

Stratégie Nationale de Cybersécurité

2024-2028

Agence Nationale de la Cybersécurité (ANCy)

63 Bd du 13 Janvier,
Nyékonakpoè, Lomé-TOGO
07 BP 7878

+228 97 52 58 58
+228 70 60 60 83

secretariat.ancy@ancy.gouv.tg
<https://www.ancy.gouv.tg/>



S.E.M. Faure Essozimna GNASSINGBÉ
Président de la République Togolaise



Mesdames et Messieurs,

La cybersécurité est un enjeu majeur pour le Togo qui a fait du numérique un levier essentiel de sa transformation économique et sociale. Elle est indispensable pour garantir la confiance des citoyens, des entreprises et des administrations dans les services numériques, pour lutter contre les menaces qui pèsent sur notre sécurité nationale et préserver notre souveraineté nationale.

La mise en place de la Stratégie nationale de cybersécurité est une étape cruciale dans l'engagement du gouvernement à anticiper et faire face aux menaces numériques de toutes natures, afin de garantir la protection des citoyens, des entreprises, ainsi que des infrastructures et services critiques contre les menaces numériques.

Je vous invite à vous approprier cette stratégie et à la mettre en œuvre avec détermination et efficacité, pour faire du Togo un pays modèle en matière de cybersécurité.

Victoire S. TOMEGA-DOGBE,
Premier ministre, Cheffe du gouvernement



Co-préface

Sous la haute impulsion du Président de la République, Son Excellence Monsieur Faure Essozimna GNASSINGBE, les technologies de l'information et de la communication (TIC) ont profondément transformé, en l'espace d'une décennie, nos habitudes personnelles et professionnelles, porté la compétitivité des entreprises à un niveau inédit, rapproché les administrations des usagers et favorisé la transparence de la vie des institutions de notre pays.

Cet usage massif des TIC s'inscrit dans l'ambition pleinement assumée de notre pays de devenir un hub logistique et un centre d'affaires par excellence à l'horizon 2025 dans la droite ligne des objectifs du Plan National de Développement (PND 2018-2022) et en conformité avec la feuille de route gouvernementale « TOGO 2025 ».

Toutefois, cette société mondiale de l'information, véritable « tour de Babel », qui ouvre la voie vers des possibilités infiniment insoupçonnées, pour le meilleur, certes, mais aussi, semble-t-il pour le pire, offre également de nouvelles possibilités aux cyberattaques qui acquièrent, des capacités illimitées de nuisance à la résilience de nos infrastructures, réseaux essentiels ; et à la prospérité économique nationale.

Ces cyberattaques dont les provenances sont de plus en plus variées et sophistiquées, s'appuient sur des motifs divers : elles sont le fait d'individus et d'activistes poursuivant des buts politiques, d'organisations criminelles recourant à l'escroquerie ou au chantage, d'espions travaillant pour d'autres nations ou d'organisations terroristes qui veulent perturber ou déstabiliser notre Etat et notre société.

Face à cette situation, bien que nous n'ayons pas encore tous collectivement pris la mesure des enjeux et des risques cyber, le Gouvernement pour préserver l'intégrité de nos frontières physiques et du cyberspace national, garantir la sécurité de nos concitoyens, protéger nos infrastructures essentielles et garder notre économie en croissance, a décidé d'inscrire la sécurité et la défense des systèmes d'informations au rang des secteurs prioritaires nationaux.

La présente Stratégie Nationale de Cybersécurité (SNCy), élaborée conformément aux meilleures pratiques internationales en la matière et soumise à l'appréciation des différentes parties prenantes, permettra à notre pays de faire efficacement face aux graves menaces sur la disponibilité, l'intégrité et la confidentialité des systèmes, des données et des processus numériques nationaux.

Elle vise à prévenir et à répondre efficacement aux cyberattaques en améliorant la résilience de notre pays dans ce domaine, en renforçant les capacités nationales, en soutenant la confiance numérique, en promouvant la coopération internationale, en vue de conforter à terme, le leadership numérique du Togo dans la sous-région.

Même si beaucoup reste à faire, nous restons convaincus que les objectifs simples et concrets, mais très ambitieux que nous nous sommes fixés, sont à la hauteur des grands défis que portent les innovations technologiques plus que jamais nécessaires pour garantir à notre pays une place de choix dans le concert des nations.

Chers compatriotes, chers partenaires, si le grand défi de la cybersécurité, lancé fin 2018 avec la promulgation de la loi sur la cybersécurité et la lutte contre la cybercriminalité, dévoilait déjà une volonté politique forte de prendre cette problématique à bras le corps, la présente SNCy confirme à tous égards, la place privilégiée que le Gouvernement accorde à cette problématique.

Elle nous appelle donc à participer, à sa mise en œuvre pour un cyberspace sûr et fiable, afin de « sauter » plusieurs étapes de notre transition digitale, grâce à l'approche participative qui est développée dans le plan d'action de cette stratégie.

Ambassadeur
Calixte Batossie MADJOULBA,
*Ministre de la Sécurité
et de la Protection Civile*

Cina LAWSON,
*Ministre de l'Économie Numérique
et de la Transformation Digitale*



Chers lecteurs,

Notre monde évolue à une vitesse sans précédent, avec la technologie numérique au cœur de chaque aspect de nos vies. Avec cette transformation vient un ensemble complexe de défis et de menaces, des acteurs malveillants cherchant à exploiter nos vulnérabilités.

Face à ces défis, c'est avec fierté et détermination que je vous présente la Stratégie Nationale de Cybersécurité (SNCy 2024-2028), un jalon essentiel de notre engagement continu à participer à la sécurité nationale, à la souveraineté numérique de notre pays.

La Stratégie Nationale de Cybersécurité repose sur quatre piliers principaux : Promouvoir une culture de la cybersécurité en sensibilisant et en formant la population, considérant que la conscientisation est la première ligne de défense contre les menaces cyber sécuritaires.

La protection des systèmes d'information critiques sera une réalité, grâce au renforcement des mesures de protection existantes, l'identification et l'atténuation des vulnérabilités, la mise en place des contrôles de sécurité appropriés et la consolidation de nos défenses contre les attaques sophistiquées.

Renforcer le système de réponse aux incidents informatiques : Nous mettrons en place un système de réponse aux incidents efficace et coordonné, capable de détecter, d'analyser et de réagir rapidement face aux incidents de cybersécurité.

Enfin, nous veillerons à ce que les auteurs de crimes et de délits de cybersécurité soient poursuivis et traduits en justice pour répondre de leurs actes, grâce aux mécanismes de poursuite efficace des crimes et délits de cybersécurité.

Fruit d'un travail acharné et d'une large concertation avec les acteurs concernés par la cybersécurité, notre SNCy, est à la fois ambitieuse et réaliste. Elle s'inspire des

meilleures pratiques internationales en la matière et s'adapte à notre contexte national unique.

Je vous invite donc à vous engager pleinement dans la mise en œuvre de cette stratégie, qui constitue un document de référence pour notre action collective en matière de cybersécurité.

Je vous remercie

Gbota GWALIBA,
Directeur Général de l'ANCy

Organigramme du comité stratégique

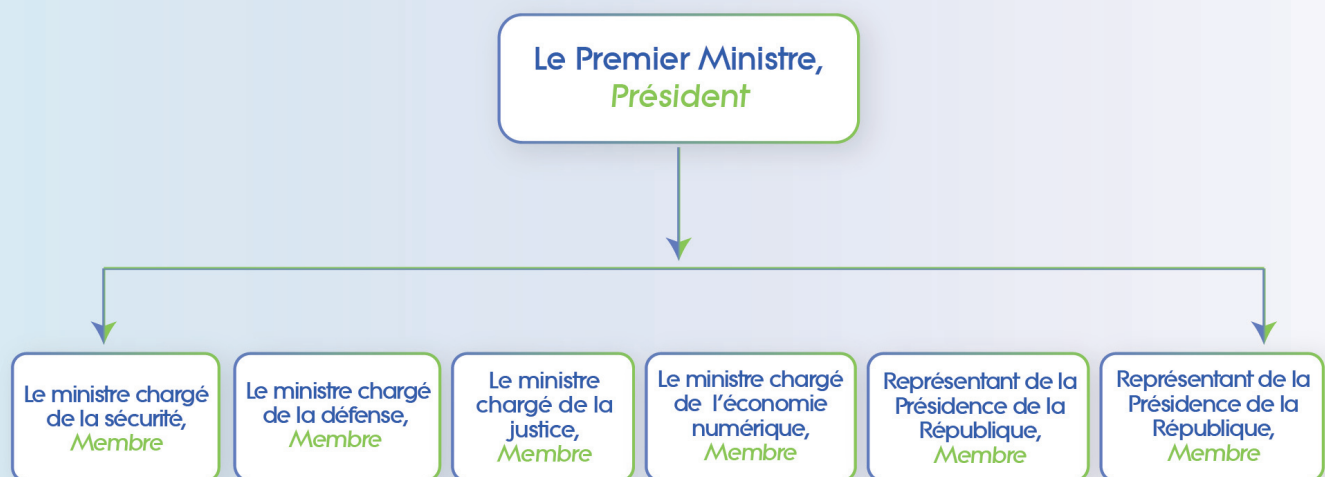


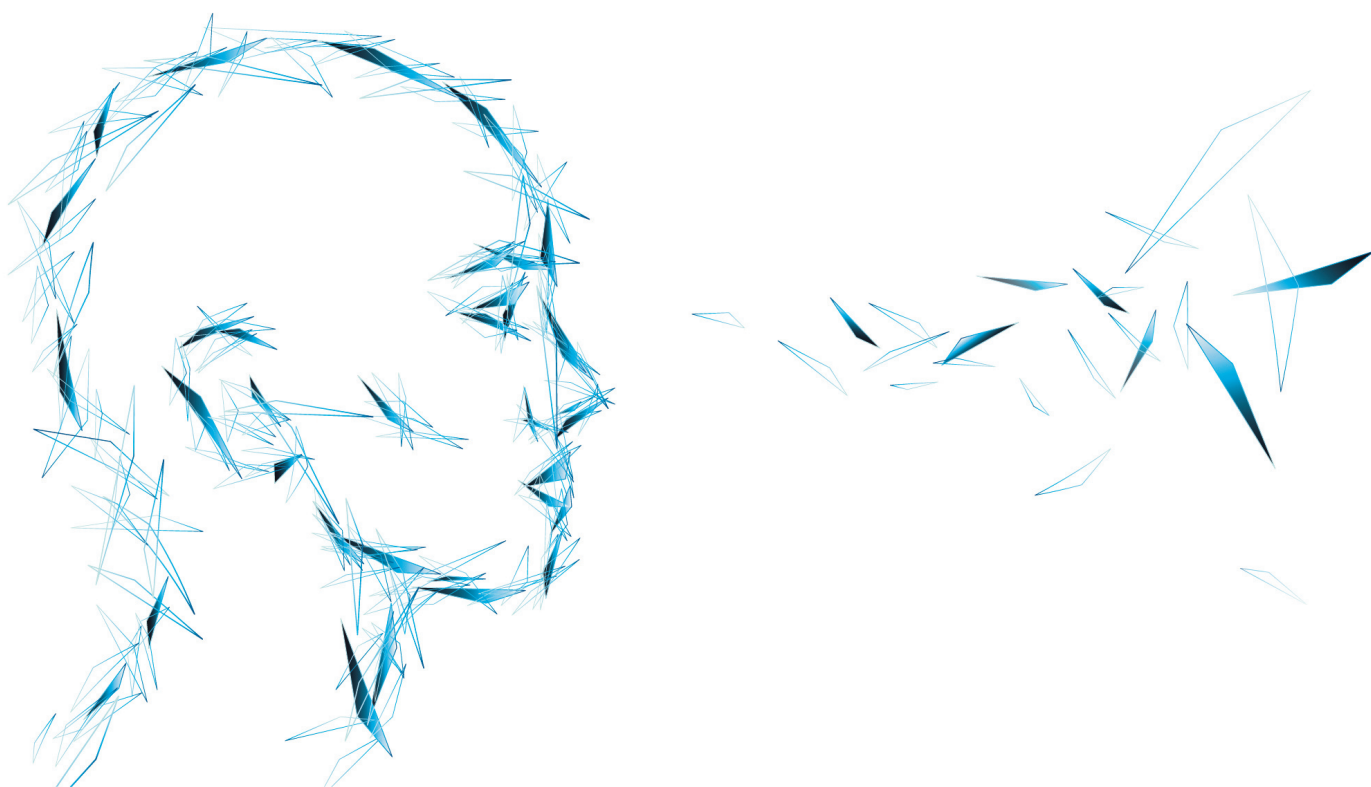
Table des matières

Résumé analytique	15
Introduction	17
1. Evaluation du contexte stratégique national	19
1.1. Le Togo, hub logistique et financier régional	19
1.2. Togo digital ou l'élan de la digitalisation du pays	22
1.3. Paysage des cybermenaces au Togo	23
1.4. Contexte stratégique de la cybersécurité	25
1.5. Cadre légal et réglementaire de la cybersécurité	26
1.6. L'Agence Nationale de la Cybersécurité (ANCy)	27
1.7. Cyber Defense Africa (CDA)	30
1.8. Répartition des rôles entre l'ANCy et CDA pour une cybersécurité nationale efficace	31
1.9. Les services du CERT.tg et du SOC National	33
2. Forces, Faiblesses, Opportunités, Menaces (FFOM)	35
2.1. Les principales forces du Togo en faveur de la stratégie de cybersécurité	38
2.1.1. L'implication des plus hautes autorités de l'Etat	38
2.1.2. Le cadre légal et réglementaire	39
2.1.3. Un cadre opérationnel innovant et à la mesure des enjeux	39
2.1.4. Le financement des activités de cybersécurité	40
2.1.5. La collaboration de tous les acteurs nationaux	41
2.1.6. La coopération internationale	41
2.1.7. Le Partenariat Public-Privé pour la cybersécurité opérationnelle	42
2.2. Les principales faiblesses de la stratégie nationale de cybersécurité	43
2.2.1. Faible niveau de maturité en cybersécurité	43
2.2.2. Pénurie de compétences en cybersécurité	43
2.2.3. Des services essentiels insuffisamment sécurisés	44
2.2.4. La poursuite peu effective des crimes et délits de cybersécurité	44
2.2.5. Une enveloppe budgétaire encore limitée	44
2.3. Les principales opportunités en faveur de la stratégie nationale de cybersécurité	45
2.3.1. L'élan de la digitalisation du Togo	45
2.3.2. La réponse africaine et mondiale aux cybermenaces	45
2.3.3. Une population jeune avec une appétence pour l'apprentissage	47
2.3.4. Une économie croissante	47
2.4. Les principales menaces contre la stratégie de cybersécurité	48
2.4.1. Le cyberspace : un espace sans frontières	48
2.4.2. Un monde en constante évolution	49
2.4.3. La cybercriminalité régionale	49
2.4.4. Crise économique réduisant les capacités de mobilisation de ressources	50
3. La stratégie nationale de cybersécurité	51
4. Orientations de la stratégie de cybersécurité	55
4.1. Pilier 1 : promotion d'une culture de la cybersécurité des populations et développement des compétences techniques nationales	55

4.1.1.	Intégrer l'enseignement de la cybersécurité dans le primaire et le secondaire	56
4.1.2.	Intégrer l'enseignement de la cybersécurité dans l'enseignement professionnel supérieur	58
4.1.3.	Mettre en œuvre un programme de sensibilisation	60
4.2.	Pilier 2 : promotion continue de la sécurité des systèmes d'information de l'administration, des opérateurs de services essentiels et de l'économie numérique	63
4.2.1.	Mettre en œuvre les dispositions législatives et réglementaires, et déterminer le cadre institutionnel	63
4.2.2.	Définir les normes et les règles de sécurité	66
4.2.3.	Encourager les investissements dans la cybersécurité	68
4.3.	Pilier 3 : renforcement du système de réponse aux incidents de cybersécurité	70
4.3.1.	Mettre en place un système national de réaction aux incidents de cybersécurité efficace	71
4.3.2.	Mettre en place un système efficace de réaction aux incidents de cybersécurité au niveau international	73
4.4.	Pilier 4 : renforcement des mécanismes de poursuite efficace des crimes et délits de cybersécurité	75
4.4.1.	Définir les règles pour la collecte de preuves numériques	75
4.4.2.	Créer une entité unique en charge de la lutte contre la cybercriminalité	77
4.4.3.	Mettre en œuvre le droit pénal de la cybersécurité	79
5.	Gestion de la stratégie nationale de cybersécurité	81
5.1.	Mécanismes institutionnels de pilotage, de coordination et d'exécution de la stratégie nationale de cybersécurité 2024-2028	81
5.2.	Instruments de planification et de mise en œuvre de la stratégie nationale de cybersécurité 2024-2028	85
5.3.	Facteurs de risques de la stratégie nationale de cybersécurité 2024-2028	86
6.	Financement de la stratégie nationale de cybersécurité	87
7.	Cadre de suivi et d'évaluation de la stratégie nationale de cybersécurité	89
7.1.	Mécanismes du suivi de la stratégie nationale de cybersécurité 2024-2028	89
7.2.	Mécanismes d'évaluation de la stratégie nationale de cybersécurité 2024-2028	90
Annexes		91
Annexe 1 – Cadre légal et réglementaire relatif à la cybersécurité du Togo		91
1)	Communications électroniques	91
2)	Transactions électroniques	91
3)	Société de l'information	92
4)	Cybersécurité	92
5)	Protection des données à caractère personnel	93
Annexe 2 – Cadre logique de la stratégie par pilier		93

Glossaire

ADS	Asseco Data Systems
AfricaCERT	Africa Computer Emergency Response Team
AFRIPOL	African Union Mechanism for Police Cooperation
AIGE	Aéroport International Gnassingbé Eyadema
ANCy	Agence Nationale de la Cybersécurité
APT	Advanced Persistent Threat
ARCEP	Autorité de Régulation des Communications Électroniques et des Postes
ATD	Agence Togo Digital
CDA	Cyber Defense Africa
CEDEAO	Communauté Economique des Etats de l'Afrique de l'Ouest
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ENISA	European Union Agency for Cybersecurity
FFOM	Forces Faiblesses Opportunités Menaces
FIRST	Forum of Incident Response and Security Teams
GFCE	Global Forum on Cyber Expertise
IPDCP	Instance de Protection des Données à Caractère Personnel
ISOC	Information Security Operations Center
LCE	Lois sur les Communications Électroniques
MENTD	Ministère de l'Economie Numérique et de la Transformation Digitale
NIST	National Institute of Standards and Technology
OCWAR-C	West African Response on Cybersecurity and fight against Cybercrime
OSE	Opérateur de Services Essentiels
OT	Operational Technologies
PAL	Port Autonome de Lomé
PPP	Partenariat Public-Privé
PSO	Plan de Sécurité d'Opérateur
SI	Systèmes d'Information
SOC	Security Operation Center
TF-CSIRT	Task Force - Computer Security Incident Response Team
TI	Technologies de l'Information
TIC	Technologies de l'Information et de la Communication
UA	Union Africaine
UEMOA	Union Economique et Monétaire Ouest-Africaine
SNCy	Stratégie Nationale de Cybersécurité



I Objectif et Vision

Le Togo est en pleine transition, avec une croissance remarquée du numérique dans les administrations, l'économie et la vie quotidienne des citoyens. Par ricochet, cette croissance expose le pays à une multitude de risques et menaces du fait de la cybercriminalité également en pleine croissance (fraudes, vols de données, chantage, rançongiciels). Face à cette situation, la protection et la sécurité des systèmes d'information et des infrastructures critiques de l'Etat deviennent une exigence d'ordre national, d'où la nécessité d'élaborer une stratégie nationale de protection du cyberspace du Togo.

L'objectif de cette stratégie nationale de cybersécurité est de faire du Togo un leader régional en cybersécurité, reconnu comme tel à l'échelle mondiale et contribuant activement et positivement à la communauté internationale de la cybersécurité.

Cette stratégie de cybersécurité vise à instaurer la confiance dans l'utilisation du numérique afin de stimuler la croissance et favoriser l'émergence de nouveaux marchés au profit des citoyens, des investisseurs nationaux et internationaux. Elle a pour objet de garantir la sécurité, la stabilité, la continuité, la résilience des infrastructures et des services digitaux essentiels, de promouvoir le développement des compétences et des emplois qualifiés au Togo en matière de cybersécurité. Elle doit enfin permettre aux citoyens de tirer profit des opportunités offertes par le monde virtuel en parfaite connaissance des dangers et risques auxquels ils sont exposés.

Résumé analytique

Le secteur de l'économie numérique est en pleine croissance au Togo. Les taux de pénétration du mobile sont à la hausse : 77,6% au second trimestre 2021, l'accès à Internet s'améliore : un taux de pénétration data fixe et mobile de 66,86% au second trimestre 2021, les paiements mobiles gagnent en popularité. Cette croissance a été favorisée par les efforts du gouvernement qui s'est engagé à stimuler l'expansion rapide des réseaux mobiles à haut débit et fixes à travers tout le pays, notamment avec la réception du câble sous-marin Equiano de Google qui fait passer le nombre de câbles sous-marins à trois (03). Grâce à ces innovations, les citoyens togolais bénéficient davantage d'opportunités offertes par l'économie numérique telles que de meilleures communications, un meilleur accès à l'information en ligne et de nouvelles opportunités pour le commerce électronique, l'augmentation des services digitaux proposés à la population togolaise à travers les programmes sociaux ou sanitaires tels que Novissi ou la plateforme de gestion des voyageurs et la plateforme de suivi des vaccinations pour lutter contre la Covid-19.

Paradoxalement, partout dans le monde, la croissance de l'économie numérique a eu comme conséquence, la croissance de la cybercriminalité. Le Togo doit donc, à l'instar des autres Etats à travers le monde, être prêt à faire face aux cybermenaces afin de favoriser la stabilité et la confiance des citoyens ainsi que celle des investisseurs nationaux comme internationaux aux services numériques.

Conscient de cette urgence, le gouvernement togolais s'est pleinement engagé depuis 2018 sur la voie de la sécurisation de son cyberspace pour protéger les citoyens, les entreprises, les institutions publiques et les infrastructures critiques contre la cybercriminalité, à travers le renforcement rapide des cadres législatifs, réglementaires et opérationnels, garantissant ainsi, la souveraineté numérique nationale et la protection des données des citoyens.

L'objectif du Gouvernement Togolais, est de faire du Togo un leader régional en cybersécurité, reconnu comme tel à l'échelle mondiale et contribuant activement et positivement à la communauté internationale de la cybersécurité.

Dans cette optique, les quatre (04) objectifs stratégiques développés dans ce document de stratégie nationale de cybersécurité ont pour but de développer un écosystème performant de la cybersécurité et de lutte contre la cybercriminalité basée sur les compétences locales.

En appliquant la stratégie décrite dans ce document, la vision des autorités nationales compétentes, est de favoriser le développement économique des emplois qualifiés et le positionnement du Togo au premier plan de l'économie du savoir en assurant la sécurité de son cyberspace, la stabilité et la continuité des services digitaux essentiels et la confiance des citoyens et des investisseurs nationaux comme étrangers dans la capacité du pays à faire efficacement face aux cybermenaces.

¹ Novissi : programme de transferts monétaires mis en place par l'État Togolais, visant à soutenir les personnes et les familles les plus vulnérables qui ont perdu leur revenu en raison de l'adoption des mesures de riposte contre le Coronavirus.



Introduction

L'accès rapide à une information fiable et utilisable dans la production et la gestion des services, tant dans le secteur public que privé participe au développement économique, social et à la préservation de la sécurité et de la stabilité nationale. Dans le cadre de l'accélération de la modernisation et de la numérisation des services publics et de l'économie, la cybersécurité se positionne désormais au rang des priorités nationales.

La Déclaration de Politique Générale présentée par le Premier ministre confirme la priorité faite à la numérisation, car sur les 42 projets et réformes importants de la feuille de route gouvernementale 2020-2025, $\frac{3}{4}$ sont liés aux questions digitales dont, entre autres, l'identité numérique, la numérisation de l'administration, l'utilisation de la biométrie et la création d'une banque de données digitale pour toutes les couches de la société togolaise.

Les changements sociaux et technologiques dynamiques imposent d'accroître la protection des ressources numériques ce qui devrait encourager les investissements dans les nouvelles technologies numériques et accélérer le développement social et économique du pays. Les technologies numériques façonnent les relations sociales. Les services sur Internet sont devenus un outil d'influence du comportement des groupes sociaux ainsi que de la sphère politique. Toute perturbation importante du fonctionnement des technologies numériques, qu'elle soit mondiale ou locale, aura une incidence sur la sécurité des transactions économiques, le sentiment de sécurité des citoyens, l'efficacité des institutions du secteur public, des processus de production et de services et, par conséquent, sur la sécurité nationale en général.

Les menaces sur le cyberspace n'ayant aucune barrière géographique, les activités de cybersécurité exigent une forte coopération internationale. Conscient de cette nécessité, la présence du Togo tant au sein des instances régionales qu'internationales est très perceptible, telles que la CEDEAO et son initiative "Organised Crime : West African Response on Cybersecurity and fight against Cybercrime (OCWAR-C)", de même que la ratification de la convention de l'Union Africaine sur la cybersécurité et la Protection des Données à Caractère Personnel dite convention de Malabo.

La protection nationale des systèmes d'information et des données traitées constitue un défi majeur pour tous les acteurs nationaux impliqués, tels que les pouvoirs publics, les autorités nationales de sécurité, les entités spécialisées et dédiées au traitement de la cybersécurité, en l'occurrence l'Agence Nationale de la Cybersécurité (ANCy) et Cyber Defense Africa (CDA), ainsi que tous les opérateurs publics ou privés qui fournissent des services essentiels par l'intermédiaire de systèmes d'information.

La pandémie de COVID-19 a favorisé l'accroissement de l'utilisation de services digitaux, à distance, renforçant ainsi le besoin de sécurisation des systèmes d'information, des transactions numériques et des données à caractère personnel. Enfin, la cybersécurité constitue une nouvelle dimension de la sécurité nationale et de la souveraineté, qu'il s'agisse notamment de l'organisation d'élections de façon sécurisée et sans interférences, de la protection des infrastructures essentielles du pays contre des attaques malveillantes, ou d'autres déstabilisations rendues possibles par les technologies de l'information et de la communication.

Le présent document a pour ambition de définir et orienter les stratégies, adopter les mesures politiques, réglementaires et opérationnelles permettant de protéger les citoyens et d'offrir un niveau de sécurisation optimal des systèmes d'information de l'écosystème numérique national, notamment :

- les administrations publiques et les services de l'Etat ;
- les opérateurs de services essentiels ;
- les exploitants d'infrastructures essentielles ;
- les autres acteurs clés dans les secteurs sensibles.

1.

Evaluation du contexte stratégique national

1.1

Le Togo, hub logistique et financier régional

Situé le long du Golfe de Guinée, en Afrique de l'Ouest, le Togo couvre une superficie de 56 785 km² et est limité au Nord par le Burkina Faso, à l'Est par le Bénin, au Sud par l'océan Atlantique, et à l'Ouest par le Ghana.

Le Togo compte 8,3 millions d'habitants, dont 1,9 millions à Lomé, sa capitale et 43% vivant dans les autres zones urbaines. La population togolaise est jeune : l'âge médian est de 20 ans et 70% de la population a moins de 35 ans. Le pays compte 6,5 millions d'abonnés en téléphonie mobile (taux de pénétration de 77%) et environ 3 millions d'abonnés internet mobile et fixe (taux de pénétration de 43%) .

La situation stratégique du Togo ainsi que son appartenance aux zones économiques de la CEDEAO et de l'UEMOA, font du pays une porte d'entrée idéale sur le marché ouest-africain en plein essor, caractérisé par une population de plus de 350 millions d'habitants en forte progression et des revenus en hausse.

Au cours des dix dernières années, le Togo a consenti des investissements considérables pour développer des infrastructures de premier ordre. Il a, par ailleurs, entrepris des réformes structurelles pour soutenir le développement d'un secteur privé prospère et est devenu, de ce fait, une destination privilégiée pour les investissements. Ces efforts se sont traduits par une croissance soutenue de ses activités portuaires et par des progrès réalisés dans l'amélioration du climat des affaires ; ce qui lui a valu d'être classé au 3ème rang parmi les 10 premiers pays les plus réformateurs au monde et au 1er rang africain selon le classement annuel 2020 du Doing Business, publié par la Banque Mondiale. Pour atteindre son objectif

de devenir un pays à revenus intermédiaires, le Togo accélère sa transformation économique en facilitant les investissements directs étrangers dans les secteurs prioritaires avec pour ambition principale de renforcer sa position de hub logistique en Afrique de l'ouest afin de devenir un important pôle agricole et industriel.

En 2019, les services centrés autour du commerce, de l'activité portuaire, aéroportuaire et bancaire ont contribué de moitié à son PIB, soit 49,9% .

Le Port Autonome de Lomé est le seul port en eau profonde de la côte ouest africaine pouvant accueillir des navires de 3ème génération, avec une profondeur naturelle de 16,60 mètres. Cela lui permet d'être en avance sur ses concurrents de la sous-région, avec un volume de trafic de conteneurs de 1,2 million d'Équivalents Vingt Pieds (EVP) enregistré .

L'Aéroport International de Lomé a déjà atteint la moitié de sa capacité avec 1 million de passagers par an (avant COVID-19) et connecte plusieurs villes dans le monde entier. Il sert de hub à la compagnie aérienne régionale de l'Afrique de l'Ouest, Askya, et à son partenaire Ethiopian Airlines qui desservent 26 villes en liaison directe de Lomé.

En plus d'être un hub logistique régional, le Togo est également un hub commercial (le marché de Lomé a un rayonnement international) ainsi qu'un hub financier, avec un certain nombre d'établissements financiers régionaux de premier plan ayant choisi le Togo pour y établir leur siège notamment Ecobank, Oragroup.

² Source ARCEP : évolution des marchés régulés : postes et communications électroniques – rapport 2019

³ <https://www.tresor.economie.gouv.fr/Pays/TG/conjoncture>

⁴ <https://www.togo-port.net/presentation-pal/atouts-port-lome/>



1.2

Togo digital ou l'élan de la digitalisation du pays

Le Gouvernement Togolais a pour ambition de faire de la numérisation de la société togolaise, une de ses priorités, avec des projets d'envergure nationale tels que l'attribution de l'identité pour tous, la mise en place d'un registre social unique des personnes et ménages, la digitalisation des services publics, et la création d'une banque digitale pour tous.

Cet élan digital, dont l'objectif stratégique est d'offrir au pays un développement inclusif de la société et de l'économie, passe par une démocratisation de l'accès à internet. Pour soutenir cette digitalisation, le Togo peut s'appuyer sur des opérateurs de télécommunication solides et une infrastructure importante qui doit encore être déployée sur toute l'étendue du territoire national. Cette digitalisation touchera l'ensemble des citoyens togolais, donnera un accès plus large aux publics d'individus et d'entreprises, passera par de nouveaux outils et de nouvelles organisations de travail et concernera des informations sensibles sur toute la population. Il devient impérieux que ces données soient sécurisées, accessibles et filtrées uniquement à ceux qui ont le droit d'y accéder selon le strict besoin de leur fonction. La Confidentialité, l'Intégrité, la Crédibilité sont essentielles.

La création de l'Agence Togo Digital, de l'Agence Nationale pour l'Identification et de la Société des Infrastructures Numériques vient renforcer cet élan de digitalisation.

1.3

Paysage des cybermenaces au Togo

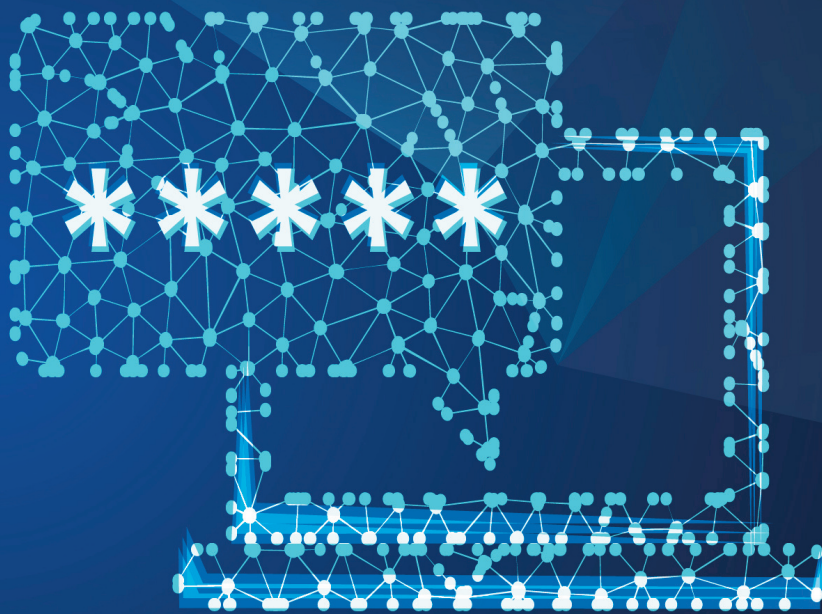
Le Togo compte six (06) opérateurs de communications électroniques : deux (02) fournisseurs de services d'accès à Internet via le mobile (Togocom et Moov Africa Togo) et quatre (04) fournisseurs de services d'accès à Internet fixe (Togocom, CAFE Informatique & Télécommunication, Téolis et Groupe Vivendi Africa Togo (GVA). L'adoption d'internet est plus rapide via le mobile avec plus de 5 millions d'abonnés en 2021 contre un peu plus de 54 000 pour l'internet fixe .

C'est donc sans surprise que les virus et trojans pour équipements mobiles sont les plus détectés au Togo, notamment les malwares visant les équipements opérant le système d'exploitation Android tels que Hummer, Backdoor prizmes, ou encore Rootnik. Ces malwares prennent le contrôle total de l'équipement, principalement pour perturber l'utilisation du propriétaire en faisant apparaître des publicités de façon intempestive ou en installant des applications non désirées. Ils sont également utilisés pour collecter des informations sur l'équipement infecté (captures d'écrans, collecte des saisies claviers, etc.).

D'autres types de cyberattaques tels que l'hameçonnage, les ransomwares, les coin miners, les attaques par rebond, les attaques DDoS, les campagnes de spams sont également détectées sur les équipements vulnérables. Les équipements au Togo sont, soit attaqués directement, soit utilisés comme vecteurs d'attaques envers d'autres destinations. Ce qui a pour conséquence d'entacher la réputation des adresses IPs provenant du Togo sur Internet. La non-application des mesures minimales de sécurité, l'utilisation de logiciels piratés vecteurs de virus et de codes malveillants, et le manque de connaissance des pièges liés à l'utilisation des supports numériques, facilitent l'installation et la persistance de ces malwares. Les Opérateurs de Services Essentiels (OSE), les administrations publiques, les services de l'Etat et les grandes entreprises togolaises les plus digitalisés sont les premières victimes de ces attaques.

L'utilisation de moyens numériques pour commettre des fraudes, notamment auprès d'institutions financières, est en croissance. À ce sujet, la création de faux sites web bancaires pour leurrer les utilisateurs et collecter leurs identifiants de connexion, les fraudes impactant les moyens de paiement, sont des attaques que la négligence des utilisateurs rend plus facile et plus lucrative. Ces attaques ont des

⁵ Source ARCEP : Observatoire du marché des communications électroniques, Tableau de bord au second Trimestre 2021



conséquences financières directes, affectent la réputation des banques et provoquent une perte de confiance des clients, avec un impact potentiel réel sur la croissance économique du pays à moyen terme.

Les réseaux sociaux les plus utilisés par les togolais servent de support à la généralisation de campagnes d'escroqueries en ligne en falsifiant les comptes de personnalités publiques et membres du gouvernement, de fausses promesses de bourses d'études, de visas, d'embauches, propagation de fake news, etc. Ces nouveaux canaux informationnels facilitent la fraude en ligne en ciblant les togolais les moins conscients des cybermenaces et les plus vulnérables aux cyberattaques. Ces menaces sont exacerbées par le facteur global du cyberspace et l'internationalisation du paiement par mobile money. Les fraudeurs se positionnent géographiquement dans les pays voisins pour perpétrer des attaques ciblant des togolais tout en s'assurant de collecter les gains via les mobiles money internationaux. A l'inverse d'autres groupes de cybercriminels basés au Togo s'adonnent à des escroqueries en ligne dans les pays voisins.

1.4

Contexte stratégique de la cybersécurité

Compte tenu, d'une part, du contexte stratégique national de la numérisation de la société togolaise, et d'autre part, de la présence permanente des cybermenaces, la cybersécurité figure au rang des priorités nationales.

Une cybersécurité efficace nécessite de s'appuyer sur quelques piliers qui doivent continuellement être renforcés, avec un niveau de qualité systématiquement améliorée. Ces piliers sont :

1. la protection et la défense des systèmes d'information ;
2. la résilience des systèmes d'information face aux cybermenaces ;
3. l'efficacité des services de détection et de répression de la cybercriminalité et des activités hybrides (y compris terroristes) et d'espionnage et le renforcement de la maturité du système judiciaire par rapport aux nouveaux délits et crimes numériques.

La République Togolaise est un membre actif de nombreuses organisations internationales dont celles Africaines, notamment :

- l'Union Africaine (UA) ;
- la Communauté Economique des Etats de l'Afrique de l'Ouest (CEDEAO) ;
- l'Union Economique et Monétaire Ouest Africaine (UEMOA) ;
- SMART Africa.

La République Togolaise est également un membre actif de plusieurs initiatives régionales en faveur de la cybersécurité et de la coopération régionale et africaine en la matière.

a. au niveau de la Communauté Economique des Etats de l'Afrique de l'Ouest (CEDEAO) , l'initiative appelée « West African Response on Cybersecurity and fight against Cybercrime (OCWAR-C) » a permis l'adoption de la stratégie régionale de cybersécurité et de lutte contre la cybercriminalité ainsi que l'adoption de la stratégie régionale de protection des infrastructures critiques.

b. s'agissant de l'Union Africaine (UA), le Togo a ratifié la convention sur la cybersécurité et la protection des données à caractère personnel, ou convention de Malabo, ce qui lui a permis d'être partie prenante à de nombreuses initiatives de la coopération internationale.

1.5

Cadre légal et réglementaire de la cybersécurité

Le gouvernement togolais a amélioré et consolidé le cadre législatif et réglementaire dans le domaine des Technologies de l'Information de la Communication (TIC), notamment en adoptant plusieurs lois permettant :

- la mise en œuvre de la stratégie sectorielle de l'économie numérique ;
- la mise en place des structures de gouvernance nécessaires ;
- la protection des citoyens face aux nouveaux risques et menaces de sécurité, portés par le cyberspace et par l'accès aux nouvelles technologies de l'information.

Il s'agit des lois, décrets et arrêtés suivants :

- loi n°2016-006 du 30 mars 2016 portant liberté d'accès à l'information et à la documentation publique ;
- loi n°2017-007 du 22 juin 2017 relative aux transactions électroniques ;
- loi n°2018-026 du 7 décembre 2018 modifiée par la loi n°2022-009 du 22 juin 2022 du 22 juin 2022 sur la cybersécurité et la lutte contre la cybercriminalité ;
- loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;
- décret n°2017-104 du 30 octobre 2019 relatif aux modalités d'application de la loi n° 2016-06 du 30 mars 2016 portant liberté d'accès à l'information et à la documentation publiques ;
- décret n°2018-062/PR du 21 mars 2018 portant réglementation des transactions et services électroniques au Togo ;
- décret n°2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence Nationale de la Cybersécurité (ANCy) ;
- décret n°2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels (OSE), aux infrastructures essentielles et aux obligations y afférentes ;
- arrêté N° 2022-040 /PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République Togolaise ;
- décret N°2022-090/PR du 25 août 2022 201 relatif à la qualification des prestataires de services de confiance en cybersécurité et des produits de cybersécurité et à l'agrément des centres d'évaluation.

⁶ Informations détaillées figurant à l'Annexe 1

1.6

L'Agence Nationale de la Cybersécurité (ANCy)

Selon l'Article 4 du Décret 2019-022/PR du 13 Février 2019 portant attributions, organisation et fonctionnement de l'Agence Nationale de la Cybersécurité (ANCy), les missions de cette dernière, sont principalement les suivantes :

- Elle apporte son concours aux services de la République togolaise en matière de défense et de sécurité nationale.
- Elle est chargée de la sensibilisation des usagers des équipements, des services et installations informatiques, de la prévention des intrusions, de la sécurisation et de la défense de l'ensemble des systèmes d'information.
- L'Agence Nationale de la Cybersécurité assure, en outre, la coordination de la riposte aux attaques informatiques.
- Elle instruit les demandes de qualification et qualifie les produits de sécurité en cybersécurité et les prestataires de services de confiance pour les besoins de la sécurité des systèmes d'information selon les modalités prévues par voie réglementaire.

UNE STRATÉGIE NATIONALE ...



...POUR UNE
RÉPONSE GLOBALE
AUX MENACES CYBER



1.7

Cyber Defense Africa (CDA)

Conscient des limites nationales en matière de ressources humaines et de financement, le gouvernement a opté pour la mise en place rapide d'un bras opérationnel et technique de l'ANCy chargé de l'analyse, de la réponse et de la remédiation aux cyberattaques. En effet, en 2019, la République Togolaise a conclu un Partenariat Public-Privé (PPP) avec Asseco Data Systems (ADS), une société informatique polonaise de premier plan et sixième producteur de logiciels en Europe, créant une joint-venture appelée Cyber Defense Africa dont la mission est d'apporter l'expertise opérationnelle nécessaire à une protection maximale du cyberspace togolais.

La création de CDA a été une réponse directe au besoin urgent de mettre en place un cadre technique au service des opérateurs de services essentiels et de l'ANCy.

Le partenariat avec Asseco a permis au Togo d'établir un centre d'excellence combinant un CERT (Computer Emergency Response Team) national et un SOC (Security Operations Center), ce qui crée des économies d'échelle et des synergies. Ce partenariat permet non seulement de résoudre le problème de la pénurie de l'expertise locale pour opérer la sécurité du cyberspace mais aussi de développer les capacités locales à gérer les infrastructures de cybersécurité sur le long terme.

Ce PPP est structuré de telle sorte que le CERT soit offert comme un service principalement gratuit au public. Le CERT alerte la population à propos des vulnérabilités et sensibilise le public sur les moyens de se protéger contre les attaques. Le CERT publie également des correctifs sur les vulnérabilités identifiées. Le SOC, quant à lui, est un service payant qui fournit une cybersécurité en tant que service sur mesure destinée aux Opérateurs de Services Essentiels (OSE), aux entreprises, aux institutions publiques et à d'autres parties intéressées par la protection de leurs réseaux informatiques.

Ainsi ce modèle permet de renforcer de façon accélérée les capacités nationales en cybersécurité, à grande échelle et à un coût raisonnable.

Grâce au partenariat en cours avec CDA, des professionnels de la cybersécurité sont formés au Togo et pourront éventuellement travailler au sein d'organisations nationales, régionales, africaines et internationales, conformément à la volonté du Togo d'être un « hub » de l'expertise en cybersécurité dans la sous-région.

Ce n'est plus qu'une question de temps avant que la demande et la recherche des compétences en cybersécurité ne soient très élevées, le Togo veut donc être prêt à fournir cette expertise le moment venu.

1.8

Répartition des rôles entre l'ANCy et CDA pour une cybersécurité nationale efficace

L'ANCy en tant qu'autorité nationale en matière de sécurité des systèmes d'information, régule le cyberspace togolais. L'ANCy coordonne les activités et les relations entre les différents acteurs du secteur, pilote les programmes nationaux de cybersécurité et contrôle l'application des lois et des différents textes du secteur.

L'ANCy surveille et contrôle les services qu'elle délègue à CDA par un contrat de délégation de service contenant des critères de mesures de performances claires et mesurables.

CDA en tant que bras opérationnel de l'ANCy est en charge :

- d'opérer le CERT National, le CERT.tg ;
- d'opérer le SOC National pour le suivi et l'accompagnement de la sécurisation des Opérateurs de Services Essentiels ;
- de la sensibilisation des usagers des équipements, des services et installations informatiques ;
- de la prévention des intrusions, de la sécurisation et de la défense de l'ensemble des systèmes d'information ;
- de la coordination de la riposte aux attaques informatiques ;
- du support technique pour le compte de l'ANCy.



1.9

Les services du CERT.tg et du SOC National

Le CERT National est responsable de la fonction générale de surveillance des risques au Togo associés au cyberspace, de la protection de la société civile contre les utilisations malveillantes des outils ou services Internet, ainsi que des réponses à apporter aux attaques qui peuvent se produire. L'équipe du CERT fournit ces services gratuitement 24 heures sur 24 et 7 jours sur 7 au gouvernement togolais, au grand public et à toute autre organisation au Togo. À cet égard, il est notamment chargé :

- d'analyser les données sur les menaces dans le cyberspace togolais selon les informations recueillies auprès de la population togolaise, des entreprises, administrations et autres organisations togolaises ainsi que de la communauté mondiale des CERT et CSIRT ;
- de traiter, répondre et coordonner les incidents de cybersécurité nationaux ;
- de recevoir les menaces détectées et communiquées par les citoyens togolais au centre d'appel, par courrier électronique et sur le site web ;
- d'annoncer les intrusions, les vulnérabilités et publier les bulletins de sécurité ;
- de faire une analyse avancée des logiciels malveillants au niveau national et/ou international ;
- de produire des rapports sur les tendances des cyberattaques et leur impact potentiel sur le pays ;
- d'organiser des formations en cybersécurité et des campagnes de sensibilisation à l'endroit du grand public, les écoles, les universités, etc. ;
- de faire des audits de sécurité et délivrer de certificats sous la supervision de l'ANCy ;
- de participer et contribuer à des études techniques spécifiques ou à des projets de recherches et développements sur la cybersécurité ;
- de participer à l'élaboration de normes de cybersécurité dans tout le pays.

En revanche, l'équipe du SOC fournit des services payants aux opérateurs de services essentiels et à toutes autres organisations souhaitant bénéficier de services de protection proactive en cybersécurité. Elle se consacre à la sécurité des entreprises qu'elle protège et utilise le soutien et les services de l'équipe CERT lorsque cela est nécessaire. Le SOC fonctionne comme une société de services en cybersécurité avec des prestations de type services managés « SOC as a Service ».

Il s'agit entre autres de :

- l'administration et de la maintenance de l'infrastructure SIEM (Security Information & Event Management) national ou du site de chaque organisme bénéficiant des services SOC ;
- de la surveillance sur mesure des événements de sécurité 24 heures sur 24 et 7 jours sur 7 ;
- de la détection et de l'identification des menaces et des attaques ciblées ;
- de la réponse aux menaces et mesures correctives (en collaboration avec l'équipe CERT) ;
- de l'assistance dans le processus de correction et de rétablissement du système d'information (en collaboration avec l'équipe CERT) ;
- de l'analyse ciblée des logiciels malveillants (en collaboration avec l'équipe CERT) ;
- de l'analyse et la gestion des vulnérabilités inhérentes à l'organisme protégé ;
- de la rédaction des rapports périodiques.

L'équipe SOC délivre également d'autres prestations nécessaires à la sécurisation des systèmes d'information des organismes protégés, en l'occurrence :

- Conseil en cybersécurité (rédaction de politiques de sécurité des systèmes d'informations, réalisation de cartographies, etc.) ;
- Formations avancées en cybersécurité ;
- Intégration de solutions de cybersécurité ;
- Audits et tests d'intrusions.



2. Forces, Faiblesses, Opportunités, Menaces (FFOM)

Le but de la stratégie de développement de la Cybersécurité du Togo, étant de mettre en œuvre les moyens nécessaires pour maîtriser les risques liés à la sécurité des systèmes d'information au Togo, il est nécessaire de faire un diagnostic des forces et des faiblesses, ainsi que les opportunités et les menaces de l'environnement cyber national afin de donner de réelles chances de réussite à l'ambition de mettre en œuvre une cybersécurité effective de haut niveau, qui soit en mesure de répondre à sa volonté de devenir un leader régional en cybersécurité, reconnu comme tel à l'échelle mondiale et contribuant activement et positivement à la communauté internationale de la cybersécurité.

FORCES



1. Forte implication des plus hautes autorités de l'Etat
2. Cadre légal et réglementaire pertinent
3. Cadre opérationnel innovant et à la mesure des enjeux
4. Financement des activités de cybersécurité
5. Collaboration de tous les acteurs nationaux
6. Coopération internationale
7. Partenariat Public-Privé pour la cybersécurité opérationnelle.

OPPORTUNITES



1. Élan de la digitalisation du Togo
2. Réponse africaine et mondiale aux cybermenaces
3. Population jeune avec une appétence pour l'apprentissage
4. Économie croissante



FAIBLESSES

1. Faible niveau de maturité en cybersécurité
2. Pénurie de compétences en cybersécurité
3. Services essentiels insuffisamment sécurisés
4. Vulnérabilité des applications déployées
5. Poursuite peu effective des crimes et délits de cybersécurité
6. Enveloppe budgétaire encore limitée



MENACES

1. Cyberspace : un espace sans frontières
2. Monde en constante évolution
3. Cybercriminalité régionale
4. Difficultés de mobilisations de ressources internes et externes liées aux crises et conflits sécuritaires

Le gouvernement togolais conscient des différentes contraintes extérieures qui peuvent influencer sur la réalisation des objectifs stratégiques de cybersécurité et de la nécessité de mener une action à la fois forte, rapide et concertée, est déterminé à mettre en œuvre un environnement de confiance fiable permettant de vulgariser les bonnes pratiques de cybersécurité à l'ensemble des acteurs concernés, que ce soit les différentes administrations publiques entre elles ou celles-ci avec les acteurs du secteur commercial, notamment les opérateurs de services essentiels.

2.1

Les principales forces du Togo en faveur de la stratégie de cybersécurité

2.1.1.

L'implication des plus hautes autorités de l'Etat

L'implication et le leadership du Président de la République, du Premier Ministre et des Ministres concernés par la transformation numérique de la société togolaise, en tenant compte de la cybersécurité nationale qui l'accompagne, est le principal gage de la réussite de la stratégie nationale de numérisation de la société et de son économie.

Cette forte volonté politique a permis de mettre en œuvre en un temps record, la réglementation nationale sur la cybersécurité et l'accord de Partenariat Public-Privé entre la République togolaise et Asseco Data Systems et le cadre opérationnel de la cybersécurité.

En effet, sont ainsi opérationnels :

- L'Agence Nationale de Cybersécurité (ANCy) ;
- Cyber Defense Africa S.A.S (CDA)
- Le CERT national (CERT.tg) ;
- Le SOC national ;
- Une équipe de spécialistes togolais pour assister les OSE.

L'engagement de tous les acteurs de la cybersécurité nationale sous le leadership du Chef de l'Etat permet une action opérationnelle optimale et un contrôle bien encadré.

2.1.2.

Le cadre légal et réglementaire

Le cadre légal et réglementaire mis en place au Togo incite les acteurs à renforcer leur posture de cybersécurité et de protection des données à caractère personnel et prévoit un ensemble de sanctions susceptibles de démotiver et de décourager les comportements déstabilisant la confiance dans la société et l'économie numérique. Ce facteur incite les citoyens, les entreprises et la société dans son ensemble à se conformer à la réglementation.

Il fixe un cadre encourageant la sensibilisation du public et attire l'attention du public sur les comportements à risque qui les expose quotidiennement aux cybermenaces. Tous ces mécanismes concourent à un changement de comportements sociaux avec une continuelle réduction du nombre, de la sévérité et de l'impact des cyberattaques qui ont lieu au Togo.

L'établissement de réglementations et de normes sociales ainsi que l'application de la loi, constituent un facteur important de la mise en œuvre d'une cybersécurité réussie.

2.1.3.

Un cadre opérationnel innovant et à la mesure des enjeux

La cybersécurité nationale est subdivisée en deux niveaux de fonctions :

1. Les fonctions de régulation, de suivi de la stratégie nationale de la cybersécurité, et de contrôle de l'application de la cybersécurité opérationnelle conformément à la réglementation nationale ;
2. Les fonctions opérationnelles de la mise en œuvre de la cybersécurité nationale.

La séparation de ces deux niveaux de fonctions permet de s'assurer d'une meilleure réussite de la cybersécurité nationale. C'est la décision qu'a prise le gouvernement togolais en décidant de confier la mise en œuvre de la politique nationale de cybersécurité à deux structures organisationnelles différentes : l'ANCy et CDA.

L'ANCy en sa qualité d'autorité nationale, dispose de l'ancrage institutionnelle nécessaire pour la réalisation de ses missions de régulation et de contrôle du secteur de la cybersécurité. CDA issu du partenariat public-privé, au-delà de son rôle de bras technique et opérationnel de l'ANCy, dispose de compétences et d'un fonctionnement plus en adéquation avec le secteur privé, ce qui lui permet de délivrer à ce secteur le service opérationnel dont il a besoin.

2.1.4.

Le financement des activités de cybersécurité

La mise en place d'une SAS en Partenariat Public-Privé en charge de la protection proactive de l'administration, des institutions de l'Etat, des opérateurs de services essentiels et des citoyens permet d'optimiser le financement et les dépenses liées à la cybersécurité.

CDA opère à la fois le CERT national et le SOC national, ce qui crée des synergies entre les ressources CERT et SOC, et génère des économies de coûts.

Au travers du SOC national, CDA offre des services de sécurité managés (appelé également infogérance) aux entreprises togolaises. Cela permet aux entreprises de confier en partie ou en totalité, la sécurité de leur système d'information au SOC national. Les entreprises gagnent à la fois en coûts, en temps et en fiabilité. La mise en place d'un système de sécurité en interne et à la hauteur des attaques les plus sérieuses demande un investissement important, tant en matériel qu'en personnel. Avec les services managés proposés par CDA, les entreprises togolaises peuvent bénéficier d'une sécurité plus qualitative à moindre coût. Elles bénéficient aussi de la garantie de la sécurisation de leur système d'information par une société nationale audité et contrôlée par l'ANCy.

Les revenus générés par ces services aux entreprises permettent de minimiser le financement par l'Etat des activités d'utilité publiques telles que le CERT national, le SOC aux administrations publiques, la formation des fonctionnaires, les campagnes de sensibilisations et d'autres activités connexes.

2.1.5.

La collaboration de tous les acteurs nationaux

Trop souvent, les dirigeants d'entreprises et de pays considèrent à tort que la cybersécurité concerne exclusivement les spécialistes informatiques ou les experts en cybersécurité. Cette compréhension réductrice de la cybersécurité offre de beaux jours à la cybercriminalité.

L'organisation d'une cyberattaque exploite aussi bien les vulnérabilités ou défaillances informatiques qu'humaines ou organisationnelles. La cybersécurité concerne tout le monde, utilisateurs, spécialistes de la communication, juristes, personnel des services de sécurité, dirigeants, informaticiens, etc.

Les autorités togolaises l'ont bien compris, en plaçant l'Agence Nationale de la Cybersécurité sous la tutelle technique et administrative du ministère de la sécurité et du ministère de l'économie numérique. Mais bien plus encore, l'agence est administrée par un comité stratégique présidé par le Premier Ministre, composé du Ministre chargé de la Sécurité, du Ministre chargé des Armées, du Ministre chargé de la Justice, du Ministre chargé de l'Economie Numérique et de deux représentants de la Présidence de la République.

CDA, l'organisme chargé de la cybersécurité nationale opérationnelle est sous la tutelle du ministère de la sécurité et de la protection civile, du ministère des armées, du ministère de l'économie numérique et de la transformation digitale et du ministère de l'économie et des finances.

2.1.6.

La coopération internationale

La coopération internationale en cybersécurité, est un élément primordial de la réussite de la sécurisation du cyberspace national. Elle est fondée sur les échanges de données, d'informations et d'expériences, concernant les menaces et les réponses, les meilleures pratiques. Il s'agit également d'une prise de conscience collective des problématiques de cybersécurité et de l'alignement des pays sur des normes et standards communs. En ce sens, le Togo a ratifié la convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel et a adopté dans le cadre du projet « Organised Crime : West African Response on Cybersecurity and fight against Cybercrime (OCWAR-C) » la stratégie régionale de cybersécurité et de lutte contre la cybercriminalité ainsi que la stratégie régionale de protection des infrastructures critiques.

Sur le plan opérationnel, la coopération internationale permet un enrichissement continu du Togo en informations, particulièrement sur les tendances du secteur. Par ailleurs le cyberspace est le centre d'échanges des données et d'informations entre humains, ce qui implique que la coopération internationale en cybersécurité concerne toutes les activités humaines de sécurité telles que les services de sécurité de la société civile, comprenant les enquêtes informatiques et policières sur le terrain, les services juridiques, les mécanismes de contrôle.

Les équipes de l'ANCy, de CDA et du CERT.tg représentant le Togo, participent activement à la coopération internationale afin de bénéficier des informations reçues de l'étranger, et de disséminer les informations et solutions utiles aux problèmes concrets qui se présentent.

L'entrée du Togo dans la coopération internationale pour la réussite de sa cybersécurité nationale connaît un élan important depuis la mise en activité de CDA. Ainsi, le CERT.tg est membre des réseaux internationaux de CERT comme AfricaCERT, TF-CSIRT et FIRST. Il est aussi dans un partenariat privilégié avec ComCERT, le CERT du groupe Asseco.

Dans le cadre de leur partenariat, l'ANCy et CDA devront impérativement accroître cette activité de coopération internationale en renforçant sa collaboration et sa contribution sur les questions de cybersécurité et en revendiquant sa place dans le cyber-écosystème global.

2.1.7.

Le Partenariat Public-Privé pour la cybersécurité opérationnelle

L'approche Partenariat Public-Privé (PPP) adoptée par la République togolaise pour la création de CDA a permis un renforcement de capacités effectives et efficientes. Bénéficiant ainsi de l'expertise de son partenaire Asseco Data Systems, le Togo s'assure d'un transfert de compétences et de technologies réussi permettant d'assister l'ANCy avec une entité opérationnelle compétente.

Ce partenariat permet non seulement de pallier immédiatement la pénurie d'expertise pour faire fonctionner le cadre technique de défense proactive face aux cybermenaces mais aussi de développer à moyen termes les capacités locales à gérer les infrastructures de cybersécurité. Cette approche permet au Togo de disposer d'une entité capable de délivrer des services de cybersécurité de haute qualité aux organismes publics et aux entreprises privées. CDA a ainsi délivré des formations en cybersécurité sur le plan national aux RSSI de plusieurs OSE et sur le plan régional pour Interpol et OCWAR-C.

2.2

Les principales faiblesses de la stratégie nationale de cybersécurité

2.2.1.

Faible niveau de maturité en cybersécurité

Les cybermenaces se développent rapidement, les cybers attaquants ont atteint un niveau élevé de maturité et s'organisent en groupes pour conjuguer leurs compétences. Leurs actions sont de plus en plus sophistiquées, persistantes et ciblées contre des organisations et des Etats.

La question de la cybersécurité est relativement récente au Togo pour la majorité des institutions et entreprises locales. L'insuffisance de sensibilisation auprès des dirigeants, de la population togolaise en général et le manque de formations spécialisées en cybersécurité, représentent une faiblesse au moment de la montée en puissance de programmes de cybersécurité dans le pays.

Pour atteindre un niveau de maturité suffisant, la montée en compétence des équipes doit être rapide, les actions optimisées, l'ensemble supporté par des budgets suffisants.

2.2.2.

Pénurie de compétences en cybersécurité

Un service opérationnel et effectif de cybersécurité nécessite l'organisation d'équipes de spécialistes sachant s'adapter à un environnement très évolutif et avec de longues années d'expérience dans des compétences diverses.

Le nombre d'experts dans le domaine est largement insuffisant au Togo comme partout en Afrique.

Au Togo, cette pénurie se reflète par une difficulté permanente de recrutement des compétences. Le recrutement dans le domaine passe le plus souvent par l'emploi d'informaticiens qu'il faut former et convertir aux métiers de la cybersécurité, ce qui nécessite un certain temps et des ressources en accompagnement.

2.2.3.

Des services essentiels insuffisamment sécurisés

Au vu du plan ambitieux de digitalisation du pays, de plus en plus de services dits essentiels pour la sécurité publique, la stabilité économique, la sécurité nationale et la stabilité internationale se basent sur des infrastructures numériques. Les opérateurs de ces services doivent prendre conscience de l'impact d'une cyberattaque sur ces infrastructures essentielles et déployer une stratégie globale de cybersécurité basée sur les obligations légales et les risques inhérents à leur secteur. Cette stratégie doit s'accompagner d'un déploiement opérationnel avec une constance dans le temps. Au-delà de ces aspects techniques, la réticence des utilisateurs au changement est un facteur sociologique à prendre en compte.

2.2.4.

La poursuite peu effective des crimes et délits de cybersécurité

Le cyberespace n'a pas de frontières et permet aux cyberattaquants de se cacher de manière efficace en brouillant les pistes. Il est donc difficile de déterminer qui est à l'origine d'une attaque informatique. Cependant, incriminer les pirates est fondamental pour la sécurisation du cyberespace.

Ainsi le cadre légal et réglementaire mis en place au Togo et la coopération internationale, sont des éléments clés pour la poursuite des cybercriminels. Il faut cependant, renforcer les capacités des acteurs de la lutte contre la cybercriminalité en formant les magistrats et les forces de l'ordre à la détection et à la poursuite effective de ces crimes et délits.

2.2.5.

Une enveloppe budgétaire encore limitée

Le Togo a décidé de mettre à contribution toutes ses forces nationales, publiques et privées, pour établir un budget conséquent dédié à la cybersécurité, afin de pouvoir à la fois déployer l'infrastructure matérielle et logicielle nécessaire, et assurer la montée en compétences rapide des équipes et mettre en œuvre, dans les meilleures conditions possibles des actions de sécurité du cyberespace togolais. Malgré les efforts consentis, les budgets restent limités, d'où la nécessité de revoir à la hausse l'enveloppe financière consacrée à cet effet.

2.3

Les principales opportunités en faveur de la stratégie nationale de cybersécurité

2.3.1.

L'élan de la digitalisation du Togo

Dans le contexte stratégique national, l'élan de la digitalisation du Togo développé au point 3.2, constitue une opportunité pour la cybersécurité du pays. Les bases légales, structurelles, organisationnelles mises en place représentent un fort atout pour sa réussite. La mise en œuvre de la digitalisation en même temps que la sécurisation est une formidable opportunité qui permettra au Togo de construire un environnement digital sécurisé.

2.3.2.

La réponse africaine et mondiale aux cybermenaces

Avec la conscience que le cyberspace n'a pas de frontières, la cybersécurité s'organise au niveau africain et mondial. Des structures importantes se créent pour assurer la coordination et la collaboration des pays pour déployer des mesures communes et harmoniser les textes régissant le secteur dans le monde.

A ce titre les travaux et initiatives suivantes, en sont la parfaite illustration :

- Les travaux menés par l'Organisation des Nations Unies, notamment dans le cadre de la Résolution n°74/247, relative à la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles adoptée par son Assemblée Générale le 27 décembre 2019, qui a décidé de l'établissement d'un comité intergouvernemental spécial d'experts ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles ;
- Les travaux menés par l'Union Internationale des Télécommunications, avec notamment le lancement en 2007 d'un cadre de coopération internationale destiné à accroître la confiance et la sécurité dans la société de

l'information, le « Global Cybersecurity Agenda » (Programme mondial de cybersécurité) ainsi que la rédaction en 2021 du « Draft Guidelines » (Lignes Directrices) pour sa mise en œuvre ;

- La multiplication des initiatives africaines en matière de cybersécurité et de lutte contre la cybercriminalité, notamment la rédaction par la Commission de l'Union Africaine et l'Internet Society (ISOC) des lignes directrices sur la sécurité de l'infrastructure Internet pour l'Afrique du 30 mai 2017 et la définition par AFRIPOL (African Union Mechanism for Police Cooperation) d'une Stratégie en matière de cybercriminalité ;
- 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 par la vingt-troisième session ordinaire de la Conférence de l'Union Africaine à Malabo, en Guinée Equatoriale, afin de permettre l'essor d'un cyberespace africain sûr ;
- Les travaux du projet « Criminalité organisée : Réponse de l'Afrique de l'Ouest sur la cybersécurité et la lutte contre la cybercriminalité » (OCWAR-C) de la CEDEAO qui visent à évaluer l'état de préparation en matière de cybersécurité et déterminer le niveau de maturité de chaque Etat membre de la CEDEAO et de la Mauritanie. Et ce, afin d'élaborer un plan d'action pour chaque pays. Ces travaux ont notamment permis de rédiger une stratégie régionale de cybersécurité et une politique régionale de protection des infrastructures d'information critiques.
- Les travaux du Global Forum on Cyber Expertise (GFCE) qui est une communauté multipartite de plus de 140 membres et partenaires de toutes les régions du monde, visant à renforcer les cyber capacités et l'expertise à l'échelle mondiale.

Pour faire efficacement face aux cyberattaques perpétrées par des individus et des groupes organisés, avec différentes motivations, il est important d'accroître continuellement les initiatives internationales visant à augmenter le niveau de cybersécurité des organisations et des pays pour assurer la continuité de la stabilité mondiale.

Cet engagement commun à lutter contre la cybercriminalité, renforce continuellement l'entraide, le partenariat et une bonne coordination technique, comportementale, organisationnelle et juridique entre les différents acteurs de la cybersécurité.

2.3.3.

Une population jeune avec une appétence pour l'apprentissage

Le Togo compte environ 8,3 millions d'habitants et 70% de la population a moins de 35 ans. Cette population jeune est l'un des piliers pour transformer structurellement l'économie et développer une croissance forte, durable, résiliente et inclusive. Cette jeunesse utilise les technologies de l'information et est avide d'apprentissage. Cela représente une opportunité pour le Togo lorsque des programmes nationaux de formations en digitalisation et en cybersécurité seront effectifs.

2.3.4.

Une économie croissante

Selon les principaux indicateurs macroéconomiques publiés par le FMI, la croissance du PIB réel par habitant en 2021 était de +2,6%, et pour le compte de 2022, il sera de +3% pour une population d'environ 8,6 millions d'habitants. Cette croissance est répartie à la hausse après un léger ralentissement dû aux conséquences néfastes de la COVID -19 .

Cette croissance a été soutenue par les réformes, dont celles de la logistique et des transports autour du Port Autonome de Lomé (PAL) et de l'Aéroport International Gnassingbé EYADEMA (AIGE), des télécommunications, des finances et des banques, qui permettent de maintenir un cadre macroéconomique stable et de motiver les partenaires techniques et financiers à continuer d'accompagner le Togo à travers des programmes et projets de développement.

Cette bonne santé de l'économie togolaise, représente une opportunité pour mutualiser l'ensemble des moyens financiers et humains en faveur du renforcement de la sécurité du cyberspace du pays.

⁷ Rapport des services du FMI N°20/107 de mai 2020



2.4

Les principales menaces contre la stratégie de cybersécurité

2.4.1.

Le cyberspace : un espace sans frontières

Le cyberspace est souvent présenté comme un territoire virtuel, un espace à part, sans frontières, qui s'affranchit des contraintes du monde physique, dont l'avènement du cloud renforce le caractère immatériel.

Cette situation oblige à repenser le principe de souveraineté à cause de la multiplicité des acteurs et de l'enchevêtrement des enjeux et des risques. En effet, les nouveaux services en ligne bouleversent les équilibres économiques et menacent des secteurs entiers; les cyberattaques sont de plus en plus nombreuses, ciblées et sophistiquées et menacent la sécurité des infrastructures vitales et des citoyens ; les entreprises peuvent voir leurs données volées, divulguées, détruites ou leurs installations sabotées à distance ; les individus sont exposés à l'exploitation de leurs données personnelles et de leur intimité par des gouvernements ou des entreprises ; les policiers et les juges font face au défi du chiffrement des communications en ligne par des terroristes et des criminels ; les militaires risquent de voir leurs capacités opérationnelles affectées par des actions de sabotage, manipulation de l'information ou d'influence.

Face à cette situation, il est nécessaire de reconstruire une nouvelle approche avec de nouvelles législations, repenser la souveraineté et les modes de gouvernance.

2.4.2.

Un monde en constante évolution

Le monde des technologies de l'information est en permanente évolution. Les cybermenaces évoluent au même rythme que les sociétés se digitalisent et que les citoyens adoptent les technologies. Les Etats, les administrations publiques, les entreprises privées, certains individus sont désormais la cible de menaces persistantes avancées. Les APT (Advance Persistent Threat) sont des menaces beaucoup plus subtiles, intelligentes, sophistiquées et plus dangereuses que les précédentes. Elles sont furtives et continues dans le temps et profitent des failles humaines ou des vulnérabilités présentes même dans les dernières versions de logiciels ou d'équipements.

Les cybercriminels adaptent continuellement leurs techniques et méthodologies pour contourner les mesures de sécurités mises en place. Face à ces menaces en perpétuelle évolution, les experts en cybersécurité doivent eux aussi se mettre en permanence à jour de toutes ces évolutions dans leur rôle de garant de la sécurité des systèmes d'information qui sont sous leur responsabilité.

2.4.3.

La cybercriminalité régionale

La région ouest africaine regorge de cyber-escrocs qui défraient régulièrement la chronique, en l'occurrence les « Yahoo boys », les « Sakawa boys », les « brouteurs » ou encore les « gayman » combattus respectivement par le Nigéria, le Ghana, la Côte d'Ivoire et le Bénin. Du fait de la proximité géographique du Togo avec ces pays et des avancées significatives faites par ces derniers en matière de lutte contre la cybercriminalité, le territoire togolais devient un refuge pour ces cybercriminels. Comme pour la sécurité physique d'un pays, la cybersécurité et la lutte contre la cybercriminalité nécessitent pour être efficaces, une compréhension détaillée des croyances et des habitudes socio culturelles des populations.

Pour orienter les approches de cybersécurité à mettre en œuvre, une analyse approfondie devra être réalisée, sur la provenance des menaces nationales, la connaissance des méthodes d'attaques organisées dans la région, les types d'actions des groupes connus, les approches criminalistiques reconnues etc. De même, une analyse devra être réalisée concernant les vulnérabilités basées sur le mode de vie, les croyances, les convictions politiques ainsi que les liens avec les populations des pays voisins.

C'est dire que la coopération et les échanges d'informations avec les pays de la sous-région est importante, de même que le niveau d'investissement de ces derniers dans la cybersécurité opérationnelle.

2.4.4.

Une enveloppe budgétaire réduite ou faible

Au Togo, le financement des activités de cybersécurité représente une nouvelle ligne que les dirigeants politiques et d'entreprises doivent désormais prendre en compte. La principale raison est de mettre en œuvre des opérations pour diminuer les coûts potentiels liés à des incidents d'envergures sur les infrastructures informatiques essentielles nécessaires, selon les cas, à l'activité de l'entreprise ou du gouvernement du pays. Pour un dirigeant dont l'objectif est de maximiser les profits ou de faire preuve de bonne gestion en diminuant au mieux les coûts, ceux liés à la cybersécurité ne sont pas prioritaires. Il faut souvent faire preuve de beaucoup de courage pour engager des coûts dont l'utilité n'est pas assez évidente pour les décideurs.

En outre la mise en œuvre des changements budgétaires au niveau administratif et législatif n'est souvent pas en phase avec le dynamisme de la cybercriminalité.

La cybersécurité ne doit plus passer au second plan de la transformation digitale et doit être mise au centre des préoccupations des entreprises privées ou publiques comme des gouvernements.

La période actuelle a ainsi mis en exergue l'importance d'allouer des budgets plus conséquents dédiés à la cybersécurité.

D'ailleurs, des enquêtes d'opinion montrent que les Etats des pays développés ont fortement augmenté les budgets dédiés à la cybersécurité, conscients que les risques et les menaces sont élevés.

Par conséquent, il devient urgent pour les pays en voie de développement de revoir à la hausse l'enveloppe financière dédiée à la cybersécurité, pour ne pas rester en marge de l'évolution de la lutte contre les cybermenaces qui menacent la transition numérique en cours.

Cette hausse de l'enveloppe budgétaire nécessite un accroissement des ressources internes mobilisées et également des ressources externes. Or, en cas de crise économique, les capacités de mobilisation interne sont réduites car les entreprises se portent mal (les ressources fiscales mobilisées ne sont plus à la hauteur des ambitions) et les ressources mobilisables deviennent rares.



3.

La stratégie nationale de cybersécurité

Nous nous attachons dans ce chapitre à définir la stratégie nationale de cybersécurité avec des actions à déployer jusqu'à la fin de l'année 2028. Une révision sera faite à mi-parcours sur la base d'une nouvelle analyse des réalisations ainsi que des évolutions des forces, faiblesses, opportunités et menaces.

Nous nous appuyons sur l'analyse FFOM du chapitre précédent avec comme priorité la consolidation des forces développées lors des années précédentes, dans le but de diminuer la prise possible des menaces sur les faiblesses existantes tout en s'appuyant sur les opportunités offertes au Togo.

L'ensemble des actions définies ont pour rôle de protéger l'économie et la société contre les perturbations liées, entre autres, aux technologies de l'information et de la communication [TI/TIC] et aux technologies opérationnelles [OT].

La stratégie nationale de cybersécurité repose sur les quatre (04) objectifs stratégiques suivants :

1. Promouvoir une culture de la cybersécurité et développer les compétences techniques nationales ;
2. Assurer la sécurité continue des services essentiels et de l'économie numérique ;
3. Renforcer le système de réponse aux incidents de cybersécurité ;
4. Assurer une poursuite efficace des crimes et délits de cybersécurité.

Afin d'atteindre les objectifs stratégiques sus-énumérés, il est nécessaire de déterminer pour chacun de ces objectifs stratégiques, les éléments suivants :

1. Les objectifs et priorités ;
2. Les mesures et des actions à mettre en œuvre ;
3. Les acteurs clés de la mise en œuvre de la stratégie nationale de cybersécurité.

La stratégie de cybersécurité vise directement les entités de l'administration publique, les opérateurs de services essentiels et indirectement, les autres pouvoirs publics, les entrepreneurs et les citoyens.

La stratégie nationale de cybersécurité SNCy 2024-2028 repose donc sur quatre (04) piliers :

- **Pilier 1** : Promotion d'une culture de la cybersécurité et développement des compétences techniques nationales ;
- **Pilier 2** : Promotion continue de la sécurité des services essentiels et de l'économie numérique ;
- **Pilier 3** : Renforcement du système de réponse aux incidents de cybersécurité ;
- **Pilier 4** : Renforcement du cadre de poursuite efficace des crimes et délits de cybersécurité.



1. Promouvoir une culture de la cybersécurité et développer les compétences techniques nationales ;
2. Assurer la sécurité des services essentiels et de l'économie numérique ;
3. Renforcer le système de réponse aux incidents de cybersécurité ;
4. Assurer une poursuite efficace des crimes et délits de cybersécurité.



4.

Orientations de la stratégie de cybersécurité

4.1

Pilier 1 : promotion d'une culture de la cybersécurité des populations et développement des compétences techniques nationales

Le facteur humain étant une cause majeure dans 95 % des cyberattaques, il ne fait aucun doute que la sensibilisation et la formation sont une partie très importante d'une solide stratégie de cybersécurité. En effet, lorsque la majorité des attaques ciblent spécifiquement les utilisateurs, pour chercher à les encourager à cliquer sur un lien malveillant, à divulguer des identifiants de connexion, à ouvrir une pièce jointe ou simplement à payer une fausse facture, la création d'une culture de la cybersécurité pour détecter et repousser ces attaques semble un choix évident.

Pour implémenter cette culture de la cybersécurité, tant en entreprise qu'au sein des populations, il est nécessaire de former les populations à un usage responsable et sécurisé des outils numériques. Mais pour être plus efficace, cette formation gagnerait davantage à s'adresser aux plus jeunes, dès le début de leur parcours scolaire.

Conscient de cette réalité, la stratégie nationale a décidé d'accorder une attention particulière aux aspects ci-après :

1. Enseignement dans le primaire et le secondaire
2. Enseignement professionnel supérieur
3. Programme de sensibilisation de la population

A terme, la mise en œuvre de ces réformes permettra de combler le déficit de compétences dont l'économie numérique a besoin pour son développement et d'améliorer les compétences des populations pour une utilisation accrue et responsable des technologies numériques.

4.1.1.

Intégrer l'enseignement de la cybersécurité dans le primaire et le secondaire

L'objectif du gouvernement togolais est de mettre l'accent sur l'ouverture des jeunes aux nouvelles technologies par la modernisation des équipements existants et de raccordement des écoles à Internet en suivant un modèle PPP mobilisant l'épargne nationale.

Mais plus encore, il existe une réelle volonté de mettre en place des programmes de formation dans le système éducatif afin de garantir l'insertion des élèves dans la société numérique et l'apprentissage des médias numériques car l'objectif de l'école reste la formation des citoyens, et la dimension numérique ne peut être négligée aujourd'hui, car investir dans la Cybersécurité, ne doit plus être perçu comme un coût, mais comme un investissement.

En effet, l'enseignement dans le primaire et dans le secondaire étant un canal privilégié de transmission de la culture sur le potentiel des technologies de l'information et des risques qui y sont liés, il est important de préparer un programme d'enseignement et d'intégrer la cybersécurité dans la formation du corps enseignant en vue de transmettre :

- La connaissance et la compréhension du fonctionnement et des limites de la technologie ;
- Les risques et les menaces, liés à cette source d'information ;
- Les meilleures pratiques d'utilisation ;
- Les moyens de trouver et de vérifier l'information à l'aide de diverses sources.

L'enseignement sur les technologies de l'information et sur la cybersécurité dans le primaire et le secondaire permettra de préparer les jeunes à la poursuite d'études universitaires dans les domaines de la technologie et de la cybersécurité. Les étudiants les plus talentueux pourraient obtenir la garantie de poursuivre leurs études (bourses) voire de trouver des débouchés dans ce secteur.

C'est pour cette raison qu'il convient d'introduire très tôt le numérique comme objet d'apprentissage dans les curricula de formation et de le généraliser au cycle supérieur. Il favorise et promeut l'utilisation des technologies dans l'enseignement, en vue d'apporter une solution digitale aux défis de capacité d'accueil des établissements et institutions d'enseignement et d'éducation.

RESPONSABILITÉ

- MINISTÈRE DE L'ECONOMIE NUMÉRIQUE ET DE LA TRANSFORMATION DIGITALE
- AGENCE NATIONALE DE LA CYBERSÉCURITÉ

PARTICIPANTS

Ministère des enseignements primaire, secondaire, technique et de l'artisanat

INTERVENTIONS

1. Préparer un programme de formation sur les nouvelles technologies, qui débute dès les premières classes du primaire et qui inclut des exercices pratiques. Cet enseignement est orienté sur :
 - a. Les bases de l'informatique ;
 - b. L'utilisation d'Internet ;
 - c. Une bonne connaissance de l'ensemble des terminaux dont les téléphones mobiles et les smartphones ;
 - d. La recherche d'information ;
 - e. La sécurité des transactions en ligne ;
 - f. L'identification et l'authentification en ligne ;
 - g. Les réseaux sociaux.
2. Intégrer des experts de la sécurité en renfort des enseignants sur le périmètre des formations et des exercices d'application à mettre en œuvre pour que les programmes soient évolutifs et adaptés aux capacités de compréhension et d'intégration des connaissances par les élèves. Pour une meilleure réussite, il est important que ces programmes de formations soient proches des habitudes d'utilisation des élèves auxquels l'enseignement sera fourni.

⁹ Ministère des enseignements primaire, secondaire, technique et de l'artisanat (<https://education.gouv.tg/>)

3. Suivant les possibilités et les capacités, faciliter et motiver les activités d'apprentissage en ligne – en particulier dans les régions rurales. Il est important de choisir les forces et les moyens qui permettront d'offrir une véritable éducation dans des régions moins numérisées. L'expérience de la pandémie COVID-19 peut fournir de nouveaux concepts à cet égard pour atteindre les zones rurales avec de l'information éducative – pas nécessairement avec l'utilisation d'ordinateurs.
4. Organiser des compétitions de cybersécurité (hackaton, CTF) pour la détection de talents, leur recrutement et leur encadrement.

4.1.2.

Intégrer l'enseignement de la cybersécurité dans l'enseignement professionnel supérieur

Le développement de l'économie numérique et la fourniture de la cybersécurité exigent un personnel hautement qualifié. La formation professionnelle est un processus pluriannuel qui demande une analyse des besoins prévisibles du marché du travail futur pour planifier les programmes d'éducation à mettre en œuvre en conséquence. Il s'agit d'un processus continu géré par le ministère de l'enseignement supérieur et de la recherche, le ministère chargé de l'enseignement technique et de la formation professionnelle et le ministère de l'économie numérique et de la transformation digitale, fondé sur les prévisions de développement du marché du travail établi.

Le gouvernement togolais s'attellera à renforcer la coopération internationale dans l'enseignement supérieur professionnel par des échanges de personnels universitaires, de programmes d'études et d'étudiants.

Pour garantir sa souveraineté dans le domaine de la formation professionnelle grâce à une main d'œuvre hautement qualifiée, la République togolaise est déterminée autant que possible, à s'assurer de son indépendance vis-à-vis des fournisseurs étrangers de technologies et de solutions, pour disposer au sein de son marché du travail, d'un personnel qualifié approprié pour la maîtrise nationale du développement et du maintien des compétences hautement qualifiées.

RESPONSABILITÉ

AGENCE NATIONALE DE LA CYBERSÉCURITÉ

PARTICIPANTS

1. Ministère de l'enseignement supérieur et de la recherche ;
2. Ministère de l'enseignement technique et de l'artisanat ;
3. Ministère de l'économie numérique et de la transformation digitale ;
4. Université de Lomé ;
5. Université de Kara.

INTERVENTIONS

1. Préparation des cours en cybersécurité post-universitaires, en particulier pour :
 - 1.1. L'ingénierie de gestion et de production ;
 - 1.2. Le développement de logiciels ;
 - 1.3. Les télécommunications – réseaux informatiques ;
 - 1.4. L'informatique – architecture de système ;
 - 1.5. La gestion de la sécurité des informations.

La préparation d'un programme de formation efficace doit être précédée par un examen du programme de formation existant. Ensuite, il est nécessaire de planifier les possibilités des nouvelles orientations en prenant en compte la cybersécurité, en vérifiant les compétences requises du personnel universitaire, l'infrastructure (par exemple les laboratoires) nécessaire à l'organisation des cours, le périmètre du programme lui-même.

2. Intégration des entreprises dans la préparation des programmes de formation :

Une étroite collaboration avec les représentants des entreprises en ce qui concerne les attentes du marché du travail est nécessaire pour atteindre le but escompté. A cet égard, les entreprises participeront à l'identification des attentes du marché du travail à l'égard des diplômés, et seront des acteurs clés dans la mise en place des programmes de formation qui fourniront des employés qualifiés attendus.

¹⁰ Ministère de l'Enseignement Supérieur et de la Recherche (<https://edusup.gouv.tg/>)

¹¹ Ministère chargé de l'enseignement technique et de l'artisanat (<https://edutech.gouv.tg/>)

¹² Ministère de l'Economie Numérique et de la Transformation Digitale (<https://numerique.gouv.tg/>)

3. La mobilisation des bourses dans le domaine de la cybersécurité

4. Formation en ligne

Il sera également nécessaire de faciliter les activités d'apprentissage et d'accès aux connaissances en ligne.

Pour la préparation de ces cours, il convient de s'assurer :

- Du choix de la plateforme de formation en ligne ;
- De la planification et du contenu des formations ;
- Du contrôle de l'exécution des formations et de l'évaluation de leur efficacité.

La pandémie du COVID-19 a permis d'acquérir de nombreuses expériences en matière d'enseignement à distance qu'il serait possible de mettre à profit.

4.1.3.

Mettre en oeuvre un programme de sensibilisation

L'objectif de la sensibilisation consiste à motiver les citoyens dans l'utilisation responsable des services et informations sur le cyberspace, en attirant continuellement leur attention sur les risques et des menaces associés.

En effet, le développement de la sécurité numérique nationale passe nécessairement par un changement dans les habitudes des citoyens, qui sont en première ligne face aux cybermenaces. Pourtant, il est constaté que dans l'état actuel des choses, la sensibilisation est encore très faible, voire inexistante à certains endroits, malgré les nombreux efforts entrepris par le gouvernement dans ce sens. Il est donc urgent de développer un programme national de sensibilisation en cybersécurité, englobant l'ensemble des couches sociales du pays, l'Etat, les entreprises, la société civile, les médias, les universités, les écoles et surtout, les populations rurales.

Dans cette optique, les modes et les supports de communication doivent être adaptés aux capacités perceptives des bénéficiaires. A cet effet, il convient que les messages soient courts, simples pour la compréhension, et adaptés aux circonstances.

Une sensibilisation effective est permanente et dynamique. Une équipe de coordination est en contact avec le plus grand nombre de sources locales, régionales et nationales de communication telles que gouvernementales, des différentes administrations territoriales, des différents secteurs d'activité (télécommunications, banques, services des eaux et d'électricité), etc. Les médias les plus accessibles sont la télévision, la radio, les sites web des annonceurs, les réseaux sociaux et autres médias. Prenant appui sur le programme de sensibilisation établi, l'équipe de coordination utilisera l'ensemble des communications des différents partenaires pour inclure les messages de sensibilisation et de sécurité à jour face aux menaces et aux vulnérabilités les plus dangereuses et émergentes.

RESPONSABILITÉ

- AGENCE NATIONALE DE LA CYBERSÉCURITÉ (ANCy) ;
- CERT.TG AVEC ÉVENTUELLEMENT D'AUTRES CSIRT/CERT SECTORIELS.

PARTICIPANTS

1. Ministère des enseignements primaire, secondaire, technique et de l'artisanat ;
2. Ministère de l'enseignement supérieur et de la recherche ;
3. Ministère de la fonction publique, du travail, de la réforme administrative et de la protection sociale ;
4. Ministère de l'économie numérique et de la transformation digitale ;
5. Ministère des droits de l'homme, de la formation à la citoyenneté et des relations avec les institutions de la République ;
6. Ministère de la sécurité et de la protection civile ;
7. Ministère de la communication et des médias ;
8. Instance de protection des données à caractère personnel (IPDCP) ;
9. Autorité de régulation des communications électroniques et des postes (ARCEP) ;
10. Fournisseurs de télécommunications (entreprises) ;
11. Banque Centrale des Etats d'Afrique de l'Ouest (BCEAO) ;
12. Banques (entreprises).

INTERVENTIONS

1. Préparation d'un programme de sensibilisation – information (dépliants/web), formations et événements

Le programme de sensibilisation sociale devrait être planifié de plusieurs façons. Tout d'abord, définir un mois de l'année civile comme étant le mois de la cybersécurité. Le mois de la cybersécurité pourrait se caractériser par des activités éducatives bien ciblées au moyen de messages sur le Web (médias sociaux) ou d'annonces dans les médias. Les messages pourront mettre l'accent sur les comportements positifs en ligne des utilisateurs ou sur les avertissements concernant les menaces.

2. Le deuxième pilier de la sensibilisation est le lancement d'un programme d'alertes sur les menaces émergentes sur Internet par les mesures suivantes :

- Les opérateurs de télécommunications au moyen d'alertes SMS ;
- Les banques par le biais de messages sur l'online Banking.

¹³ Ministère de la fonction publique, du travail, de la réforme administrative et de la protection sociale (<https://fonctionpublique.gouv.tg/>)

¹⁴ Ministère de l'économie numérique et de la transformation digitale (<https://numerique.gouv.tg/>)

¹⁵ Ministère des droits de l'homme, de la formation à la citoyenneté, des relations avec les institutions de la République (<https://droitsdelhomme.gouv.tg/>)

4.2

Pilier 2 : promotion continue de la sécurité des systèmes d'information de l'administration, des opérateurs de services essentiels et de l'économie numérique

La sécurité des systèmes d'information (SSI) est un enjeu majeur pour les opérateurs de services essentiels (OSE), l'administration publique et l'économie numérique. Ces acteurs sont exposés à des risques croissants de cyberattaques, qui peuvent compromettre la continuité de leurs activités, la protection des données personnelles et la confiance des usagers. Pour renforcer la résilience de ces secteurs stratégiques, il est nécessaire de promouvoir une culture de la SSI et de mettre en œuvre des mesures adaptées à leur niveau de criticité.

4.2.1.

Dispositions législatives et réglementaires, et détermination du cadre institutionnel

La loi 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité constitue la base légale de la cybersécurité et établit le cadre de la lutte contre la cybercriminalité.

L'Agence Nationale de la Cybersécurité (ANCy) est chargée de l'application effective des orientations et mesures stratégiques, ainsi que du fonds de souveraineté nationale, qui contribue notamment au financement de la mise en œuvre de la stratégie nationale de cybersécurité et des actions de l'ANCy.

Dans la continuité de cette loi, le décret 2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes détermine entre autres, la méthode de désignation des opérateurs de services essentiels (OSE) en s'appuyant sur la liste des services essentiels par secteur d'activité structurant pour la société togolaise, ainsi que les règles de cybersécurité

que les OSE sont tenus de respecter. Dans ce cadre, ils doivent se doter d'un Plan de Sécurité d'Opérateur (PSO) en conformité avec les "règles de cybersécurité" fixées par l'ANCy et d'un "Security Operations Center", (SOC) pour protéger leurs infrastructures informatiques essentielles et réagir en cas d'incident.

L'élaboration et l'application de la stratégie nationale de cybersécurité nécessite l'établissement d'indicateurs d'évaluation et de progression des niveaux de sécurité atteints.



RESPONSABILITÉ

- AGENCE NATIONALE DE LA CYBERSÉCURITÉ (ANCy) ;
- CERT.TG AVEC ÉVENTUELLEMENT D'AUTRES CSIRT/CERT SECTORIELS.

PARTICIPANTS

Ministère de l'économie numérique et de la transformation digitale

INTERVENTIONS

1. Suivre et optimiser la mise en œuvre effective de la législation

Avec la loi sur la cybersécurité, les décrets relatifs aux OSE et à la création de l'ANCy ainsi que de CDA et les règles de cybersécurité, la République Togolaise a mis en place une base législative et réglementaire de la sécurité du cyberspace national ainsi que des institutions responsables de son application. C'est le point de référence pour la mise en place du système national de cybersécurité. L'application de la réglementation nécessite un suivi pour s'assurer que les effets sont ceux attendus afin de déterminer les ajustements à mettre en œuvre au cas échéant. Le bon fonctionnement de l'autorité de contrôle (ANCy) est essentiel à l'efficacité de l'application de la loi. Son action est déterminante et devrait se manifester par des sanctions à l'encontre des entités ne respectant pas la législation, ainsi que des rapports sur l'évolution des indicateurs de mesure des effets de la réglementation et de son application, ainsi que des propositions rationnelles et justifiées sur l'évolution éventuelle de la législation.

2. Tenir à jour la liste des OSE

Une liste évolutive des opérateurs de services essentiels par secteur et sous-secteur d'activité est tenue à jour.

3. Superviser les opérateurs de services essentiels

Le décret sur les opérateurs de services essentiels établit avec précision leurs obligations qui sont déterminées dans les règles de cybersécurité, sous peine d'amendes. Un audit annuel est prévu pour s'assurer que les OSE sont bien en conformité avec la législation togolaise et le plan de sécurité accepté par le régulateur ce qui assure un niveau respectable de sécurité de leurs infrastructures informatiques essentielles.

Le plan de sécurité d'opérateur doit, entre autres, établir des audits, enquêtes, rapports sur l'exploitation des services essentiels, rapports d'incidents, afin de faire le suivi des indicateurs de mesure de leur niveau de sécurité face aux objectifs fixés dans leur plan de sécurité d'opérateur.

4.2.2.

Définir les normes et les règles de sécurité

La définition de normes et de règles pour la sécurité des infrastructures informatiques supportant les services essentiels est un élément important dans la mise en œuvre de la cybersécurité. Ces éléments précisent la façon de mettre en œuvre concrètement les exigences et les intentions générales prévues par la réglementation.

RESPONSABILITÉ

- AGENCE NATIONALE DE LA CYBERSÉCURITÉ (ANCy) ;
- CERT.TG AVEC ÉVENTUELLEMENT D'AUTRES CSIRT/CERT SECTORIELS.

INTERVENTIONS

1. Elaborer les lignes directrices pour la mise en œuvre de la législation sur la cybersécurité

Afin de garantir une mise en œuvre correcte et efficace de la législation sur la cybersécurité, il est nécessaire d'élaborer ou d'utiliser des lignes directrices internationales existantes à l'intention des opérateurs de services essentiels dans ce domaine. Ces lignes directrices identifient chaque étape de la mise en œuvre de la législation, en tenant compte de toutes les mesures que doivent prendre les entités tenues de mettre en œuvre les prescriptions.

2. Élaborer et maintenir une méthodologie comparable d'évaluation du niveau de sécurité (fondée sur les risques)

La méthodologie est mise au point par un groupe d'experts. Les hypothèses de la méthodologie tiennent compte du fait qu'elle est compréhensible, simple et qu'elle reflète en même temps l'état réel de la sécurité de l'information dans une entité donnée.

La méthode de gestion des risques couvre les aspects suivants :

- L'identification des menaces ;
- L'identification des vulnérabilités ;
- L'évaluation des risques ;
- L'évaluation des contrôles de sécurité ;
- Le traitement des risques.

La méthodologie garantit que les résultats de l'évaluation des risques fournissent des résultats objectifs et comparables. Cette évaluation est effectuée de manière cyclique (c'est-à-dire tous les ans) afin d'en maximiser l'efficacité.

3. Élaborer et tenir à jour des rapports d'évaluation du niveau de sécurité (vérification)

L'élaboration de la procédure d'audit se fonde sur les bonnes pratiques reconnues internationalement, telles que les lignes directrices de l'ENISA (Agence de l'Union Européenne pour la Cybersécurité) ou du NIST (National Institute of Standards and Technology). Ces types de lignes directrices pour la mise en œuvre des audits permettent de tirer parti de l'expérience mondiale pour élaborer une méthodologie d'audit.

4. Faire une étude annuelle sur l'état de la cybersécurité au Togo auprès des OSE et des administrations :

Il s'agira d'interroger les opérateurs de services essentiels, les administrations, des fonctionnaires, ou membres du gouvernement qui travaillent ou connaissent le domaine. L'objectif sera de faire un état des lieux complet, d'évaluer les résultats de la stratégie et de comprendre la tendance et les perspectives. L'objectif visé est notamment de :

- déterminer le niveau des entreprises et institutions du pays dans leur protection contre les cybermenaces ;
- déterminer le niveau de menaces auxquelles ces structures font face ;
- évaluer leur degré de connaissance dans le domaine ;
- évaluer leurs pratiques et usages en la matière ;

INTERVENTIONS

- apprécier le niveau d'engagement des décideurs sur des problématiques de cybersécurité ;
- anticiper sur les perspectives du marché.

5. Faire une étude annuelle sur l'état de la cybersécurité au Togo auprès des citoyens :

Il s'agira d'évaluer les résultats de la stratégie sur la population togolaise, notamment :

- déterminer le niveau de conscience du grand public sur les problématiques de cybersécurité et son intérêt pour le sujet ;
- évaluer la perception du grand public sur ces questions.

6. Maintenir un forum de discussion sur la cybersécurité pour échanger sur les meilleures pratiques

Un forum de discussion est un support à l'amélioration des connaissances actuelles par les spécialistes en charge de la sécurité du cyberspace. Pour son efficacité il devra tenir compte de la participation d'un large éventail d'experts de différents secteurs importants pour le fonctionnement du système national de cybersécurité. Le forum devrait également être précédé d'une analyse des tendances des menaces et se concentrer sur des questions bien définies nécessitant un débat. Des mécanismes seront mis en place pour garantir la communication des conclusions de ces débats aux parties intéressées. Afin d'assurer une grande efficacité des forums de discussion, il importe de définir à l'avance leur calendrier et (si possible) leur ordre du jour.

4.2.3.

Encourager les investissements dans la cybersécurité

Les investissements dans la cybersécurité ne donnent pas toujours de retour sur investissement mesurable, surtout à court terme. Comment chiffrer un risque qui a été évité ou préempté ? Toutefois, les dirigeants d'entreprises sont largement sensibilisés aux cyber-risques ces dernières années, entre autres par la forte médiatisation des attaques dont la fréquence et les coûts pour les sociétés et les administrations publiques qui en sont victimes sont en croissance.

Certaines études de perception des risques par les dirigeants d'entreprises, comme celle effectuée chaque année par la compagnie d'assurance Allianz, montrent que ces derniers perçoivent le risque cyber comme faisant partie des 3 plus grands risques pour leurs entreprises. Aujourd'hui, les dirigeants d'entreprises dans leur majorité acceptent de mettre en place un budget pour accroître la sécurité des systèmes d'information de leurs sociétés.

Les dirigeants d'entreprises sont alors confrontés au dilemme de devoir accorder un budget annuel supplémentaire, très difficile à redistribuer sur les prix des services proposés et qui affecte le résultat de la société qu'ils gèrent.

Cette situation contraint les conseils d'administration à limiter l'attention dévolue à ces investissements. Face aux risques et menaces qui s'accroissent, toutes les initiatives pouvant proposer des fonds supplémentaires sont à étudier. Les intérêts des entreprises et des Etats se rejoignent dans le besoin de sécurité du cyberspace. Les initiatives du gouvernement pour encourager, faciliter et supporter les investissements des entreprises dans la cybersécurité sont à analyser. Entre autres, des aides indirectes, comme des réductions d'impôts ou de remises de dettes envers l'État peuvent être envisagées, avec des montants et des conditions définis annuellement dans le budget de l'État.

RESPONSABILITÉ

AGENCE NATIONALE DE LA CYBERSÉCURITÉ

PARTICIPANTS

- Ministère de l'économie et des finances ;
- Ministère de l'économie numérique et de la transformation digitale.

INTERVENTIONS

1. Élaborer un programme incitatif pour les investissements dans la cybersécurité.

Compte tenu de la spécificité de chaque secteur et entreprise, un plan d'incitation équilibré en matière de cybersécurité sera élaboré. Le plan définira les domaines dans lesquels des investissements sont nécessaires et identifiera les entreprises présentant un intérêt mutuel. En raison de l'évolution dynamique de l'environnement technologique et commercial, le programme sera mis à jour chaque année. Cela garantira l'inclusion de programmes incitatifs dans les plans budgétaires annuels de l'État.

¹⁶ Ministère de l'Economie et des Finances (<https://finances.gouv.tg/>)

¹⁷ Ministère de L'Economie Numérique et de la Transformation Digitale (<https://numerique.gouv.tg/>)

INTERVENTIONS

2. Organiser une table ronde de mobilisation de ressources pour la mise œuvre du programme

Une table ronde des bailleurs de fonds devra être organisée autour du plan d'investissement élaboré. Les différents projets de sécurité de l'information dans les différents domaines pour lesquels les investissements sont nécessaires.

3. Faire le suivi de la mise en œuvre du plan d'investissement élaboré

Un rapport annuel sur la mise en œuvre du plan d'investissement devra être élaboré. Cela permettra d'apprécier l'état de la mise en œuvre du plan, de déceler les goulots d'étranglement et de faire des propositions en vue d'améliorer sa mise en œuvre dans tous les secteurs impliqués.

4.3

Renforcer le système de réponse aux incidents de cybersécurité

Le renforcement du système national de réponse aux incidents de cybersécurité est une priorité stratégique pour assurer la protection des infrastructures critiques et des données sensibles. Il s'agit de mettre en place des mécanismes de coordination, de partage d'information, d'analyse de risques, de prévention et de réaction face aux menaces et aux attaques informatiques. Le système national de réponse aux incidents de cybersécurité doit être capable de détecter, identifier, contenir, éradiquer et restaurer les systèmes affectés par des incidents de cybersécurité.

4.3.1.

Mettre en place un système national de réaction aux incidents de cybersécurité efficace

Aucun système d'information ne peut être sécurisé à 100%, et les incidents de sécurité en sont des éléments imminents. La sécurisation d'un système d'information est un processus en constante amélioration et la détection d'un incident doit être interprétée comme un potentiel d'amélioration, avec comme objectif de prévenir le système d'information de ce genre d'incident à l'avenir. C'est une des activités du CSIRT (Computer Security Incident Response Team) ou du CERT (Computer Emergency Response Team), dont l'une des principales missions, est d'apporter des réponses aux incidents informatiques ainsi qu'aux risques et menaces qui pèsent sur les systèmes d'informations.

Ces équipes de réponse aux incidents s'appuient, dans leur travail, sur des échanges d'informations au sein des réseaux internationaux de CSIRT / CERT pour développer des compétences en matière de gestion des menaces et des méthodes de prévention et de défense contre celles-ci. Elles fournissent leurs services aux administrations, entreprises et citoyens touchés par des incidents de sécurité et pour apporter de nouveaux scénarios de protection et de défense à ces derniers.

Le CERT national du Togo CERT.tg est opérationnel depuis le 1er Février 2021 et est opéré par Cyber Defense Africa (CDA) en tant que service délégué par l'Agence Nationale de la Cybersécurité (ANCy). Le CERT.tg traite, coordonne et répond aux incidents de sécurité informatique des administrations, entreprises et citoyens togolais. Il publie des annonces d'intrusions, des vulnérabilités et des bulletins de sécurité via son site web <https://cert.tg>. Ce site web contient également des informations de sensibilisation à la cybersécurité pour les familles, les petites et moyennes entreprises, les grandes entreprises, les administrations et les Opérateurs de Services Essentiels.

RESPONSABILITÉ

- AGENCE NATIONALE DE LA CYBERSÉCURITÉ (ANCy) ;
- CYBER DEFENSE AFRICA (CDA) ;

1. Améliorer continuellement les services offerts par le CERT.tg

Inscrit dans un processus d'amélioration continu, le CERT.tg doit chercher constamment des pistes d'amélioration pour garantir la meilleure qualité de services à ses constituants et lutter efficacement contre les cybermenaces qui évoluent en permanence.

Les principaux objectifs du CERT.tg sont la reconnaissance, la prévention et la détection des menaces touchant la sécurité des systèmes d'information des opérateurs de services essentiels publics, parapublics et privés du Togo.

Le CERT.tg ajoutera à son arsenal des services en cours, des recherches sur les nouvelles techniques et les tendances du secteur, de sorte à être continuellement à jour.

Le CERT national est également chargé d'enregistrer et de traiter les incidents de sécurité des réseaux et de réagir en cas de menaces directes contre les utilisateurs. A ce sujet, des procédures claires à suivre, par les entreprises et les citoyens, ont été élaborées en cas de détection d'un incident.

2. S'assurer que le CERT national répond aux besoins de tous les intervenants

Le CERT national est centré sur une approche pro-active, ciblant différents groupes de constituants (télécommunication, banque, gouvernement, etc.). À cette fin, il est recommandé de développer au sein du CERT national des compétences sectorielles afin de fournir un service public ciblé de gestion des incidents avec des méthodes de travail, une terminologie et une compréhension des besoins et risques particuliers de chaque constituant.

3. Organiser des exercices nationaux et internationaux de cybersécurité à intervalles réguliers.

Dans le but d'effectuer des tests de sécurité pour les OSE, ainsi que des simulations qui permettront de tester les comportements et la résistance des systèmes à des conditions réelles causées par un incident de sécurité, des programmes d'exercices auxquels participeront divers

intervenants du système national de cybersécurité, seront organisés.

4. Rédiger le plan national de réponse aux incidents de cybersécurité

Avec l'augmentation de la fréquence et de la sévérité des incidents de cybersécurité, il est crucial de doter le Togo d'un plan national de réponse aux incidents pour se préparer aux menaces pouvant impacter la sécurité publique, la stabilité économique, la sécurité nationale ou la stabilité internationale. Ce plan aidera le Togo à minimiser les conséquences d'une attaque d'envergure pour la nation et assistera les parties prenantes pour la prise des bonnes décisions en cas d'attaque afin de reprendre le contrôle du système d'information impacté.

Le plan permet :

- d'établir les rôles et les responsabilités des parties prenantes lors d'une situation de crise ;
- de concevoir des moyens de résolution des incidents ;
- d'assurer le bon partage d'informations entre les parties prenantes ;
- de servir de base pour améliorer la gestion et la coordination des incidents de cybersécurité au niveau institutionnel ;
- de définir le canal de communication efficace pour la transmission des messages liés aux incidents.

4.3.2.

Mettre en place un système efficace de réaction aux incidents de cybersécurité au niveau international

Le cyberespace tend à échapper aux règles qui gouvernent les frontières physiques des Etats car le cadre juridique qui encadre cet espace est encore très incomplet. Pour preuve, les matériels, logiciels ou outils logiciels composant les systèmes d'information des entreprises et des administrations sont internationaux et interconnectés et, par conséquent, les vulnérabilités, les failles peuvent être exploitées de n'importe quel endroit sur la planète. De ce fait, il est capital de répertorier l'ensemble des éléments composant un système d'information et de

pouvoir échanger à haut niveau, sur ces éléments et sur des services rendus équivalents (tels que services bancaires, de télécommunication etc.), entre spécialistes, des informations et des expériences sur les cybermenaces actuelles ainsi que sur les pratiques dans le domaine de la sécurité de l'information.

Ces échanges en cybersécurité permettent de profiter des connaissances et expériences acquises ailleurs dans le monde pour une réponse rapide et cohérente à une menace ou un incident de sécurité local existant. Les réseaux de CSIRT/CERT nationaux sont le support de la coopération internationale dans le monde de la cybersécurité. Conscient de ce fait, le CERT.tg représente le Togo au niveau international et établit ces canaux d'échanges avec les autres instances internationales.

En ce sens, le CERT.tg est déjà membre de AfricaCERT et membre listé de TF-CSIRT. Les collaborateurs du CERT.tg et de l'ANCy participent régulièrement aux conférences, symposiums et autres activités organisées par les communautés de CERT comme le FIRST.

RESPONSABILITÉ

- AGENCE NATIONALE DE LA CYBERSÉCURITÉ (ANCy) ;
- CYBER DEFENSE AFRICA (CDA).

INTERVENTIONS

Participer et/ou organiser des échanges internationaux d'expériences en matière de cybersécurité à intervalles réguliers.

Dans le domaine de la coopération internationale, il est possible de participer activement à des ateliers de recherche, à des forums, à la constitution d'un corpus commun de connaissances ou à des exercices. L'orientation retenue dans ce document de stratégie consistera à procéder au lancement de procédures pour commencer à utiliser les expériences extérieures et partager ses propres observations dans le domaine de la cybersécurité.

4.4

Pilier 4 : renforcement des mécanismes de poursuite efficace des crimes et délits de cybersécurité

La cybersécurité est un enjeu majeur pour la protection des droits et des libertés des citoyens, ainsi que pour la défense des intérêts nationaux. Face à la multiplication et à la diversification des menaces en ligne, il est nécessaire de renforcer le mécanisme national de poursuite des délits et des crimes de cybersécurité. Ce mécanisme vise à garantir une réponse pénale efficace et proportionnée aux infractions commises sur le cyberespace, en tenant compte de leur gravité, de leur impact et de leur caractère transnational. Il implique une coopération étroite entre les autorités judiciaires, les services de police et de renseignement, les acteurs du secteur privé et les partenaires internationaux

4.4.1.

Règles pour la collecte de preuves numériques

La preuve numérique est tout à fait différente des autres preuves matérielles. Les preuves numériques sont faciles à recueillir, mais il pourrait s'avérer difficile d'en évaluer l'authenticité et de les protéger contre toute modification. Les preuves numériques peuvent être accessibles de n'importe où dans le monde, il est donc essentiel de définir des règles concernant :

- leur lieu de stockage ;
- le contrôle d'accès à leur contenu ;
- la durée de stockage ;
- les moyens de les protéger contre toute modification ;
- les mécanismes de transmission des preuves numériques.

Le transfert de preuves numériques entre deux sujets autorisés peut prendre un temps important. Le chemin du transfert peut avoir plusieurs milliers de kilomètres de distance et de milliers de stations informatiques d'échange situées dans des dizaines de pays. La définition des règles nécessitera une coopération étroite avec les entreprises de télécommunications au niveau local et international.

RESPONSABILITÉ

- AGENCE NATIONALE DE LA CYBERSÉCURITÉ (ANCy)

PARTICIPANTS

1. MINISTÈRE DE LA JUSTICE ET DE LA LÉGISLATION ;
2. POLICE NATIONALE ;
3. GENDARMERIE NATIONALE.

INTERVENTIONS

1. Établir un ensemble de règles techniques pour la collecte de preuves numériques

À cette fin, il est nécessaire de définir : les types de données pouvant être considérées comme des éléments de preuve à recueillir, les types de sources de données et les mécanismes de sécurité de base pour garantir l'intégrité et la confidentialité des données. Les règles en matière de preuve devraient couvrir la gestion des données tout au long du cycle de traitement (collecte, traitement, sauvegarde, stockage, suppression) tout en maintenant la responsabilité de l'opération, qui est le facteur le plus important pour que les données recueillies soient finalement considérées comme des éléments de preuve devant un tribunal. L'élaboration d'une approche par processus signifie :

- la collecte des moyens – prélèvement d'échantillons de preuves (enregistrements des opérateurs de télécommunications) ;
- les moyens de traitement – examiner le matériel et évaluer si le matériel recueilli peut être considéré comme un élément de preuve ;
- les techniques de sauvegarde – consigner la preuve dans un format approprié pour éviter toute modification non autorisée ;
- les moyens de stockage – placer les éléments de preuve dans un endroit sûr pour empêcher tout accès non autorisé ;
- la suppression effective des données du système lorsque cela est légalement autorisé.

Les étapes susmentionnées seront détaillées dans la partie technique de l'ensemble de règles relatives à la collecte de preuves numériques.

2. Définir et mettre en place un cadre harmonisé pour la conservation des données avec les acteurs clés du secteur

4.4.2.

Créer une entité unique en charge de la lutte contre la cybercriminalité

La lutte contre la cybercriminalité au Togo s'organise autour de trois grandes entités, la Police Nationale, la Gendarmerie Nationale et l'Agence Nationale de la Cybersécurité (ANCy) via son bras opérationnel, Cyber Defense Africa (CDA).

Ce travail en silo, limite la coopération, ralentit les investigations et augmente les coûts de la lutte contre la cybercriminalité. Ces trois (3) entités utilisent les mêmes technologies, les mêmes compétences et les mêmes procédures pour leurs missions d'investigations mais ne créent pas de synergies ni d'économies d'échelles.

Cette répartition au Togo empêche également d'avoir une vision globale de la problématique, une stratégie efficace de lutte contre la cybercriminalité et un interlocuteur unique pour l'ensemble des parties prenantes notamment les opérateurs de télécommunications.

En outre, la lutte contre la cybercriminalité passe par la collecte effective des preuves numériques. Or elles sont différentes des autres preuves matérielles. Les preuves numériques sont très difficiles à collecter et à protéger contre les modifications. Certaines preuves numériques ne se produisent pas sur la « scène du crime » et doivent être protégées sur le réseau qui relie l'attaquant et la victime. Ce réseau peut être long de plusieurs milliers de kilomètres et relié par des milliers d'équipements informatiques situés dans des dizaines de pays. Cela nécessite une coopération étroite avec les entreprises de télécommunications au niveau local et international, et le renforcement des capacités des laboratoires numériques de criminalistique, qui permettront de mener des travaux de restauration de l'utilité des preuves.

RESPONSABILITÉ

AGENCE NATIONALE DE LA CYBERSÉCURITÉ

PARTICIPANTS

1. MINISTÈRE DE LA SÉCURITÉ ET DE LA PROTECTION CIVILE ;
2. MINISTÈRE DES ARMÉES ;
3. MINISTÈRE DE LA JUSTICE ET DE LA LÉGISLATION ;
4. POLICE NATIONALE ;
5. GENDARMERIE NATIONALE ;
6. AGENCE NATIONALE DE LA CYBERSÉCURITÉ (ANCy).

INTERVENTIONS

Créer une entité unique en charge de la lutte contre la cybercriminalité

Le but premier est de réunir les compétences en numérique aujourd'hui dispersées dans plusieurs unités de police et de gendarmerie en une seule. Cela pour créer des synergies, mutualiser et rendre plus efficace la lutte contre la cybercriminalité.

Cette entité ainsi composée d'experts en numérique et en cybersécurité pourra concevoir, implémenter, maintenir et exploiter tous les projets de lutte contre la cybercriminalité.

Elle aura pour missions globales :

1. d'être le point focal sur la lutte contre la cybercriminalité et des projets liées au numérique et à la sécurité ;
2. de mettre en place et opérer le laboratoire national de criminalistique numérique ;
3. de former les agents et les accompagner au changement ;
4. de collecter, traiter, analyser et publier les statistiques y compris sur la cybercriminalité au Togo.

Cette entité composée d'agents de la Police, de la Gendarmerie et de civils assermentés sera le noyau dur d'une grande entité opérationnelle dédiée à la sécurité publique avec des outils de lutte contre la cybercriminalité, la remontée d'information (centre d'appel du type police secours), la lutte contre les fausses informations (fake news), etc.

Cette entité opérera un laboratoire de criminalistique numériques sur la base de directives précises. Les activités du laboratoire devraient porter sur la recherche scientifique, les travaux de développement dans le domaine de la criminalistique, en particulier les techniques criminalistiques utilisées dans le processus de prévention, de détection et de lutte contre la cybercriminalité, ainsi que les travaux d'expertise, d'analyse et de formation. Il s'agira également de mettre au point des méthodes, des normes et des règles applicables au travail des investigateurs numériques dans les unités de police et de gendarmerie.

Elle sera en soutien aux autres forces de sécurité de la nation (Police, Gendarmerie, FAT, Sapeurs-pompiers, gardes forestiers, douanes, protection des frontières, etc...).

4.4.3.

Mettre en œuvre le droit pénal de la cybersécurité

Il est important d'indiquer clairement les procédures et les réglementations spécifiques dans le domaine de la lutte contre la cybercriminalité. Afin de garantir la haute compétence des juges dans le domaine de la cybersécurité et la lutte contre la cybercriminalité, il est nécessaire d'accroître leurs connaissances. Cela suppose la participation des juges à une formation régulière.

RESPONSABILITÉ

AGENCE NATIONALE DE LA CYBERSÉCURITÉ

PARTICIPANTS

1. MINISTÈRE DE LA JUSTICE ET DE LA LÉGISLATION ;
2. MINISTÈRE DE LA SÉCURITÉ ET DE LA PROTECTION CIVILE.

ACTIVITÉS

1. Définir la réglementation et les procédures relatives à la cybercriminalité.

Les autorités policières et judiciaires sont confrontées à de multiples obstacles et incertitudes concernant les procédures liées à la cybercriminalité surtout lors de la collecte de preuves numériques de nature transfrontalière.

Il faut donc adapter la réglementation et les procédures pénales pour faire face à l'intangibilité et à la volatilité de la preuve numérique sans créer d'incertitude juridique.

Les procédures et les réglementations devraient également fixer les limites des activités de la police et des laboratoires judiciaires et fournir des outils juridiques pour détecter et poursuivre les infractions criminelles.

¹⁸ Ministère de la justice et de la législation (<https://justice.gouv.tg/>)

¹⁹ Ministère de la Sécurité et de la Protection Civile (<https://securite.gouv.tg/>)

ACTIVITÉS (SUITE)

2. Former les juges sur les procédures et la réglementation en matière de cybersécurité.

Un programme de formation à l'intention des juges qui seront chargés de trancher sur les délits et les crimes de cybercriminalité sera élaboré et mis en place. Le programme de formation fournira une introduction au domaine de la sécurité de l'information et du système national de cybersécurité, discutera des menaces et des défis et fournira des informations sur les effets potentiels des activités criminelles. Le programme destiné aux juges vise à rendre la prise de décision efficace et efficiente dans le domaine des procédures judiciaires.

5.

Gestion de la stratégie nationale de cybersécurité

5.1.

Suivi et Evaluation de la stratégie via les résultats du SOC National et du CERT.tg

La stratégie nationale de cybersécurité couvre la période allant de 2024 à 2028.

La stratégie est en lien avec le PND et la feuille de route gouvernementale. Sa mise en œuvre concerne tous acteurs de développement, notamment, les ministères, les partenaires techniques et financiers, le secteur privé, les ONG internationales et Organisations de la Société Civile (OSC), chacun dans son domaine de compétences. La stratégie est placée sous la tutelle de la Primature. A cet égard, cette dernière apportera des facilitations nécessaires pour une mise en œuvre réussie de la stratégie.

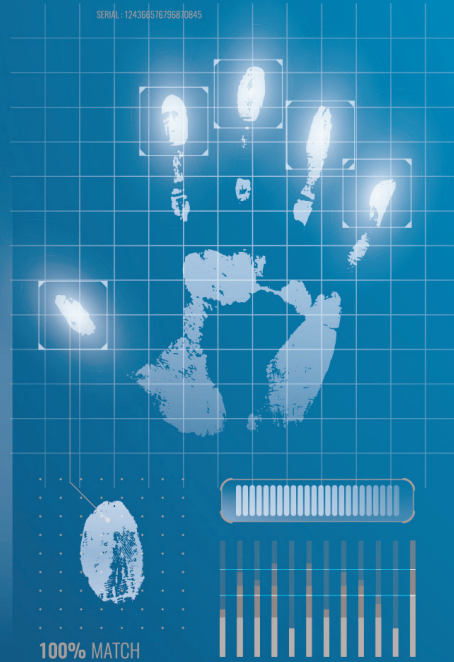
La stratégie sera supervisée par le Comité stratégique présidé par le Premier ministre. La coordination de mise en œuvre du programme sera assurée par l'Agence nationale de cybersécurité (ANCy). Le coordonnateur de la mise en œuvre de la stratégie de cybersécurité est donc le Directeur Général de l'Agence nationale de la cybersécurité. L'ANCy dans la coordination de la mise en œuvre et le suivi-évaluation de la stratégie va s'appuyer sur un Comité technique dont les membres seront les points focaux désignés par chaque ministère impliqué dans la mise en œuvre de la stratégie.

FACE RECOGNITION SYSTEM



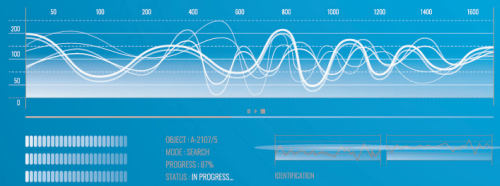
HAND RECOGNITION SYSTEM

SERIAL: 124306576795810845



VOICE IDENTIFICATION SYSTEM

SERIAL: 124306576795810867



FINGERPRINT RECOGNITION SYSTEM

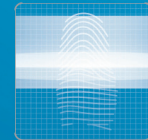
SERIAL: 124306576795810867

CURL-SHAPED



OBJECT: A-2107/2
MODE: SEARCH
STATUS: COMPLETE

WAVEY-SHAPED



OBJECT: A-2107/3
MODE: SCANNING
PROGRESS: 45%
STATUS: IN PROGRESS

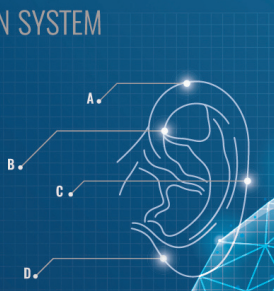
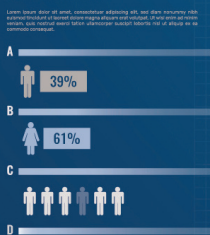
ARCH-SHAPED LOOK



OBJECT: A-2107/1
MODE: SCANNING
PROGRESS: 57%
STATUS: IN PROGRESS

EAR IDENTIFICATION SYSTEM

SERIAL: 124306576795810867



EYES SCANNER

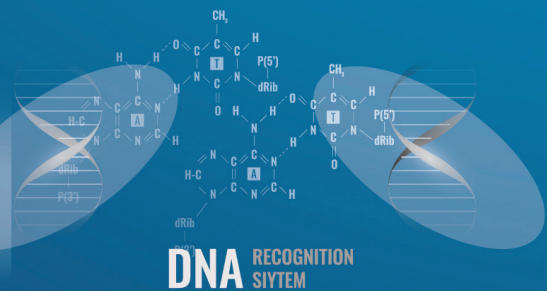
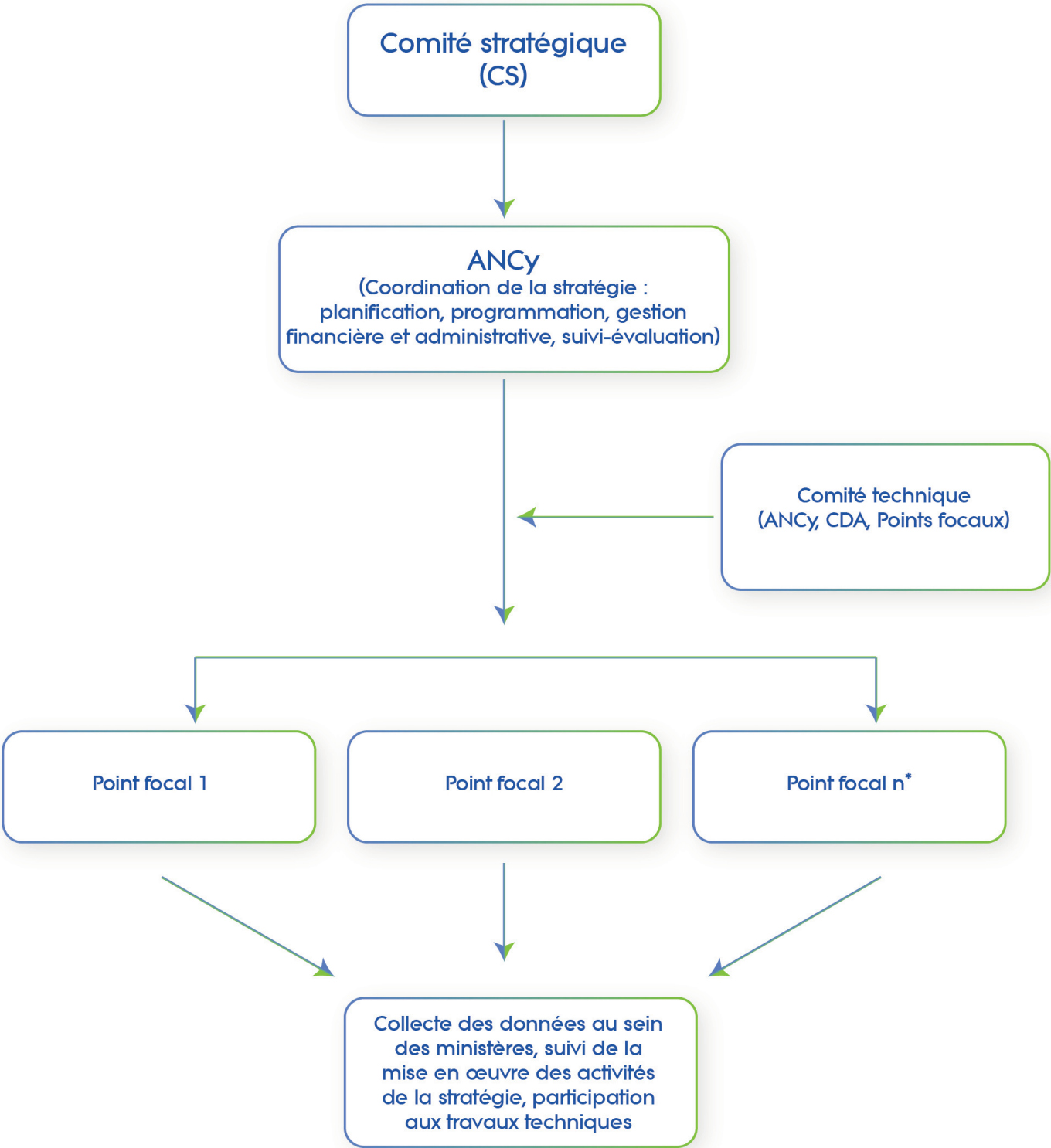


Tableau 1 : Cadre de coordination de la stratégie

ORGANES	ROLES ET MISSIONS	MEMBRES
Comité stratégique (Cs)	Le CS va assurer la coordination de la stratégie. Le CS est créé par décret pris en conseil des ministres. Il est présidé par le Premier ministre. Le CS a pour mission de : ✓ définir les orientations et les directives politiques de la mise œuvre de la stratégie ; ✓ assurer une communication et une information intersectorielle effective ; ✓ mobiliser les ressources internes et externes pour la mise en œuvre de la stratégie ; ✓ valider les rapports annuels de mise en œuvre de la stratégie ; ✓ approuver les budgets et programmes annuels de mise en œuvre de la stratégie. Il se réunit une fois tous les trois mois.	Les membres du CS sont nommés en Conseil des ministres et sont composés de : - o du/de la premier ministre ; - o du/de la ministre de l'économie numérique (MEN) ; - o du/de la ministre de la sécurité - o du/de la garde des sceaux, ministre de la justice et de la législation ; - o du/de la ministre des armées ; - o deux personnalités de la Présidence.
ANCY	L'ANCy va assurer la coordination de la stratégie nationale de la cybersécurité et aura comme mission : ✓ préparer et faire adopter les outils de gestion et de suivi-évaluation de la stratégie ; ✓ préparer les documents à soumettre à la validation du comité stratégique ; ✓ assurer le suivi de la mise en œuvre des interventions ; ✓ élaborer et soumettre les rapports périodiques sur la mise en œuvre des activités de la stratégie au CS ; ✓ préparer les revues à mi-parcours et d'évaluation finale de la stratégie ; ✓ tenir des réunions périodiques de suivi de l'exécution des activités planifiées avec tous les Points Focaux de toutes les parties prenantes pour s'assurer de l'évolution des activités ; ✓ prendre part aux réunions du CS dans le cadre de la mise en œuvre et le suivi-évaluation de la stratégie nationale de cybersécurité	L'ANCy est mise en place par décret n°--Le directeur général de l'ANCy est le Coordonnateur national de la stratégie.
Comité technique	Le Comité technique est la structure opérationnelle de l'ANCy dans la coordination et la mise en œuvre de la stratégie. Il a pour rôle d'appuyer l'ANCy dans l'élaboration de certains documents qui seront soumis à l'approbation du comité stratégique et dans la validation technique de certains documents/outils.	Il est présidé par le Directeur général de l'ANCy et est composé des points focaux désignés par chaque ministère impliqué dans la mise en œuvre de la stratégie. Il va se réunir périodiquement et à chaque fois que le besoin se présente. Les Points focaux ont l'obligation de transmettre régulièrement à l'ANCy l'état de mise en œuvre des activités de la stratégie relevant de leur ministère.

Figure 1 : Dispositif institutionnel de coordination de la stratégie nationale de cybersécurité



* Les points focaux sont assignés à chaque ministère

5.2.

Instruments de planification et de mise en œuvre de la stratégie nationale de cybersécurité 2024-2028

L'opérationnalisation de la stratégie se fonde sur la mise en œuvre du plan d'action opérationnel qui contient les activités à mettre en œuvre en vue de l'atteinte de ses objectifs. Un cadre de mesure des indicateurs de performance et de suivi-évaluation est également défini.

Dans un délai de six mois à compter de l'adoption de la stratégie de cybersécurité, le coordonnateur élabore et soumet à l'approbation du conseil des ministres un plan d'action pour la mise en œuvre de la stratégie de cybersécurité. Lors de l'élaboration du plan d'action, les autorités susmentionnées tiennent compte des questions de cybersécurité dans les limites de leurs compétences statutaires.

Le plan d'action comprendra notamment :

- 1) Le nom de l'objectif spécifique ;
- 2) Le nom de la tâche ;
- 3) Le nom de l'action servant à l'exécution de la tâche ;
- 4) Le type d'action : action législative, organisationnelle, technologique, éducative, information, promotion et autre ;
- 5) Le calendrier : date de début et date d'achèvement de l'initiative entreprise ;
- 6) L'organisme ou les organismes : l'organisme chef de file et les organismes coopérant à l'exécution de la tâche (le cas échéant) ;
- 7) Les KPIs
- 8) Les effets escomptés de la mise en œuvre de l'action ;
- 9) Le coût estimé de la mise en œuvre de l'action.

Le plan d'action comprend des activités de type projet, caractérisées par le début et la fin de la période de mise en œuvre et par les produits résultant de la mise en œuvre de l'activité. Une revue annuelle du plan d'action sera effectuée afin d'évaluer l'état d'avancement des activités.

Les instruments ci-dessous permettront une meilleure planification et une mise en œuvre efficace de la stratégie. Il s'agit de :

- Budget de l'Etat : tous les ministères impliqués dans la mise en œuvre de la stratégie doivent inscrire les actions qui les concernent dans leur enveloppe budgétaire. En outre, l'enveloppe budgétaire de l'ANCy devra lui permettre d'exécuter année par année durant les cinq années de mise en œuvre de la stratégie, les activités dont elle a la charge ;

- Plan de Travail et Budget Annuel (PTBA) : les activités à mettre au cours d'une année doivent être inscrites dans le PTBA de chaque ministère impliqué. Toutefois, un plan de travail annuel consolidé au titre de la stratégie devra être élaboré par l'ANCy et soumis à l'approbation du Comité stratégique.

5.3.

Facteurs de risques de la stratégie nationale de cybersécurité 2024-2028

- **Risque lié à l'instabilité socio-politique** : la paix sociale constitue un facteur important qui favorise le respect des droits humains et des libertés individuelles garantissant ainsi une bonne exécution de la stratégie.

- **Risque lié à la situation sécuritaire** : les menaces terroristes font peser des risques sécuritaires sur les pays, ce qui pourrait compromettre tous les efforts de développement consentis. Le Togo doit donc concentrer ses priorités sur la lutte contre le terrorisme et la criminalité organisée afin de favoriser une mise en oeuvre efficace et efficiente de la stratégie.

- **Risque lié au financement** : Le schéma de financement de la stratégie se fonde essentiellement sur les ressources internes. Or, la capacité du Togo à mobiliser des ressources internes reste encore faible. En outre, les procédures de mobilisation des ressources externes demeurent assez lourdes en dépit des efforts accomplis dans le cadre de la recherche mutuelle de l'efficacité de l'aide. Tous ces éléments constituent un risque réel pour la disponibilité des moyens financiers et par ricochet un risque majeur d'échec de la stratégie.

Ce risque d'une insuffisante mobilisation des financements nécessaires à la mise en oeuvre de la stratégie ne pourra être réduit qu'au prix d'un effort accru de mobilisation des ressources internes et d'un redéploiement de la coopération économique extérieure afin de diversifier les partenariats au développement, etc.

- **Risque lié aux insuffisances de capacités** : le succès de la stratégie dépendra en grande partie du cadre de pilotage. De nouvelles formes d'association des acteurs de développement (acteurs publics, privés et OSC) s'avère nécessaire. La nouveauté de ces approches comporte un risque qu'il faudra minimiser par le renforcement des capacités des acteurs étatiques à encadrer et suivre la réalisation des activités sur le terrain. La réussite de la stratégie suppose également que les ressources nécessaires soient disponibles dans les délais.

Par ailleurs, la réussite de la stratégie nécessite des acteurs communautaires motivés et dévoués et qui disposent des moyens adéquats pour appuyer la mise en oeuvre des activités de la stratégie.

- **Risque de catastrophes naturelles et crises sanitaires** : les catastrophes naturelles et les crises naturelles créent des instabilités, et entraînent des déplacements de population, ce qui n'est pas de nature à favoriser la mise en oeuvre des activités de développement. Les périodes de crise entraînent le plus souvent une réorientation des priorités de développement, ce qui pourrait affecter les ressources nécessaires à la mise en oeuvre de la stratégie.

6.

Financement de la stratégie nationale de cybersécurité

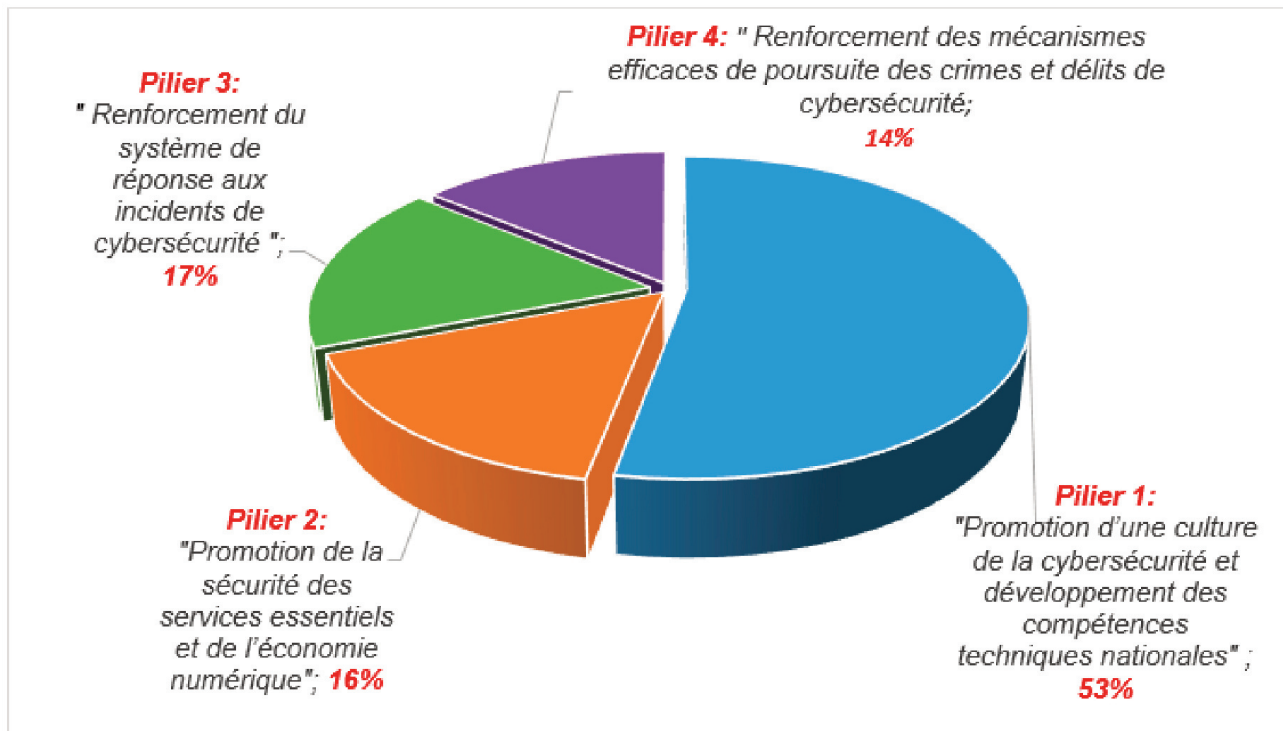
En vertu de la législation actuelle, les entités de mission publique sont tenues d'inclure les dépenses de cybersécurité dans leurs plans financiers.

Les sources de financement pour la mise en oeuvre des activités décrites dans le document seront précisées dans les plans financiers des différentes entités participant à la mise en oeuvre de la stratégie de cybersécurité.

Les partenariats public-privé (PPP) sont encouragés pour minimiser les dépenses sur les deniers publics, les durées de mise en oeuvre et maximiser la qualité de service. Le Ministre de l'économie numérique et de la transformation digitale (MENTD) est ordonnateur du Fonds de souveraineté numérique qui a pour objectif de financer toutes les actions à mener pour protéger et garantir la souveraineté numérique du Togo. Ces actions comprennent la mise en place du CERT national, la fourniture de services de SOC aux administrations publiques, la formation des fonctionnaires à la cybersécurité et d'autres activités connexes.

D'autres mécanismes de financement seront mis en place à mesure que le marché togolais de la cybersécurité se développe.

Figure 2 : Répartition du coût global de la stratégie par pilier



7.

Cadre de suivi et d'évaluation de la stratégie nationale de cybersécurité

7.1.

Mécanismes du suivi de la stratégie nationale de cybersécurité 2024-2028

Afin de garantir l'atteinte des objectifs poursuivis, la stratégie doit être accompagnée d'un dispositif de suivi évaluation. Ce système de suivi évaluation sera assuré par l'ANCy.

Le suivi-évaluation de la stratégie permettra de s'assurer que les activités planifiées :

- sont mises en œuvre conformément au planning des activités et qu'il existe une cohérence/harmonie entre les interventions ;
- permettent d'atteindre les résultats escomptés ;
- sont efficaces, appropriées par les parties prenantes et gérées de façon pérenne ;
- sont pertinentes par rapport aux besoins et aux priorités de développement ;
- sont suivies de façon à pouvoir identifier à temps les goulots d'étranglement et les facteurs de risques.

Pour ce faire, l'ANCy va élaborer les outils de collecte de données, les canevas de rapports, le circuit de transmission des données et des rapports, les plans d'analyse et de traitement des données adaptés aux besoins de la cible qui seront validés par l'ensemble des acteurs impliqués au sein du comité technique composés des points focaux.

En vue d'assurer un bon circuit de l'information et que les rapports soient validés à chaque niveau d'intervention, toutes les parties prenantes, notamment, les points focaux sont responsables du cadre de suivi évaluation et devront ainsi faire des rapports trimestriels et les envoyer à l'ANCY.

L'ANCy vérifie, synthétise, et élabore le rapport annuel sur l'état d'avancement de la mise en œuvre de la stratégie et le remonte au Comité technique.

Le comité technique de la stratégie vérifie, examine et valide techniquement les rapports annuels élaborés par l'ANCy. Les rapports validés par le comité technique sont transmis au comité stratégique pour approbation.

7.2.

Mécanismes d'évaluation de la stratégie nationale de cybersécurité 2024-2028

La stratégie nationale de cybersécurité a prévu deux évaluations :

- Evaluation à mi-parcours en 2026

Deux ans après le démarrage de sa mise oeuvre, le document de stratégie fera l'objet d'une évaluation à mi-parcours. Les résultats de l'évaluation seront résentés au comité stratégique de l'Agence nationale de la cybersécurité. Les procédures et modalités de cette évaluation seront déterminées par l'ANCy. Les résultats validés seront partagés à l'ensemble des acteurs.

À la suite de cet examen, l'Agence nationale de la cybersécurité élabore une proposition de mesures correctives qui seront soumises à l'approbation du Comité stratégique.

- Evaluation finale en 2028

En fin d'année 2028, une évaluation finale sera organisée. Les termes de référence de cette évaluation seront élaborés par l'ANCy et soumis au comité stratégique pour validation. Les procédures et modalités de cette évaluation seront déterminées par le comité stratégique. Les résultats de l'évaluation finale seront soumis à validation et partagés.

Les résultats de cette évaluation finale permettront d'élaborer la deuxième génération de la stratégie nationale de cybersécurité pour les prochains cinq ans.

Annexes

Annexe 1

Cadre légal et réglementaire relatif à la cybersécurité du Togo

1. Communications électroniques

Loi :

- Loi n°2012-18 du 17 décembre 2012 sur les communications électroniques modifiée par la loi N°2013-003 du 19 février 2013

Cette loi organise le secteur des communications électroniques et définit les rôles de chaque partie prenante et leurs relations.

2. Transactions électroniques

Lois et Règlements :

- Loi n°2017-007 du 12 juin 2017 relative aux transactions électroniques ;
- Décret n°2018-062 du 21 mars 2018 portant règlement des transactions et services électroniques au Togo ;
- Arrêté n°016/MPEN/CAB du 17 décembre 2018 fixant les conditions de reconnaissance au Togo des certificats et signatures électroniques délivrés par des prestataires de services de confiance établis hors du territoire national.

La loi sur les transactions électroniques s'applique aux transactions et aux services par voie électronique et traite :

- les certificats / signatures électroniques et leur reconnaissance juridique ;
- les informations à mettre à la disposition des clients sur les personnes exerçant une activité de commerce électronique ;
- les informations qui doivent être mises à la disposition du public par les éditeurs en ligne de services de communication publique ;
- les données permettant l'identification de toute personne ayant contribué à la création du contenu ou de l'un des éléments du contenu des services des prestataires ;
- l'autorité de certification.

3. Société de l'information

Loi :

- Loi n°2017-006 du 22 juin 2017 d'orientation sur la société de l'information au Togo (LOSITO)

Cette loi définit les objectifs et les principales orientations de la société de l'information au Togo.

4. Cybersécurité

Lois et Règlements :

- loi n°2016-006 du 30 mars 2016 portant liberté d'accès à l'information et à la documentation publique ;
- loi n°2017-007 du 22 juin 2017 relative aux transactions électroniques ;
- loi n°2018-026 du 7 décembre 2018 modifiée par la loi n°2022-009 du 22 juin 2022 sur la cybersécurité et la lutte contre la cybercriminalité ;
- loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;
- décret n°2017-104 du 30 octobre 2019 relatif aux modalités d'application de la loi n° 2016-06 du 30 mars 2016 portant liberté d'accès à l'information et à la documentation publiques ;
- décret n°2018-062/PR du 21 mars 2018 portant réglementation des transactions et services électroniques au Togo ;
- décret n°2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence Nationale de la Cybersécurité (ANCy) ;
- décret n°2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels (OSE), aux infrastructures essentielles et aux obligations y afférentes ;
- arrêté N° 2022-040 /PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République Togolaise ;
- décret N°2022-090/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance en cybersécurité et des produits de cybersécurité et à l'agrément des centres d'évaluation

La loi sur la cybersécurité définit les mécanismes de promotion de la cybersécurité et établit le cadre de la lutte contre la cybercriminalité, ainsi que les peines pour les crimes et délits numériques.

La loi sur la cybersécurité prévoit la création de l'Agence Nationale de la Cybersécurité (ANCy), chargée de la mise en œuvre effective des orientations et mesures stratégiques, et du Fonds de souveraineté numérique, qui contribue notamment au financement de la mise en œuvre des stratégies nationales de cybersécurité et soutient les actions de l'ANCy.

5. Protection des données à caractère personnel

Loi :

- Loi n° 2019-014 du 29 Octobre 2019 relative à la protection des données à caractère personnel.
- décret n°2020-111 /PR du 9 décembre 2020 portant organisation et fonctionnement de l'instance de protection des données à caractère personnel

Cette loi vise à mettre en place un cadre juridique et institutionnel permettant de protéger efficacement les libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel.

Les textes prévoient également la création de l'Autorité de protection des données à caractère personnel, l'Instance de Protection des Données à Caractère Personnel (IPDCP).

Stratégie Nationale de Cybersécurité

2024-2028



Stratégie Nationale de Cybersécurité 2024-2028

Agence Nationale de la Cybersécurité (ANCy)

Adresse : 63 Bd du 13 Janvier,
Nyékonakpoè, Lomé-TOGO
07 BP 7878
+228 97 52 58 58
+228 70 60 60 83