement
INFRASTRUCTURES DE MARCHÉS FINANCIERS	Exploitation de plateformes de négociation d'instruments financiers
	Service de contrepartie centrale pour les transactions sur les marchés financiers (chambres de compensation)
	Tenue de registre Gestion des garanties (collatéral) Règlement-livraison de titres
SERVICES FINANCIERS	Service de paiement Émission de titres spéciaux
	Planification et exploitation des transports de fonds Gestion des demandes de collecte et d'approvisionnement
ASSURANCE	Assurance vie Assurance non vie Réassurance
SOCIAL	Calcul et paiement des prestations sociales (assurance maladie, vieillesse, allocations familiales et chômage) Gestion du recouvrement et de la trésorerie des organismes sociaux
SANTÉ – Établissements de soins de santé (y compris les hôpitaux et les cliniques privées)	Service concourant aux activités de prévention, de diagnostic ou de soins
	Réception et régulation des appels Service mobile d'urgence et réanimation
SANTÉ – Produits pharmaceutiques	Distribution pharmaceutique
FOURNITURE ET DISTRIBUTION D'EAU POTABLE	Fourniture d'eau en bouteille (puisage, embouteillage, planification, logistique, contrôle de la qualité de l'eau) Production d'eau courante (conduite, supervision et maintenance des installations de captation, de transport, de traitement et de stockage, contrôle de la qualité de l'eau) Distribution d'eau courante (conduite, supervision et maintenance des installations de distribution d'eau, logistique, contrôle de la qualité de l'eau)
TRAITEMENT DES EAUX NON POTABLES	Collecte des eaux usées Traitement des eaux usées
	Collecte et évacuation d'eaux pluviales
INFRASTRUCTURES. NUMÉRIQUES	Services de communications électroniques au public Services de communication électroniques à haut et très haut débit Service d'interconnexion par appairage pour l'échange de trafic internet
	Enregistrement et gestion de noms de domaine Hébergement de noms de domaine
	Hébergement de zones de premier niveau
	Gestion d'affection en parcours scolaire ou étudiant

EDUCATION	Organisation d'examens nationaux
	Gestion des bourses
RESTAURATION	Gestion des commandes Gestion de l'approvisionnement, de la logistique, du stockage et de la distribution
AVIATION CIVILE	Transport de passagers (enregistrement, contrôle des documents de voyages, embarquement et débarquement des passagers, exploitation des aéronefs) Transport de fret (enregistrement, contrôle des documents, chargement et déchargement du fret, exploitation des aéronefs)
	Exploitation d'installations aéroportuaires (contrôle d'accès des personnes et des véhicules, inspection-filtrage, enregistrement, chargement et déchargement du fret, gestion des passagers et des bagages) Avitaillement et armement des aéronefs Explosion d'aéronefs avec déversement de marchandises dangereuses dans le réseau public d'eau Interférence avec les systèmes de télécommunication aéronautiques sol-sol
	Contrôle et régulation de la navigation aérienne en route Contrôle et régulation des aérodromes Contrôles de l'évolution des aéronefs télé pilotés, drones au voisinage d'aéronefs dans les phases de décollage, atterrissage et phase en route.
	Maintenance et réparation aéronautique Protection des aides à la navigation aérienne Rupture brusque du circuit électrique du balisage lumineux interférences et perturbation des fréquences aéronautiques
	Gestion des flux passagers (mécanisme d'enregistrement et de contrôle des bagages)

ANNEXE 3

Extrait de la Politique de Sécurité des Systèmes d'Information de l'état (PSSIE)

INTRODUCTION

La Politique de Sécurité des Systèmes d'Information de l'État – PSSIE – a vocation de définir le cadre de référence en matière de sécurité du système d'information de la République Démocratique du Congo.

Elle spécifie les éléments stratégiques et principes permettant de protéger les Systèmes d'Information de l'État.

Elle précise :

- Les enjeux et objectifs relatifs à la sécurité du système d'information
- La démarche au travers de principes sécurité permettant d'instaurer des systèmes d'information sécurisés, fiables et de confiance

La PSSIE repose sur des principes fondamentaux :

- Une politique pragmatique et des mesures au regard de nos enjeux
- Une gouvernance sécurité assurant le respect des mesures de sécurité définies
- Une gestion et une maîtrise des risques
- Des contrôles garantissant une d marche d'amélioration continue

La sécurité des systèmes d'information (SSI) a pour finalité de garantir la maîtrise des risques SSI et d'assurer :

- La disponibilité des systèmes d'information, et en particulier des applications supportant des processus critiques
- L'intégrité des informations et des moyens de traitement, afin d'attester de l'exactitude et de la fiabilité de nos opérations
- La confidentialité des informations, en particulier du traitement des données sensibles pour nos métiers et nos clients et ce, quelle que soit leur nature personnelles ou protégées par la propriété intellectuelle

PERIMÈTRE

La PSSIE s'applique à l'ensemble des informations et leurs traitements (création, conservation, échange, suppression) sous leur forme matérielle ou immatérielle (email, papier, image).

Elle s'applique également à toute personne physique ayant accès au système d'information au sein de l'État, qu'elle soit interne ou externe.

Par déclinaison, les sous-traitants concourant à l'exploitation du système d'information, éditeurs, constructeurs, prestataires de services, se verront appliquer un ensemble de règles en cohérence avec la PSSI, quel que soit leur lieu d'implantation.

1. ENGAGEMENT DE L'ÉTAT

Afin de réaliser la meilleure transformation numérique sécurisée, l'État doit en permanence s'assurer de :

- Se préserver des menaces et maîtriser ses risques informatiques
- Préserver la cybersécurité comme une composante à part entière des activités et projets de l'État
- Apporter des réponses adaptées à la réglementation et aux exigences de toutes les parties prenants
- Faire de la cybersécurité un soutien notre croissance
- Que la cybersécurité demeure une démarche d'intelligence collective

2. MODUS OPERANDI

Article 1. Objet du document

Le présent document fixe les conditions de mise en œuvre de la politique de sécurité des systèmes d'information de l'État (PSSIE).

Article 2. Champ d'application

La PSSIE s'applique à tous les systèmes d'information (SI) de l'État.
La PSSIE concerne l'ensemble des personnes physiques ou morales intervenant dans des SI, qu'il s'agisse des agents de l'État ou bien de tiers (prestataires ou sous-traitants) et de leurs employés.

La PSSIE s'impose aussi aux systèmes aptes à traiter des informations classifiées de défense même s'ils sont soumis à un corpus réglementaire spécifique et complémentaire.

La plupart des règles de sécurité de la PSSIE constituent des règles de base.

Article 3. Date d'entrée en vigueur

La PSSIE entre en vigueur le jour de sa publication.

Article 4. Dispositions transitoires

La mise en application de la PSSIE s'effectue selon les règles suivantes :

- Les SI de l'État devront être en conformité totale dans les 3 ans suivant la publication de la PSSI
- Les entités devront, au 1er janvier 2025, avoir mis en conformité leur politique de sécurité des systèmes d'information (PSSI) et défini un plan d'action.

Article 5. Formation des agents

L'État via l'Agence Nationale de Cybersécurité forme les agents chargés d'appliquer la PSSIE. Ces derniers doivent être sensibilisés la sécurité des SI (SSI) et au respect des règles de sécurité. Les agents exploitant les SI ou assurant des missions en lien avec la SSI font l'objet de formations adaptées.

Article 6. Pilotage et évolutions de la PSSIE

La PSSIE est amené à évoluer dans le temps. Elle pourra notamment être revue afin de prendre en compte :

- Les évolutions des menaces et les retours d'expérience des traitements d'incidents
- Les résultats d'analyses de risques ainsi que les actions découlant de contrôles ou d'inspections
- Les évolutions des contextes organisationnel, juridique, réglementaire et technologique.

Le suivi de ces évolutions est assuré par l'Agence Nationale de Cybersécurité en liaison avec le gouvernement, il a pour principales missions :

- De suivre la mise en œuvre de la PSSIE
- De proposer des mises à jour
- De proposer des documents complémentaires et des directives permettant d'en faciliter ou d'en préciser la mise en œuvre
- De suivre les évolutions des documents techniques.

Article 7. Organisation de l'État pour la mise en application de la PSSIE

L'Agence Nationale de Cybersécurité est l'autorité en charge de la sécurité des systèmes d'information.

A ce titre, elle :

- Est chargée de valider les mesures de protection des SI élaborées et de veiller à leur application.
- Est chargée de faire mener des inspections des systèmes d'information au sein des services de l'État
- Se fait présenter régulièrement la situation des systèmes d'information de l'État en liaison avec le gouvernement

L'Agence Nationale de Cybersécurité a notamment pour mission de désigner, sur leur périmètre de compétence, les autorités d'homologation de sécurité des SI.

Article 8. Mise en application de la PSSI

Chaque entité met en place un dispositif de gestion des risques pour ses systèmes d'information. Ce dispositif doit permettre une meilleure maîtrise de la sécurité des SI par la mise en œuvre de mesures de protection proportionnées aux enjeux et en adéquation avec les risques encourus.

Cette gestion s'appuie sur un processus régulier d'identification, d'appréciation et de traitement des risques. Ce dispositif doit aussi permettre de s'assurer que les mesures de sécurité sont adaptées.

Le choix de ces mesures est effectué en s'assurant que les actions prévues et les coûts engendrés sont proportionnés à la réduction du risque.

Les entités peuvent s'appuyer sur les guides et recommandations publiés par l'ANCY.

Dans ce but, chaque institution :

- met en place une organisation en application de la PSSIE
- établit un inventaire de ses systèmes d'information et en évalue la sensibilité
- conduit une analyse de risques pour ses systèmes d'information, selon la méthode préconisée par l'ANCY et met en place les mesures de sécurité applicables
- conduit des actions de motivation : sensibilisation et formation à la sécurité des systèmes d'information

Chaque institution élabore un bilan annuel comportant :

- une synthèse de l'état d'avancement de la cartographie des SI et de ses mises à jour
- l'état d'avancement de l'application des règles dictées par la PSSIE
- un récapitulatif des actions réalisés pour la mise en conformité de la PSSIE
- un récapitulatif des incidents significatifs constatés
- mise en œuvre pour les résoudre

Article 9. Contrôle et suivi de l'application de la PSSIE

Le respect de la PSSIE fait l'objet de contrôles réguliers à différents niveaux, à définir par l'ANCY.

L'ANCY vérifie, lors de ces contrôles, la conformité des dispositions prises par les entités avec les exigences de la présente PSSIE.

En complément, des actions de contrôle peuvent être engagées à la suite d'incidents de sécurité majeurs, ou en cas de forte suspicion de non-conformité.

Article 10. Traitement des incidents et gestion de crise

La rapidité des attaques informatiques rend nécessaire une veille renforcée et une réaction coordonnée des différents acteurs.

Afin de rétablir le fonctionnement rapide des activités vitales de l'État, une stratégie de traitement des incidents et de gestion de crise est mise en place.

3. OBJECTIFS

Les objectifs sécurité visent à atteindre les enjeux de la lutte contre la cybercriminalité selon une approche pragmatique et adaptée à la maturité et aux ambitions de l'État mais également aux risques de sécurité identifiés :

- S'acculturer en matière sécurité de l'information : toutes les parties prenantes doivent d'être au courant des dernières bonnes pratiques de sécurité et sont sensibilisés et formés au niveau de sécurité nécessaire.
- Protéger les actifs essentiels : le système d'information se doit d'être à jour pour palier toute exploitation de vulnérabilités.
- Intégrer la sécurité dans les projets : tout projet exploitant de l'informatique se doit d'évaluer et de tester sa sécurité tout au long de son cycle de vie
- Garantir une continuité de service : les systèmes critiques du système d'information doivent être protégés au travers d'une cartographie actualisée et d'un plan de secours informatique défini.

4. LES RISQUES

L'État doit se prémunir contre les multiples menaces auxquelles il est soumis telles que :

- Événements accidentels
- Panne, incendie, coupure électrique, coupure fournisseur réseau
- Événements environnementaux
- Menace externe
- Cybercriminalité
- Vol d'informations
- Fraude ciblant l'extorsion de fonds
- Menace interne
- Erreur de manipulation
- Mauvaise gestion des droits
- Collaborateurs malveillants

5. REGLES

La PSSIE s'appuie sur les thématiques ci-dessous ressorties de la Stratégie Nationale de Cybersécurité

- Politique, organisation, gouvernance
- Sécurité des ressources humaines
- Gestions des biens
- Intégration de la SSI dans le cycle de vie des systèmes d'information
- Sécurité physique
- Sécurité physique des datacenters
- Sécurité des réseaux
- Exploitation des SI
- Sécurité du poste de travail
- Sécurité du développement des systèmes
- Traitement des incidents
- Continuité des activités
- Contrôles

6. SUIVI

Cette politique sera révisée tous les trois ans ou ponctuellement lorsqu'un événement majeur le nécessite.

République Démocratique du Congo

présidence.cd