ANCy
Agence Nationale de la Cybersécurité

ETAT DES LIEUX DE LA CYBERCRIMINALITÉ AU TOGO

2023

AGENCE NATIONALE DE LA CYBERSECURITÉ LOMÉ - TOGO

ETAT DES LIEUX DE LA CYBERCRIMINALITÉ AU TOGO

2023

SOMMAIRE

INTRODUCTION 6

ANALYSE DE L'ETAT DE LA CYBERCRIMINALITÉ AU TOGO . . 8

A. Le développement des technologies de l'information et de la communication au Togo 9

B. Le cadre juridique et institutionnel relatif à la cybercriminalité au Togo 10

1. Les conventions internationales ratifiées par le Togo en matière de cybersécurité 10

2. Les lois nationales adoptées par le Togo pour prévenir et réprimer la cybercriminalitété 11

3. Les statistiques de la cybercriminalité au Togo 12

4. Les facteurs favorisant la cybercriminalité au Togo 13

LA LUTTE CONTRE LA CYBERCRIMINALITÉ AU TOGO 15

C. Les principales cybermenaces au Togo 18

1. Escroqueries en ligne 18

2. Extorsion en ligne 19

3. Escroqueries aux faux ordres de virement 20

4. Rancongiels 24

D. Impact de la cybercriminalité 25

E. Mesures contre la cybercriminalité 27

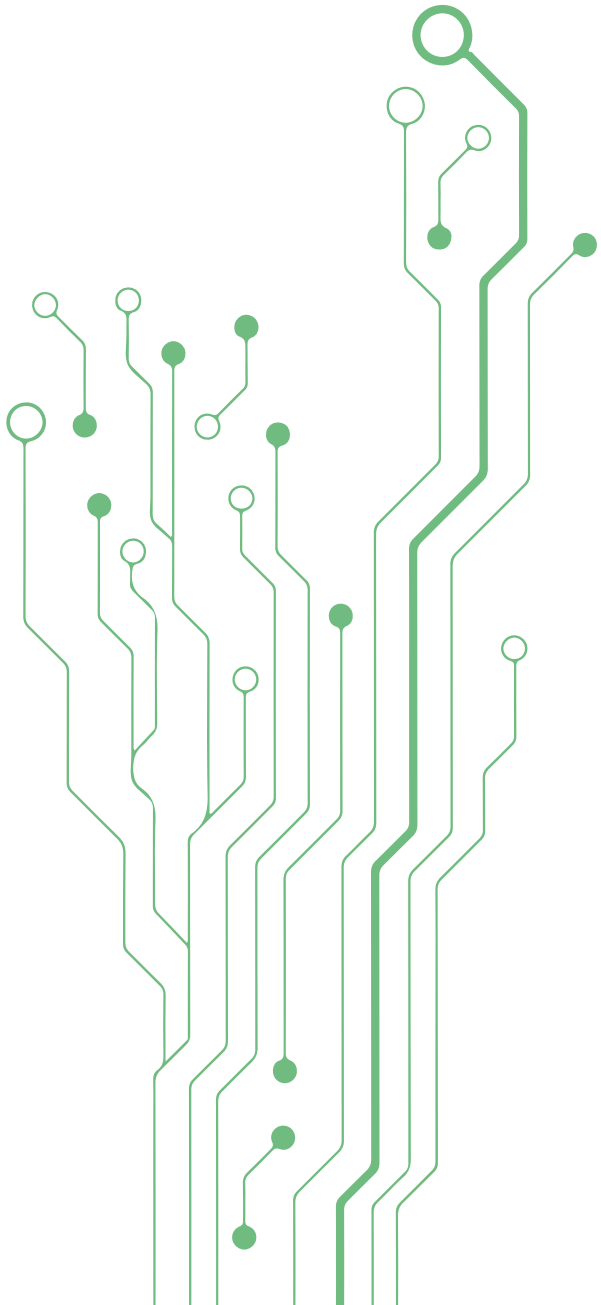
F. Les perspectives 28

CONCLUSION 30


//mobile


teNotice">…
mw-indicators">
firstHeading" class="
bodyContent" class="
siteSub" class="
contentSub">
contentSub2">
jump-to-nav">
mw-jump-link" href="
mw-jump-link" href="
mw-content-text" class="
mw-parser-output">
</noscript>
printfooter" data-
catlinks" data-

INTRODUCTION



De nos jours, il ne fait plus aucun doute que les technologies de l'information et de la communication (TIC) constituent un enjeu majeur pour le développement de l'Afrique. Cependant, elles sont devenues des moyens de réalisation d'activités criminelles dont Internet constitue désormais un vecteur privilégié de propagation.

En effet, Internet n'est plus le réseau libre et ouvert, tourné vers le partage du savoir, dont certains de ses concepteurs avaient rêvé. Il est maintenant devenu le moyen d'expression d'une nouvelle forme de criminalité informatique. Qu'on l'appelle cybercrime, délinquance informatique, criminalité des hautes technologies, criminalité informatique, criminalité numérique, la cybercriminalité constitue une véritable menace pour la sécurité des réseaux informatiques, celle des cybercitoyens et cyberconsommateurs dont la protection reste très précaire ainsi que pour le développement de la société de l'information et de l'économie du savoir dans notre pays.

Cette grave menace, sans frontières et à laquelle tous les pays sont confrontés, connaît actuellement une amplification sans précédent. Cette tendance est accentuée par la fracture numérique : « l'hypo-connexion » des régions reculées et encore enclavées de notre pays, l'ignorance de nombreux usagers qui va de pair avec le manque de maturité du dispositif de lutte contre la cybercriminalité qui n'est qu'à ses prémices.

Cette menace risque malheureusement de durer longtemps, car il appert qu'Internet sera l'objet d'un nombre grandissant de crimes simplement parce que c'est par son truchement que les transactions humaines et commerciales se font de plus en plus.

Au Togo, cette pratique que l'on croyait propre au Nigéria, au Benin et à la Côte d'Ivoire et qui a débuté dans les années 2000, s'est très tôt généralisée, au fil des ans, chez les jeunes. Il est en effet noté, au niveau des internautes, un usage sophistiqué et novateur d'Internet qui englobe les différentes sphères d'activités avec une orientation privilégiée dans la criminalité numérique. Escroqueries de toutes sortes, mensonges, piratage de systèmes informatiques privés ou étatiques, sont autant de crimes pratiqués par les cyber délinquants qui font perdre à Internet son « innocence ».

Dans la mesure où ce phénomène menace la sécurité et le développement de notre pays qui ambitionne de se positionner comme une référence en matière de services numériques en Afrique de l'Ouest, cette étude vise à identifier les acteurs, les formes, les causes, les conséquences et les moyens de lutte contre ce fléau.

ANALYSE DE L'ETAT DE LA CY-BERCRIMINALITÉ AU TOGO

A. Le développement des technologies de l'information et de la communication au Togo

Les technologies de l'information et de la communication (TIC) sont des outils qui permettent de créer, de traiter, de stocker, d'échanger et de diffuser des informations sous différentes formes (texte, image, son, vidéo, etc.). Elles regroupent notamment l'informatique, l'internet, le téléphone mobile, la télévision numérique, etc.

Les TIC ont connu un essor considérable au Togo ces dernières années, grâce à plusieurs facteurs tels que :

- La libéralisation du secteur des télécommunications en 1998, qui a permis l'entrée de nouveaux opérateurs privés sur le marché et a favorisé la concurrence et la baisse des tarifs ;
- L'extension du réseau national de fibre optique en 2012, qui a permis d'améliorer la qualité et la couverture du service internet haut débit sur tout le territoire ;
- Le déploiement du réseau 4G en 2017, qui a permis d'offrir une connexion internet plus rapide et plus performante aux utilisateurs de smartphones ;
- Le développement des services numériques innovants dans divers domaines tels que l'éducation, la santé, l'administration publique, le commerce électronique, etc.

Selon les données du ministère des Postes et de l'Economie numérique du Togo, le taux de pénétration du téléphone mobile était de 83% en 2019, soit environ 6 millions d'abonnés. Le taux d'accès à internet était quant à lui de 35%, soit environ 2,5 millions d'internautes. Le nombre d'utilisateurs des réseaux sociaux était estimé à 1 million en 2019.

Ces chiffres montrent que le Togo dispose d'un potentiel important en matière de développement des TIC.

Toutefois, ils révèlent également que notre pays fait face à plusieurs défis tels que :

- La fracture numérique entre les zones urbaines et rurales ;
- Le coût élevé des équipements et des services ;
- Le faible niveau d'alphabétisation numérique ;
- La vulnérabilité aux cybermenaces.

B. Le cadre juridique et institutionnel relatif à la cybercriminalité au Togo

1. Les conventions internationales ratifiées par le Togo en matière de cybersécurité

Le Togo a ratifié plusieurs conventions internationales relatives à la cybersécurité, qui constituent un cadre normatif commun pour harmoniser les législations nationales, faciliter l'entraide judiciaire et renforcer la coopération entre les Etats.

Parmi ces conventions figurent :

- La Convention des Nations Unies contre la criminalité transnationale organisée (dite Convention de Palerme), adoptée en 2000 et entrée en vigueur en 2003. Elle vise à prévenir et combattre les formes graves de criminalité organisée qui impliquent des groupes criminels transnationaux. Elle contient notamment un protocole additionnel sur la prévention, la répression et la sanction du trafic illicite des migrants par terre, air et mer (dite Protocole contre le trafic illicite des migrants), qui traite notamment du phénomène des «brouteurs», c'est-à-dire des escrocs qui utilisent internet pour soutirer de l'argent aux victimes sous divers prétextes (amour, héritage, loterie, etc.).

- La Convention africaine sur la cybersécurité et la protection des données à caractère personnel (dite Convention de Malabo), adoptée en 2014 par l'Union africaine. Elle vise à harmoniser les législations nationales des Etats membres dans les domaines de la cybersécurité et de la protection des données personnelles. Elle reprend les dispositions essentielles de la Convention de Budapest sur les infractions pénales liées aux systèmes informatiques, et y ajoute d'autres infractions spécifiques au contexte africain, telles que le racisme, la xénophobie, le négationnisme ou l'apologie du génocide sur internet.

Elle prévoit également des mesures relatives à la prévention, à l'éducation, à la sensibilisation, à la recherche, à l'innovation et à la coopération régionale.

Le Togo a ratifié ces deux conventions internationales respectivement en 2005 et en 2018. Il s'est ainsi engagé à respecter les obligations qui en découlent et à adapter sa législation nationale aux normes internationales.

2. Les lois nationales adoptées par le Togo pour prévenir et réprimer la cybercriminalitété

Le Togo a adopté plusieurs lois nationales pour prévenir et réprimer la cybercriminalité, en tenant compte des conventions internationales ratifiées.

Parmi ces lois figurent :

• la loi n°2008-005 du 30 janvier 2008 relative aux transactions électroniques ;

• la loi n° 2018-026 du 07 décembre 2018, modifiée par la loi n°2022-009 du 24 juin 2022 sur la cybersécurité et la lutte contre la cybercriminalité ;

• le décret n° 2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;

• la loi n° 2019-014 du 29 Octobre 2019 relative à la protection des données à caractère personnel ;

• l'arrêté n° 2022-040/PMRT portant adoption des règles de cybersécurité en République togolaise.

3. Les statistiques de la cybercriminalité au Togo

La cybercriminalité est un phénomène qui touche de nombreux pays dans le monde, y compris le Togo.

Selon la cellule de lutte contre la cybercriminalité de la police nationale, le préjudice financier de la cybercriminalité au Togo est d'environ 45 millions FCFA par an.

En outre, selon les statistiques de la police et de la gendarmerie nationales, quatre-vingt-six (86) cybercriminels impliqués dans des incidents de sécurité informatique, tels que l'atteinte à un système informatique, la cyber escroquerie, l'arnaque, le faux et groupements de malfaiteurs, ont été déférés en 2022.

Comme on peut s'en douter, ces chiffres ne peuvent être considérés comme reflétant la réalité des actes de cybercriminalité au niveau national car à ce stade, les statistiques sur la cybercriminalité sont rares, non complètes et donc pas entièrement fiables, d'où la difficulté d'évaluer l'ampleur et les impacts de ce fléau.

Plusieurs raisons peuvent expliquer ce manque de données :

- Malgré les efforts de sensibilisation déployés par l'ANCy, le déficit de signalement par les utilisateurs d'Internet des cyberattaques, reste persistant ;
- Le faible niveau de coopération entre les acteurs impliqués dans la lutte contre la cybercriminalité, tels que les autorités judiciaires, les services de sécurité, les opérateurs de télécommunications et les fournisseurs de services Internet ;

Ces facteurs limitent la capacité du Togo à collecter, analyser et diffuser des informations fiables sur la cybercriminalité au Togo.

4. Les facteurs favorisant la cybercriminalité au Togo

Si l'utilisation de systèmes et de réseaux informatiques représente un progrès certain pour notre société, elle n'en accroît pas moins sa vulnérabilité car elle pose des problèmes liés aux infractions et crimes électroniques. Avec l'essor de ces technologies, notamment d'internet, on assiste en effet à l'avènement de la cybercriminalité qui émerge d'une forme de commerce opérant sur des espaces immatériels qui ignorent les frontières des États et les législations propres à ceux-ci.

Avec un âge moyen compris entre 20 et 30, 80% des déviants numériques sont de sexe masculin qui opéraient au début des années 2000 pour la plupart, depuis les cybercafés.

Toutefois, on assiste depuis peu, à une « domestication » des activités des cybercriminels qui se dotent de connexion privée, ce qui leur permet d'opérer depuis leur domicile ou parfois depuis les zones périurbaines afin d'éviter tout soupçon.

Au Togo, outre les jeunes togolais qui s'adonnent à cette activité, on dénombre dans le rang des cybercriminels, des béninois, des nigérians, des ivoiriens et autres nationalités de la sous-région.

Il existe quatre facteurs principaux qui déterminent l'entrée des individus dans le monde de la criminalité informatique (la vengeance, le besoin d'autodéfense, l'appât du gain facile et le défi ou la volonté d'accéder à une certaine reconnaissance sociale).

En outre, deux motivations fondamentales expliquent l'engouement des cybercriminels au Togo pour cette activité : la motivation financière (80%) et celle sociale qui trouve ses racines dans une ambition de vengeance et dans le besoin de reconnaissance par ses pairs ou par la communauté dans laquelle il vit ou a grandi. Cette dernière forme de motivation s'inscrit bien dans la logique développée par les cybercriminels pour justifier leur forfait, surtout lorsqu'ils considèrent le phénomène comme une occasion de corriger les injustices commises par les puissances occidentales en Afrique. La motivation financière apparaît comme le principal facteur qui pousse les jeunes à s'adonner à cette activité, parce qu'ils y voient une opportunité pour améliorer leurs conditions de vie et une issue au chômage.

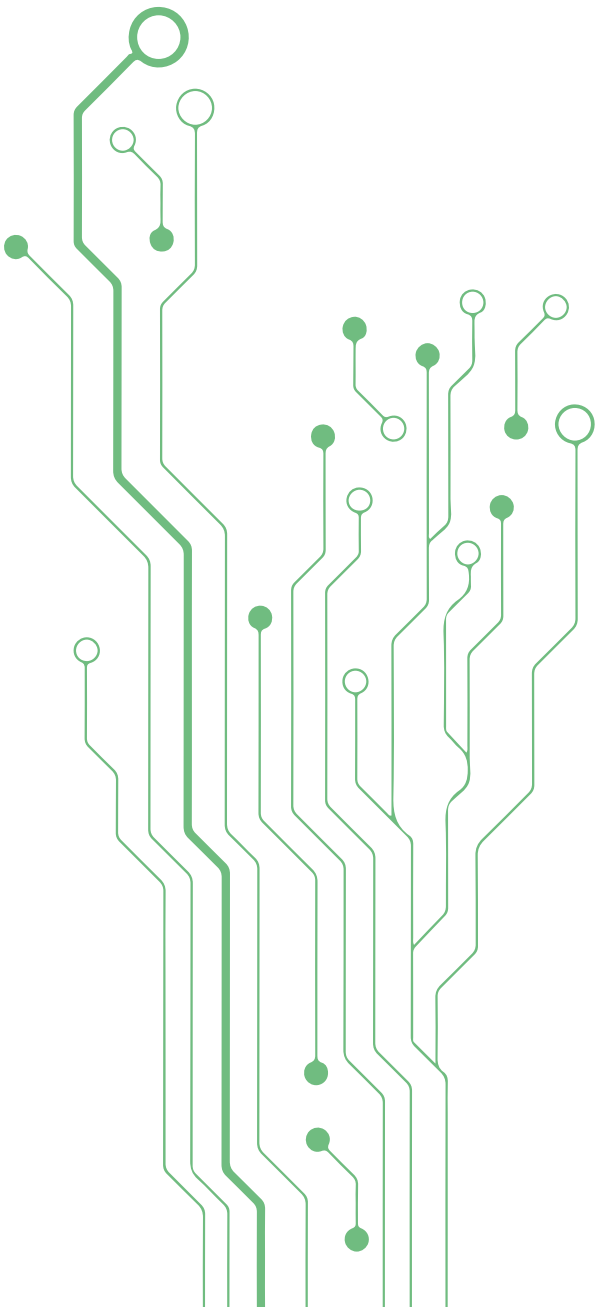
Plusieurs autres facteurs expliquent l'essor et la persistance du phénomène:

• Le développement rapide des technologies de l'information et de la communication (TIC) qui offre aux cybercriminels des opportunités de commettre des actes illicites tels que le piratage, l'escroquerie, le vol de données, la diffusion de contenus illicites, etc.

• Le pourcentage de sensibilisation et de formation des utilisateurs des TIC sur les risques et les bonnes pratiques en matière de cybersécurité, demeure encore faible malgré les efforts de l'ANCy. Les cybercriminels profitent donc de la naïveté ou de la négligence des internautes pour les piéger ou les infecter par des logiciels malveillants ;

• Le caractère transfrontalier de la cybercriminalité rend difficile son identification, sa prévention et sa répression. Il nécessite une coordination et une harmonisation des législations et une meilleure coopération régionale et internationale dans la lutte contre la cybercriminalité des actions entre les pays concernés.

LA LUTTE CONTRE LA CYBERCRIMI-NALITÉ AU TOGO




<!DOCTYPE html>
<html style="height:100%">
<head>
</head>
<title>
<body

C. Les principales cybermenaces au Togo

1. Escroqueries en ligne

Les escroqueries en ligne englobent différents types de fraudes réalisées dans le cyberespace. Il s'agit aussi bien de l'hameçonnage que du vol de carte de crédit, de l'usurpation d'identité, de l'escroquerie à l'avance de frais et de la fraude au paiement à distance. Etc.

Elles cherchent habituellement à exploiter les peurs, les insécurités ou les vulnérabilités des victimes en employant de multiples tactiques, techniques et procédures en ligne. Des groupes criminels organisés complexes utilisent souvent des logiciels malveillants sophistiqués sur mesure pour réaliser des gains financiers illicites au détriment de victimes sans méfiance.

L'escroquerie en ligne la plus répandue est l'hameçonnage. Il peut être réalisé par courriel, SMS, appel téléphonique ou à l'aide d'un kit d'hameçonnage.

En ce qui concerne la fraude bancaire et la fraude à la carte de crédit, les acteurs des menaces exploitent les vulnérabilités des systèmes non protégés des banques ou des particuliers, en mettant en œuvre des tactiques d'ingénierie sociale pour obtenir les informations des cartes de crédit ou accéder aux informations bancaires en ligne.

Les courriels d'hameçonnage peuvent employer des scénarios mettant en scène des services de livraison, des services postaux, des services financiers ou des services RH et convaincre les victimes d'ouvrir des pièces jointes malveillantes ou de cliquer sur des liens malveillants.

Les escroqueries en ligne constituent une stratégie rentable pour les acteurs des menaces, car elles nécessitent un équipement technique minimal et présentent de faibles coûts de démarrage.

2. Extorsion en ligne

L'extorsion en ligne avec chantage et sextorsion, consistent pour les acteurs des menaces d'employer soit de fausses allégations soit des preuves de données ou de fichiers à caractère personnel volés pour forcer les victimes à payer une rançon afin de les récupérer ou d'éviter leur publication en ligne.

Plus spécifiquement, les acteurs des menaces de sextorsion utilisent l'hameçonnage et le chantage sur de nombreuses plateformes pour obtenir de l'argent de leurs victimes en alléguant avoir obtenu des images sexuelles compromettantes ou leur historique de navigation sur des sites à caractère sexuel.

Le cyberchantage peut aussi être combiné aux techniques d'ingénierie sociale qui visent à étudier les victimes et à tirer parti des données à caractère personnel qu'elles laissent en ligne sur les billets de médias sociaux ou qui ont été exposées sur les forums du Web de surface ou du dark Web à la suite de violations de données antérieures, dans la mesure où les acteurs des menaces emploient des techniques toujours plus sophistiquées pour créer des messages d'extorsion personnalisés adaptés à chaque victime.

De même, le mode opératoire en cas de sextorsion peut impliquer de fausses allégations d'accès à la webcam ou à l'historique de navigation des victimes, suivies de demandes de paiement pour éviter la diffusion de ces informations aux proches ou dans la sphère publique. Même si ces allégations sont souvent produites en masse, des activités de sextorsion ont aussi été détectées via des applications mobiles : les acteurs des menaces trompent les victimes sans méfiance, habituellement des hommes, pour qu'elles s'enregistrent ou envoient des vidéos intimes à des personnes qu'elles pensent être des femmes. Les acteurs des menaces utilisent ensuite ces enregistrements pour faire chanter les victimes si elles veulent éviter leur diffusion.

3. Escroqueries aux faux ordres de virement

Les escroqueries aux faux ordres de virement constituent un type d'escroqueries qui cible les entreprises et les organisations pour obtenir un gain financier ou voler des données. Les cybermalfaiteurs compromettent ou contrefont un compte de messagerie électronique légitime afin d'envoyer des courriels frauduleux demandant le transfert de fonds ou de données sensibles tout en se faisant passer pour le propriétaire légitime. Les cybermalfaiteurs ciblent habituellement des dirigeants de haut niveau travaillant dans la finance ou s'occupant de paiements par virement bancaire. Ils en compromettent les comptes de messagerie professionnelle par des méthodes comme l'enregistrement de frappe ou des attaques par hameçonnage ou ils en contrefont simplement les courriers électroniques pour donner l'impression qu'ils ont été envoyés du compte de messagerie légitime de la victime. Des courriels frauduleux sont ensuite envoyés depuis ces comptes de messagerie au niveau de confiance établi aux autres salariés ou à des contacts de la victime en leur demandant de transférer des données ou des fonds sur un compte bancaire spécifique.

Les trois types d'escroqueries aux faux ordres de virement sont les suivantes :

• Fraude à la facture fictive

La fraude à la facture fictive implique habituellement une entreprise qui a une relation établie avec un fournisseur. Le fraudeur demande par le biais d'un courriel, d'un appel téléphonique ou d'une télécopie contrefaite(e) à ce que le virement dû au titre d'une facture soit réalisé sur un nouveau compte, frauduleux.

• Fraude au président

Dans le cas de la fraude au président, les fraudeurs se présentent comme des dirigeants de haut niveau (DAF, DG, DSI, etc.), des avocats ou d'autres catégories de représentants légaux. Ils prétendent s'occuper d'affaires confidentielles ou contraintes par le temps et demandent un transfert par virement sur un compte qu'ils contrôlent. Dans certains cas, la demande frauduleuse de virement est envoyée directement à l'institution financière avec des instructions pour transférer de manière urgente les fonds à une banque.

•Compromission de comptes

Dans les cas de compromission de comptes, le compte de messagerie électronique d'un(e) salarié(e) est piraté, puis utilisé pour envoyer des demandes de paiement de factures sur des comptes bancaires contrôlés par le fraudeur. Les messages sont envoyés à plusieurs fournisseurs identifiés dans la liste de contacts de la victime. L'entreprise cliente peut rester dans l'ignorance de cette fraude tant que les fournisseurs ne s'enquièrent pas du statut du paiement de leurs factures.

4. Rancongiels

Un rançongiciel est un logiciel malveillant qui crypte les données de la victime ou verrouille ses systèmes, désorganisant les opérations des organisations victimes en rendant leurs données et leurs systèmes inaccessibles. Les opérateurs des rançongiciels demandent ensuite une rançon en échange du décryptage des données.

Il est à noter que le déploiement du code des rançongiciels sur le réseau d'une organisation fait suite à une violation de ce réseau par un acteur légitime (personne interne de confiance) ou illégitime, à l'exploration du réseau par les cybermalfaiteurs et au vol des informations et des données de l'organisation.

Le déploiement d'un rançongiciel est généralement la phase finale d'un piratage ou d'une pénétration réussie(e) du réseau de l'organisation. Avec la complexification des tactiques, techniques et procédures, la facilitation des attaques par rançongiciel par les groupes criminels organisés s'est élargie pour inclure les doubles et triples extorsions : l'attaque par rançongiciel initiale est démultipliée par le vol de données sensibles de l'entreprise, des demandes de rançon aux victimes en les menaçant de les humilier publiquement par la diffusion des informations volées, et la réexploitation des vulnérabilités exposées par le passé, ce qui soumet les organisations à un cycle sans fin d'attaques par rançongiciel.

Capables d'interrompre instantanément l'activité des administrations, des entreprises et des chaînes d'approvisionnement, les attaques par rançongiciel se traduisent aussi par un impact sur la réputation des victimes, sans oublier les répercussions économiques.

D. Impact de la cybercriminalité

La cybercriminalité est un phénomène qui menace l'économie, la société et la sécurité nationale. Elle engendre des coûts directs et indirects pour les victimes, les entreprises, les administrations et l'Etat. Elle fait peser des risques sur les infrastructures critiques, les données personnelles et notre souveraineté numérique.

Pour évaluer l'impact de la cybercriminalité sur le Togo, nous prenons en compte plusieurs aspects :

• Le coût direct de la cybercriminalité est le montant des pertes financières subies par les victimes ou les acteurs économiques à cause des attaques informatiques. Il inclut les dommages matériels, les vols d'informations, les rançons exigées, les fraudes en ligne, etc. ;

• Le coût indirect de la cybercriminalité est le montant des dépenses engagées pour prévenir, détecter, réparer ou sanctionner les attaques informatiques. Il inclut les investissements en matériels et logiciels de sécurité, les coûts de formation et de sensibilisation, les coûts de rétablissement des systèmes affectés, les coûts judiciaires, etc.

• Le risque sur les infrastructures critiques est le danger que représente la cybercriminalité pour le fonctionnement des services essentiels à la vie économique et sociale du pays, comme l'énergie, les transports, les télécommunications, la santé, la défense, etc. Une attaque informatique réussie sur ces infrastructures pourrait avoir des conséquences graves sur la sécurité des personnes et des biens, ainsi que sur la stabilité du pays ;

• Le risque sur les données personnelles est le danger que représente la cybercriminalité pour la protection de la vie privée et des droits fondamentaux des citoyens togolais. Une attaque informatique réussie sur les données personnelles pourrait entraîner des violations de l'identité, du secret des correspondances, de la réputation, etc. ;

• Le risque sur la souveraineté numérique est le danger que représente la cybercriminalité pour l'autonomie et l'indépendance du Togo dans le domaine du numérique. Une attaque informatique réussie sur les systèmes d'information de l'Etat pourrait compromettre sa capacité à exercer son autorité et à défendre ses intérêts dans le cyberespace ;

Cependant, il est encourageant de constater que des mesures sont prises pour prévenir et combattre la cybercriminalité dans notre pays. Le gouvernement, les entreprises et les organisations travaillent ensemble pour renforcer la sécurité en ligne, en mettant en place des réglementations, en sensibilisant les citoyens et en investissant dans des technologies de pointe pour détecter et prévenir les attaques. Bien que des défis subsistent du fait de la complexité de la lutte contre la cybercriminalité, il est clair que des progrès sont réalisés.

Au Togo, le début de l'année 2023, l'on a assisté à de nombreuses et répétées tentatives d'attaque contre des banques ; A ce jour, grâce aux efforts conjugués de toutes les parties prenantes, nous parvenons à anticiper sur d'éventuelles conséquences désastreuses de ces actes.

Pourtant, il faut avouer que ce n'est probablement que le début du scandale numérique, car les cyberattaques deviennent une menace beaucoup plus grande pour notre pays et mettent en péril les données à caractère personnel des particuliers.

Les hackers jouent sur les vulnérabilités pour lancer leurs cyberattaques aussi bien au départ du territoire national, qu'en provenance d'un peu partout dans le monde. Aujourd'hui, il semble que les motivations des cybercriminels vont bien au-delà de l'argent mais plus sur leur capacité à prouver la vulnérabilité des entreprises et des Etats.

E. Mesures contre la cybercriminalité

La délinquance numérique est en plein essor au Togo, tendance favorisée par le développement de l'accès à internet.

Face à la cybersécurité, le gouvernement togolais a une double responsabilité : celle de se protéger en tant qu'Institution et celle de mettre en place un cadre nécessaire pour la protection des organisations, des personnes et des infrastructures publiques.

Au Togo, pour faire face à cette double mission, le gouvernement a mis en place des organes et des lois spécifiques pour garantir la cybersécurité et réprimer les cyber infractions.

Il s'agit de :

• La création de l'ANCy en 2019, qui a pour mission de définir les règles de cybersécurité, d'auditer les opérateurs de services essentiels, de délivrer des agréments aux prestataires en cybersécurité, de former et sensibiliser les secteurs public et privé en cybersécurité. A ce titre, l'Agence est chargée d'identifier, d'analyser et d'atténuer les cybermenaces affectant l'État togolais, les citoyens, les entreprises et les organisations ;

• L'ANCy dispose d'un Centre national de réponse aux incidents de cybersécurité (CERT) qui est opéré par Cyber Defense Africa S.A.S (CDA), en tant que service délégué par l'ANCy ; le CERT.tg a pour mission d'identifier, analyser et mitiger les cyberattaques affectant l'Etat, les citoyens, les entreprises et organisations togolaise ;

• La construction d'un Data Center Carrier Hotel, qui offre un site d'hébergement sécurisé des données des entreprises ;

• L'adoption d'un cadre législatif et réglementaire dans le domaine des TIC, qui comprend notamment la loi n°2018-026 du 6 décembre 2018 relative à la cybersécurité et à la lutte contre la cybercriminalité qui prévoit des sanctions allant de l'emprisonnement au paiement de lourdes amendes pour les auteurs d'infractions sur Internet, la loi n°2019-014 du 5 juillet 2019 relative à la protection des données à caractère personnel, ainsi que les décrets y afférents ; L'IPDCP a pour mission de veiller au respect des principes et règles relatifs à la collecte, au traitement, à la conservation et à la communication des données à caractère personnel au Togo.

F. Les perspectives

La cybercriminalité est un phénomène qui menace la sécurité et le développement des pays africains, y compris le Togo. Face à ce défi, en dehors des nombreux efforts déjà fournis par le Togo, il est nécessaire d'accentuer les actions et d'envisager d'autres actions visant à renforcer la lutte contre la cybercriminalité, en s'appuyant sur les bonnes pratiques internationales et régionales, et en identifiant les axes prioritaires d'action.

Voici quelques pistes de réflexion pour les années à venir :

- Poursuivre et accentuer la sensibilisation des citoyens, des entreprises et des institutions publiques aux risques et aux conséquences de la cybercriminalité, ainsi qu'aux moyens de se protéger et de signaler les incidents ;

- Réprimer la cybercriminalité en dotant les services chargés de l'application de la loi des compétences, des moyens et des outils nécessaires pour enquêter, poursuivre et sanctionner les cybercriminels, en coopération avec les autres pays et les organisations internationales comme INTERPOL ;

- Coopérer avec les autres pays africains et les partenaires régionaux pour harmoniser les législations, échanger les informations, coordonner les actions et mutualiser les ressources dans la lutte contre la cybercriminalité ;

- Renforcer la résilience face à la cybercriminalité en mettant en place des mécanismes de gestion des crises, de réponse aux incidents, de restauration des systèmes et de soutien aux victimes ;

- Développer et promouvoir une solide culture de cyber sécurité qui reconnaît et répond efficacement aux menaces et aux défis mondiaux liés à l'Internet et réseaux mobiles interconnectés et technologies connexes ;

Par ailleurs sur le plan légal et réglementaire, les efforts seront consacrés à :

• Accélérer le processus de ratification et la mise en œuvre de la Convention de Budapest sur la cybercriminalité qui à ce jour, est considérée comme le seul instrument international juridiquement contraignant en matière de cybersécurité et de lutte contre la cybercriminalité ;

• Finaliser et publier la stratégie nationale sur le cyber sécurité et son plan d'action opérationnel pour la lutte contre la cybercriminalité ;

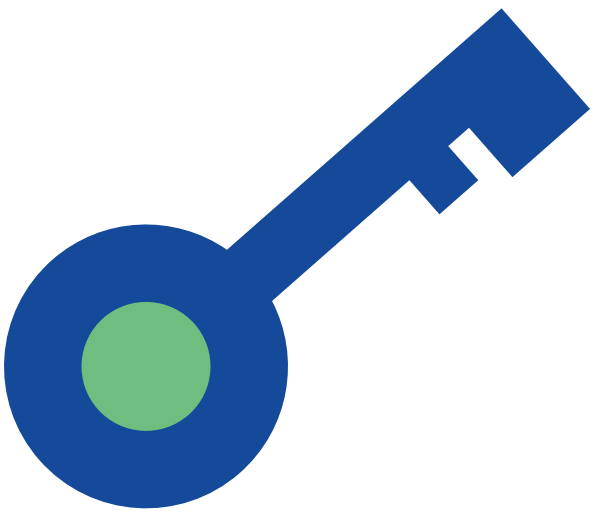
• Revoir la loi sur la cybersécurité et la lutte contre la cybercriminalité nationale pour criminaliser toutes les nouvelles formes d'infractions liées à l'usage illicite des TIC qui viennent de voir le jour, si nécessaire ;

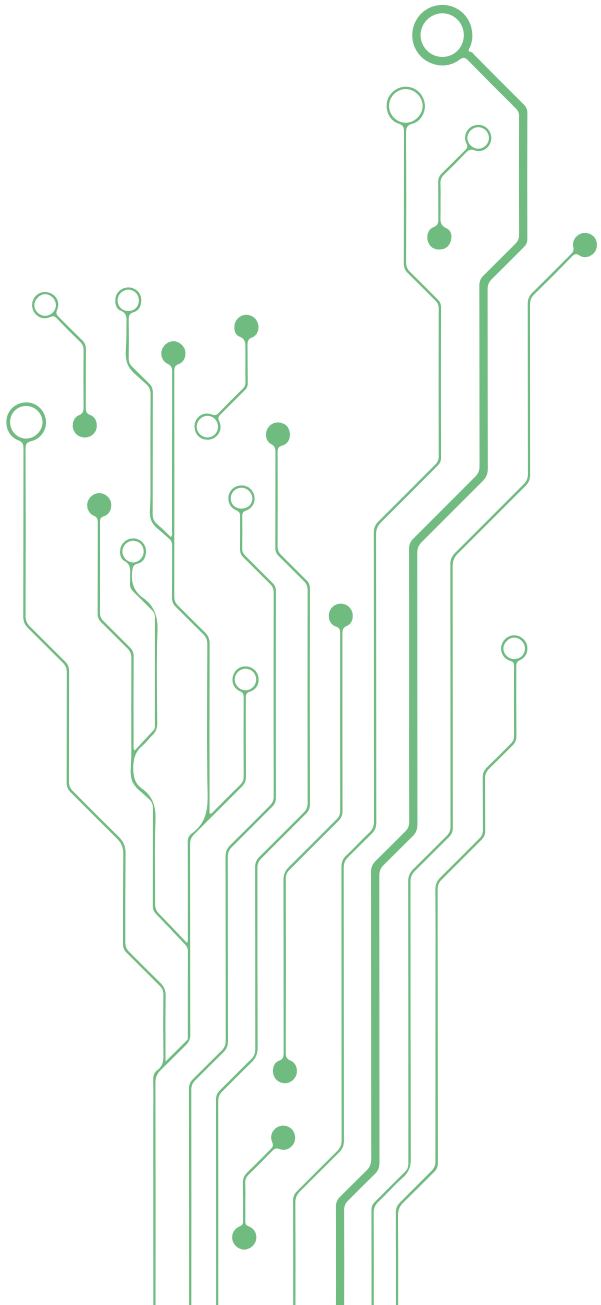
• Opérationnaliser l'instance de protection des données à caractère personnel (IPDCP) ;

• Développer des capacités en cyber diplomatie et participer aux discussions menées au niveau international comme le Groupe d'experts gouvernementaux des Nations Unies ;

• Opérationnaliser le Centre Africain de Cybersécurité, avec l'appui de la Commission Economique des Nations Unies pour l'Afrique (UNECA), qui est chargé de fournir au niveau sous-régional, une expertise en matière de cybersécurité et de mener des activités liées à la promotion de la cybersécurité et aux enquêtes sur la cybercriminalité.

CONCLUSION





Les TIC constituent un outil sans pareil qui s'insère progressivement dans le quotidien de chaque citoyen et offre d'innombrables perspectives dans les domaines les plus divers (économique, politique, social, etc.). Dans leur ensemble, elles apparaissent comme un facteur de développement, car elles peuvent faciliter la réalisation des objectifs de développement du millénaire, en luttant contre la pauvreté et en améliorant les conditions de vie des populations. A l'instar de plusieurs pays africains, le Togo tente donc de saisir les fenêtres d'opportunités que lui offre le marché mondial de l'externalisation pour promouvoir son développement.

Cependant, cette révolution numérique expose également notre pays à la cybercriminalité, dans un contexte où les entreprises et même les populations ne prennent pas toujours la pleine mesure des risques cyber qui accompagnent la transformation numérique.

Ces formes de cybercriminalité peuvent avoir des conséquences graves pour les individus, les organisations et l'Etat togolais. Elles peuvent entraîner des pertes financières, des atteintes à la vie privée, des dommages matériels, des troubles à l'ordre public ou des risques pour la sécurité nationale.

Face à cette situation, nous avons toutes les raisons de nous inquiéter, car l'émergence de la cybercriminalité au Togo tient au fait qu'une décennie seulement après son apparition, certains jeunes ont rapidement excellé dans la maîtrise des rouages de l'outil informatique et du web. Cette appropriation des TIC a très tôt favorisé un usage d'internet orienté vers la criminalité numérique.

Néanmoins, le dispositif légal, technique, financier, opérationnel, technique qui a été mis en place par les plus hautes autorités de notre pays, ont permis de ralentir considérablement les velléités de ces cybercriminels, recherchés pour la plupart au Benin, en Côte d'Ivoire et au Nigeria, qui pensaient trouver au Togo une terre d'accueil.

Voilà pourquoi, dans la perspective des années à venir, ces nombreuses autres mesures, visant à garantir à notre pays la sécurité et la stabilité nationale ainsi que la continuité de nos activités sociétales, seront davantage accentués.

En poursuivant nos efforts pour lutter contre la cybercriminalité dans notre pays, nous pouvons créer un avenir plus sûr et plus prospère pour tous.

ANCy
Agence Nationale de la Cybersécurité

Outil de garantie de la **souveraineté numérique** au Togo.

ANCy
Agence Nationale de la Cybersécurité

63 Bd du 13 Janvier,
Nyékonakpoe, Lomé-TOGO
07 BP 7878
secretariat.ancy@ancy.gouv.tg
+228 22 21 25 28
+228 97 52 58 58
+228 70 60 60 83

ancy.gouv.tg