Le renseignement à l'épreuve de l'extension de champs et moyens de criminalité traditionnelle en RDC

Kinshasa, 29 décembre 2024.

Clément Kivuna Tsheko (Ingenii).

Juriste de formation.

Chercheur en Droit du numérique

Les activités de renseignement se déploient dans quatre registres d'action de l'Etat, notamment la défense, la diplomatie, la police, l'économie. S'ajoute désormais le ″cyber‟, qui dévient un nouveau cadre d'affrontement aux cotés de la terre, l'air, la mer et l'espace.[1] En République Démocratique du Congo, tout mot précédé par le préfixe cyber semblait provenir de l'imaginaire, notamment le cyberespace, cybercriminalité, cyberespionage etc. Ceci malgré l'existence d'un grand nombre d'auteurs congolais en la matière. Cependant, il a falluattendre non seulement l'avènement de la Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication (TIC). Mais aussi celui de l'ordonnance-Loi n°23/010 du 13 mars 2023 portant code du numérique[2], la plupart de ces concepts ont été légalementdéfini par ces instruments juridiques précités. Malgré ce prisen compte de ces concepts liés aux activités numériques par lesdits instruments juridiques, ces derniers omettent cependant de définir le concept cyber espace. Dans ce contexte, la doctrine l'emportecar certains auteurs en droit du numérique congolais considèrent le cyberespace comme un nouvel environnement, un espace opérationnel qui s'ajoute aux cotés des espaces traditionnels, notamment « l'air, terre et mer ».[3]Il est définit comme une interconnexion mondiale des réseaux qui transmettent, traitent ou stockent les données numériques, sans limite spatio- temporelle.[4] Mais alors, la question fondamentale qui intrigue l'esprit c'est celle de savoir si réellement les attaques cyber existent en RDC ?

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

[1] Lire O. CHOPIN, B. OUDET, *Renseignement et sécurité*, Ed. Armand Collin, Paris, 2023, pp.187-214.
[2] JORDC – N° spécial – 11 avril 2023.
[3]K. NDUKUMA ADJAYI, « Explication du cyber espace », Mémoire de fin de cycle de 2e LICENCE, UPC, 2024.
[4] Idem, *Droit des télécoms et du numérique,* Ed. L'Harmattan, Paris, 2019, P.35.

social.[5]Cette digitalisation de la RDC présente non seulement des avancées technologiques. Mais aussi, elle présente des risques énormes pour la sécurité nationale du système d'information et favorise l'extension de criminalité traditionnelle.

ledit Plan National du Numérique, décliné en quatre piliers fondamentaux (Infrastructures, contenus, usages applicatifs, gouvernance – régulation) permet à l'État Congolais, tant au niveau national, provincial que local, d'aligner dans son agenda la nécessaire transformation numérique des institutions, des entreprises et des services publics, de refondre l'architecture pyramidale d'actions en privilégiant la transversalité et de se construire un écosystème gouvernemental digital afin d'atteindre ses objectifs qui sont ceux de bâtir une économie solide, prospère et résiliente à l'ère du Numérique.[6] C'est une révolution systémique et structurelle majeure qui va nécessiter un encadrement par des mécanismes et de dispositifs adaptés aux réalités du cyberespace.

Avec l'avènement des nouvelles technologies de l'information et de la communication, le cyberespace est devenu pour les services de renseignements un lieu de collecte d'information et de conduite d'Operations dont l'importance croit chaque jour, à mesure que l'espace numérique augmente[7]. Les nouvelles technologies de l'information et de la communication (NTIC) désignent l'ensemble des outils, dispositifs et techniques utilisés pour collecter, stocker, traiter, transmettre et échanger des informations à l'aide des technologies numériques.[8]

Dans le cadre de l'extension des champs et moyens de criminalité traditionnelle, les enjeux du renseignement des services de sécurité s'adaptent à l'ère du numérique. Cette adaptation nécessite non seulement une approche pro active et préventive, mais aussides politiques bien définies avec une collaboration étroite entre les acteurs concernés. Le renseignement public est une activité qui consiste à la collecte des informations d'intérêts nationaux par des agences gouvernementales dont notamment les services de renseignement, forces de l'ordre et de défense, aux fins de gérer les menaces et de garantir la sécurité de l'Etat.[9]

Pour l'essentiel, l'extension de criminalité traditionnelle appel à l'étude des cyberattaques en tant qu'enjeux globalisant les acteurs régaliens **(I),** ainsi que le renseignement et sécurité du système d'information **(II).**

---

[5] Présidence de la république, « stratégie nationale de cyber sécurité de la République Démocratique du Congo », p.6.

[6] *Idem.*

[7] Lire S.-Y. LAURENT, « Pour une véritable politique publique du renseignement », Institut Montaigne étude juillet 2014, p. 10.

[8] Les nouvelles technologies de l'information et de la communication, [en ligne] disponible sur : [https://www.certitude- management.com/], (consulté le 11 aout 2024).

[9] C. GHRENASSIA et R. BINSARD, « La preuve, le renseignement et le droit », [en ligne] disponible sur : [https://www.dalloz-actualite.fr/], (consulté le 05/08/2024).

I. Enjeux des cyberattaques

De nos jours, l'Internet connait une utilisation croissante et des espaces numériques, tout le monde peut être victime d'un cyber attaque. Les cibles des attaques du cyber se sont diversifiées au point d'englober même le secteur public que privé (particuliers, professionnels, grande ou petite entreprise). Pour le secteur public, toutes les institutions ne sont pas à l'abri de ces attaques cyber. La protection contre ces menaces est cruciale. Il est cependant apparut l'importance d'exploiter les cyberattaques existant **(A),** mais aussi relever les enjeux du renseignement liés à ces activités **(B).**

A. Cyberattaques

Les Cyberattaques sont des actes malveillants de piratage informatique dans le cyberespace. Elles incluent la désinformation, l'espionnage électronique, la modification clandestine des données sensibles ou la perturbation des infrastructures critiques d'un pays.[10] De par la diversité des cyberattaques possibles, il faut établir une divergence entre plusieurs phénomènes, en fonction du but poursuivi par les attaques, des acteurs impliqués et des cibles visées. Dans le cas sous examen, nous traitons de manière restreinte deux phénomènes, il s'agit de la Cybercriminalité **(1),** et de la cyberespionnage **(2).**

1. Cybercriminalité.

L'adoption universelle des technologies Internet, la dépendance des organisations et des Etats à ces mêmes technologies et l'interdépendance des infrastructures, introduisent un degré de vulnérabilité non négligeable dans le fonctionnement des institutions.

La cybercriminalité est devenue un fléau de société qui touche tous les acteurs tant sur le plan national qu'international. Simultanément au cyberespace, elle reflète l'évolution des pratiques criminelles qui ont su s'adapter et tirer parti des technologies de l'information et de la communication. La cybercriminalité est une extension du champ et des moyens de criminalité traditionnelle. Cette dernière est devenue plus performante grâce aux technologies de l'information.[11]

En RDC, le législateur a définit la cybercriminalité comme l'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la

[10] Art.4.24, Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication.
[11] P. PIRON, la cyberdéfense, nouvelle arme géopolitique « La Jaune et la Rouge », Magazine N°753, p.3.

communication telles que définies par l'Ordonnance-Loi n°23/010 du 13 mars 2023, ainsi que celles prévues dans d'autres lois particulières, dont la commission est facilitée ou liée à l'utilisation des technologies.[12]

2. Cyber espionnage

En ligne, les États se comportent de la même manière que dans le reste de leurs politiques : ils emploient les mêmes tactiques et poursuivent les mêmes objectifs. Tous les États espionnent, chacun à leur façon.[13] Quoi qu'il en soit, l'espionnage est bel et bien appliqué par les Etats. Cette pratique d'espionnage ne se limite pas aux activités traditionnelles, la dématérialisation des activités classiques a fait donner naissance au cyber espionnage. D'autant que, le cyberespace est devenu un champ de bataille économique et militaire. Bien que, la guerre dans le cyberespace utilise des moyens non militaire (au sens traditionnel du terme) et Internet modifie également l'art de faire la guerre : sans une armée, mais avec des informaticiens, sans arme à feu mais avec des informations.

En droit congolais, aucun cadre légal ne définit de manière express l'espionnage. Cependant, le service de sécurité et de renseignement britannique, définit l'espionnage comme « le processus visant à obtenir des renseignements qui ne sont normalement pas accessibles au public, et ce, par des moyens humains (des agents des renseignements) ou techniques (le piratage d'un système informatique). Ce processus peut aussi avoir pour but d'influencer des décideurs et des leaders d'opinion au profit d'intérêts étrangers ».[14] En tant que forme d'espionnage, le cyberespionnage consiste à mener des opérations informatiques ou techniques pour extraire des renseignements et des données des systèmes informatiques d'une cible ou d'un adversaire.[15]

Juridiquement, le droit international reconnaît l'espionnage en temps de guerre, et cela, depuis la Convention de La Haye de 1907 concernant les lois et coutumes de la guerre sur terre.[16]

Mais l'espionnage n'est en revanche pas reconnu par le droit international en temps de paix, ce qui a pour conséquence qu'un acte d'espionnage révélé, est plutôt réglé dans le cadre « des arrangements extrajudiciaires »[17].

---

[12] Art 2.24. Ordonnance- Loi n°23/023 du 10 mars 2023, préc.

[13] P. DIOTTE, « Les quatre grands auteurs de menaces et le cyberespionnage : quand la Chine, la Russie, l'Iran et la Corée du Nord espionnent en ligne », in Revue militaire canadienne, Vol. 20, no. 4, automne 2020, p.32.

[14] *Ibidem*, p.33.

[15] D. WEISSBRODT, « *Cyber-Conflict, CyberCrime, and CyberEspionage* », *University of Minnesota Law School Scholarship Repository*, 2013, vol. 347, p. 354.

[16] Art. 29, Convention IV de La Haye du 18 octobre 1907 concernant les lois et coutumes de la guerre sur terre et son Annexe.

En 2019, le directeur du renseignement national (DNI) des États-Unis souligneque les adversaires et les concurrents stratégiques des États-Unis auront de plus en plus recours aux cybercapacités, notamment au cyberespionnage, aux cyberattaques et à la cyberinfluence, pour obtenir un avantage politique, économique et militaire sur les États-Unis, leurs alliés et leurs partenaires. Selon ce même rapport, la Chine, la Russie, l'Iran et la Corée du Nord mèneraient de plus en plus de cyberopérations, multipliant les façons d'effrayer les esprits et d'affoler les machines dans le but de voler de l'information, d'influencer les citoyens ou de perturber des infrastructures essentielles.[18]

De ce qui précède, la Chine, la Russie, l'Iran et la Corée du Nord sont les quatre principaux auteurs de menaces. Ils exploitent tous le cyberespionnage d'une manière qui reflète leurs intérêts géopolitiques et leurs approches habituelles en matière de renseignement et de conduite de la guerre.

Par rapport à la Chine, elle est devenue un acteur prédominant dans le cyberespace et ses actions s'inscrivent dans ses principaux objectifs stratégiques, soit l'hégémonie et la sécurité économiques.

Concernant la Russie, elle a pour sa part adoptée une approche différente et considère sa capacité de cyberespionnage comme un élément clé de sa stratégie globale en matière de guerre de l'information, tant dans les pays avoisinants qu'ailleurs dans le monde.

Par contre l'Iran se sert du cyberespionnage comme il le fait avec les forces interposées, c'est-à-dire pour projeter sa puissance, exercer un contrôle étatique et user des représailles.

De son côté, la Corée du Nord considère le cyberespionnage comme un moyen d'assurer la survie du régime et de déstabiliser ses ennemis régionaux, en particulier les États-Unis et la Corée du Sud.

La RDC quant à elle occupe une place stratégique en Afrique centrale, et ce, depuis plusieurs années qu'elle demeure en guerre contre le Rwanda. Ce dernier géant en technologies, possède un satellite en orbite. Ceci sous-entend que la RDC doit s'enligné dans l'ordre des pays fort en technologies pour faire face à son adversaire.

En somme, le cyberespionnage s'exerce dans l'intention de voler des renseignements sur les activités diplomatiques, économiques et de défense d'un Etat.

---

[17]B. WARUSFEL, « Le cadre juridique et institutionnel des services de renseignement en France », in Fondation pour les Etudes de Défense, La Documentation française, Paris, 1997, p. 20.

[18]P. DIOTTE, « Les quatre grands auteurs de menaces et le cyberespionnage : quand la Chine, la Russie, l'Iran et la Corée du Nord espionnent en ligne », op.cit.p.33

B. Enjeux du renseignement

À l'ère du numérique, le cyberespace fournit aux Etats un moyen de recueillir des renseignements et de mener des attaques sans craindre de répercussions importantes, leur conférant une immunité imprévue qui aura tôt fait de disparaitre. En ces termes, le cyberespace a complètement changé la face de la guerre puisque les Etats sont maintenant en constante compétition directe. Le renseignement dans ce contexte, constitue un moyen de cybersécurité **(1)** et cyberdéfense contre les cyberattaques **(2).**

1. Cybersécurité

La sécurité est l'un des tous premiers besoins humains à l'ère de la dématérialisation, cette approche doit nécessairement intégrer la culture de notre pays (RDC) à l'évolution de la technologie. Quelques années plutôt, le mot « cybersécurité » semblait encore relever de l'imaginaire. Il était commun de penser que la sécurité de l'information ne concernait qu'un nombre très restreint de structures et d'individus. Aujourd'hui, tout le monde est touché, de près ou de loin, par ces enjeux de sécurité.

L'Ordonnance-Loi n° 23/023 du 10 mars 2023, définit la cybersécurité comme étant, l'ensemble des mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain et procédural ou autre permettant d'atteindre les objectifs de sécurité des systèmes informatiques et des réseaux de communication électronique et de garantir la disponibilité, l'intégrité , la confidentialité, l'authenticité ou la traçabilité des données stockées, traitées ou transmises et des services connexes.[19]

En d'autres termes, La cybersécurité c'est « l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité, la confidentialité ou la traçabilité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles ».[20]

La cybersécurité concerne la sécurité informatique, celle de l'information et de la sécurité des réseaux, des environnements connectés à Internet. En ce sens, la cybersécurité repose sur la complémentarité et la cohérence des mesures stratégiques et opérationnelles. Elle n'est pas acquise définitivement car elle est un processus continu.[21]

---

[19] Art 2.25, Ordonnance- Loi n°23/023 du 10 mars 2023, préc.

[20] S. Ghernaouti, « Cybersécurité : Analyser les risques, Mettre en œuvre les solutions », 6e Ed.Dunod, Malakoff, 2019, p.

[21] *Idem*.

En somme, l'objet de la cybersécurité est de maitriser les risques liés à l'usage du numérique et du cyberespace. Cela concerne toutes les infrastructures, tous les systèmes d'information, services et données ainsi que tous les acteurs qui dépendent du numérique.

2. Cyberdéfense

À l'ère des NTIC, l'affrontement dans le cyberespace est désormais une réalité. Les menaces cyber sont permanentes et en évolution continue. Le nombre et l'intensité des attaques menées dans ce milieu ne cessent de croitre dans des pays fortement numérisé, visant le profit financier, la captation de données, la déstabilisation des institutions par la manipulation des opinions ou paralysie de systèmes étatiques et privés.[22] Désormais, les forces armées quant à elles intègrent le combat cybernétique comme un mode d'action à part entière dont les effets se combinent aux autres dans une manœuvre globale.

Le législateur congolais a eu l'avance de définir la Cyberdéfense dans la loi n° 20/017 du 25 novembre 2020 comme un ensemble des moyens physiques, virtuels et organisationnels mis en place par un pays pour détecter et contrer les Cyberattaques dont la cible et la finalité sont liées à la défense nationale.[23]

La cyberdéfense est une technique pro active qui vise à protéger les systèmes et les informations contre les attaques informatiques. Elle implique l'utilisation de techniques telles que la surveillance des réseaux, l'analyse des menaces, la sécurité des données et la gestion des identités, ainsi que la formation à la sécurité informatique et à la sensibilisation aux menaces.

La cyberdéfense active met l'accent sur l'importance du renseignement cyber qui consiste à collecter, analyser, corréler, contextualiser, de partager les signaux faibles voir de les provoquer afin de passer du mode réactif au mode proactif. Tout en tentant de semer le doute ou la confusion chez l'agresseur. Bien qu'une telle approche requiert le développement d'outils fortement automatisés voire d'intelligence artificielle, et met l'accent sur la capitalisation des connaissances des attaquants qui implique une coopération public-privé internationale plus avancée.[24]

La cyberdéfense est une priorité des Etats fortement numérisés, elle diffère sur leur doctrine et leur gouvernance, notamment sur l'usage et l'organisation des volets offensif et défensif. En ce sens, les pays anglo-saxons ont plutôt opté des

[22] La cyberséfense, priorité ministérielle et enjeu militaire « ministère des Armées », [en ligne], disponible sur [https://www.defense.gouv.fr/], (consulté le 05/08/2024).
[23] Art.4.26, Loi n°20/017 du 25 novembre 2020 préc.
[24] P. PIRON, la cyberdéfense, nouvelle arme géopolitique, op.cit. p.96

structures en charge des deux volets (Cyber Command/NSA aux Etats-Unis et GCHQ/SIS au Royaume-Uni). La France quant à elle a voulu a résolument souhaité séparer la lutte informatique défensive (ANSSI, ministère de l'intérieur) de la lutte informatique offensive (Comcyber, DGA, agences de renseignements) et ce, afin de mieux garantir la protection des libertés fondamentales.[25]

En RDC, depuis le mois d'aout 2023, un Service spécialisé a été créé au sein du Cabinet du Président de la République dénommé « Conseil Nationale de Cyberdéfense » en sigle CNC. Ce service a pour mission principale, la coordination de tous les services en rapport avec la cyberdéfense et le cyber renseignement.[26] En ces termes, dans lignes qui suivent nous passerons en revue les missions du Conseil National de Cyberdéfense **(a)** et l'organisation dudit Conseil **(b)**.

a. Missions du CNC

Conformément à l'Ordonnance-Loi n°23/170 du 15 aout 2023, plusieurs missions sont attribuées à cet organisme, parmi lesquelles nous pouvons énumérés : Conseiller et informer le Président de la république sur toutes les questions ayant trait à la cyberdéfense et Cyber-renseignement ; superviser et coordonner les systèmes nationaux de Cyberdéfense et Cyber-renseignement ; veiller après transmission, à ce que les budgets spécifiques élaborés par les différents services intervenant en matière de cyberdéfense et cyber-renseignement soient en adéquation avec les directives données.

Promouvoir, par ailleurs, la création et le développement des services de cyberdéfense et Cyber-renseignement ; d'encourager la collaboration et la coopération entre les différents services concernés ; proposer au Président de la République des lignes directrices nécessaires à la définition de politique nationale de cyberdéfense et Cyber-renseignement, aussi ilparticipe, en collaboration avec des structures dédiées, à la gestion des situations de crise dans le cyberespace. En fin, il vérifie la conformité de la mise en œuvre de la stratégie de Cyberdéfense et Cyber-renseignement ; il assure en fin, toutes les missions lui confiées par le Président de la république.[27]

---

[25] *Ibidem,* p.97.
[26] Art 1, Ordonnance-Loi n°23/170 du 15 aout 2023 portant création, organisation et fonctionnement d'un service spécialisé dénommé Conseil National de Cyberdéfense, en sigle « CNC », col.44.
[27] Art 2, Ordonnance-Loi n°23/170 du 15 aout 2023, préc.

b. Organisation et fonctionnement du CNC

L'organisation interne et le fonctionnement du CNC sont fixés par un règlement intérieur approuvé par le Président de la République.[28] Le CNC est dirigé par un Coordonnateur qui assure la coordination, l'administration et la surveillance des activités de cyberdéfense et cyber-renseignement, suivant les instructions du Président de la République à qui il fait directement rapport.[29]

Le coordonnateur a rang de conseiller spécial du Chef de l'Etat, il est nommé, relevé de ses fonctions et, le cas échéant, révoqué par le Président de la République. Il a pour rôle d'assurer la liaison entre les institutions extérieures et le CNC en rapport avec les missions de celui-ci.[30]

Dans le cadre de sa compétence, le Coordonnateur statue par voie de décision. Il dispose d'un cabinet restreint composé d'experts et d'un personnel d'appuie suivant le cadre organique fixé par le règlement intérieur.[31] Les membres du personnel du CNC, autres que les Assistants principaux, sont désignés, relevés de leurs fonctions et le cas échéant, révoqués par le Coordonnateur, après approbation du Président de la République.[32]

En ce qui concerne son fonctionnement, le Conseil National de Cyberdéfense bénéficie d'un grand nombre des ressources, dont notamment une dotation émargeant au budget de l'Etat, des subventions, dons et legs etc.[33]

II. Renseignement et sécurité du système d'information

Le renseignement désigne à la fois l'information estimée pour sa valeur et sa pertinence auprès d'une organisation, d'un Etat, ou d'un groupe, ainsi que l'action de fournir ces informations.[34] Dans ce contexte, le renseignement serait un moyen important dans la sécurité des systèmes d'information **(A)**, pour assurer la sécurité informatique **(B)**, contre les cybermenaces qui affectent le bon fonctionnement des outils informatiques, des réseaux de télécommunication et de tous les services et activités humaines qui en dépendent.

---

[28] Art 7, Ordonnance-Loi n°23/170 du 15 aout 2023, préc.
[29] Art 3.al 1, Ordonnance-Loi n°23/170 du 15 aout 2023, préc.
[30] Art 3.al 3, Ordonnance-Loi n°23/170 du 15 aout 2023, préc.
[31] Art 5, Ordonnance-Loi n°23/170 du 15 aout 2023, préc.
[32] Art 6, Ordonnance-Loi n°23/170 du 15 aout 2023, préc.
[33] Art 8, Ordonnance-Loi n°23/170 du 15 aout 2023, préc.
[34] G.ARBOIT et M. MATIEN, « Médias et exploitation politique des services de renseignement », in Annuaire Français de Relations Internationales (AFRI), Ed. Bruyant, Bruxelles, 2015, p.956.

A. Importance du renseignement dans la sécurité des systèmes de l'information

À l'ère du numérique, la sécurité des systèmes d'information est cruciale pour protéger les données et garantir le bon fonctionnement des organismes tant publics que privés. Par ailleurs, le renseignement permet d'anticiper et des prévenir les dangers ainsi que de détecter les différentes menaces dans la sécurité des systèmes d'informations de l'Etat. De ce fait, il faudra au préalable déterminer concrètement le domaine d'application de la sécurité d'un système d'information **(1),** avant de définir le rôle des cybergardiens au sein des services de sécurité **(2).**

1. Domaine d'application de la sécurité d'un système d'information

Pour une organisation publique que privée, toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité d'un système d'information. En fonction de son domaine d'application, la sécurité informatique peut se décliner en : sécurité physique et environnementale ; sécurité de l'exploitation ; sécurité des réseaux ; sécurité logique, sécurité applicative et sécurité de l'information ; sécurité des infrastructures des télécommunications et en fin la cybersécurité.[35]

De ce qui précède, dans un contexte beaucoup plus restreint, s'abordedeux composantes de la sécurité d'un système d'information dans les points qui suivent : d'une part la sécurité d'exploitation **(a)**, et d'autre part, la sécurité des infrastructures des télécommunications **(b).**

a. Sécurité d'exploitation

La sécurité de l'exploitation doit permettre un bon fonctionnement opérationnel des systèmes informatiques. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jour. La sécurité de l'exploitation dépend fortement de son degré d'industrialisation, qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches.[36]

Bien que relevant de la responsabilité de l'exploitation, ces conditions concernent directement la conception et la réalisation des applications elles-mêmes et

[35] S. GHERNAOUTI, *Cybersécurité sécurité informatique et réseaux*, 5ème édition © Dunod, Paris- Malakoff, 2016, pp.6-7.
[36]S. GHERNAOUTI, *Cybersécurité sécurité informatique et réseaux*, *op.cit*., pp.7-8

leur intégration dans un système d'information. Les points clés de la sécurité de l'exploitation sont les suivants : gestion du parc informatique ; gestion des configurations et des mises à jour ; gestion des incidents et suivi jusqu'à leur résolution ; plan de sauvegarde ; plan de secours ; plan de continuité ; plan de tests ; inventaires réguliers et, si possible, dynamiques ; automatisation, contrôle et suivi de l'exploitation ; analyse des fichiers de journalisation et de comptabilité ; gestion des contrats de maintenance etc.[37]

b. Sécurité des infrastructures des télécommunications

La sécurité de télécommunications consiste à offrir à l'utilisateur final et aux applications communicantes, une connectivité fiable de « bout en bout ». Cela passe par la réalisation d'une infrastructure réseau sécurisée au niveau des accès au réseau et du transport de l'information (sécurité de la gestion des noms et des adresses, sécurité du routage, sécurité des transmissions à proprement parler) et cela s'appuie sur des mesures architecturales adaptées, l'usage de plates-formes matérielles et logicielles sécurisées et une gestion de réseau de qualité.

La sécurité des télécommunications ne peut à elle seule garantir la sécurité des informations. Elle ne constitue qu'un maillon de la chaîne sécuritaire car il est également impératif de sécuriser l'infrastructure informatique dans laquelle s'exécutent les programmes. Pris au sens large, cela comprend la sécurité physique et environnementale des systèmes notamment poste de travail de l'utilisateur, serveur ou système d'information.[38]

2. Cybergardiens au sein des services de sécurité

En droit comparé, le législateur français a prévu à côté de l'ANSSI (l'Agence Nationale de Sécurité des Systèmes d'information), des services de cybergardiens dans le ministère de l'intérieur et de la défense. A titre d'exemple, la DIRISI (Direction Interarmées des Réseaux d'Infrastructures et des Systèmes d'Informations) qui est l'opérateur de gestion d'administration des réseaux, BFTI (Brigade d'Enquête sur les fraudes aux technologies de l'information), DGSI (Direction Générale de la Sécurité Intérieure) qui a pour mission de détecter les nouvelles cybermenaces et de permettre à l'Etat de s'en prémunir.[39]

En RDC, le ministère de l'intérieur dispose d'un cybergardiens au sein de la Police nationale dans le cadre de sa réforme. Il s'agit de la DTNTIC (Direction des

---

[37] *Idem.*
[38] S. GHERNAOUTI, *Cybersécurité sécurité informatique et réseaux*, *op.cit*., p.16.
[39] X.LEONETTI, *Guide de Cybersécurité, Droits, méthodes et bonnes pratiques*, Ed. L'harmattan, Paris, pp.121-122.

télécoms et des Nouvelles technologies de l'Information et de la communication. tel que nous l'avions annoncé un peu plus haut, la DTNTIC a pour objet de lutter contre la cybercriminalité.[40]

Au sein des FARDC, il existe un département des NTIC qui a comme attributions : de rechercher et appliquer les nouvelles NTIC dans les Forces armées ; émettre des avis techniques sur les matériels et équipements des NTIC en dotation au sein des Forces armées.[41] De ce qui précède, le ministère de la défense ne dispose pas des services des cybergardiens au regard de la prise en compte ou de la considération des NTIC. Ceci demeure une exposition aux cyberattaques, dans la mesure où l'utilisation des NTIC fait jeu égal avec le pouvoir des armes.

B. Sécurité informatique

La sécurité informatique passe par une gestion rigoureuse des ressources humaines, des systèmes informatiques, des réseaux, des locaux, de l'infrastructure environnementale, et des mesures de sécurité.[42] La maîtrise de la sécurité informatique est avant tout une question de gestion dont les outils, technologies ou solutions de sécurité constituent une partie liée à la réalisation opérationnelle des environnements sécurisés. En première vue, des outils comme ceux de « chiffrement ou les pare-feu » ne permettent pas de sécuriser correctement un environnement à protéger s'ils ne sont pas inscrits dans une démarche de gestion précise des risques. Et s'ils ne sont pas accompagnés de procédures qui régissent leur utilisation ou configuration.[43]

En ce sens, piloter la sécurité correspond à la volonté de maîtriser les risques liés à l'usage des technologies de l'information, les coûts engendrés pour se protéger des menaces et au déploiement des moyens nécessaires pour gérer les incidents ou les situations de crise, pour réagir à une situation non sollicitée mettant en danger la performance du système d'information et celle de l'organisation concernée.

Par ailleurs, gouverner la sécurité informatique s'inscrit dans une dimension humaine, organisationnelle, managériale et économique des organisations, répondant à une volonté politique de leur direction pour maîtriser les risques et protéger les valeurs.

Ainsi, la sécurité repose sur la complémentarité et la cohérence de ces dimensions. Elle n'est jamais acquise définitivement. La constante évolution des

---

[40] Art 45, Décret n°13/017 du 06 juin 2013, préc.
[41] Art 21, Ordonnance n°13-076 du 17 juin 2013 portant organisation et fonctionnement du service de communication et d'information des Forces armées, in J.O.RDC, 22 juin 2013, n°spécial, col.158.
[42] S. Ghernaouti, *Cybersécurité sécurité informatique et réseaux, op.cit.,* p. 20
[43] *Idem.*

besoins, des systèmes, des menaces ou des risques rend instable toute mesure de sécurité. Dans ce contexte, la sécurité informatique ne peut s'appréhender que comme un processus continu de gestion afin de répondre de manière optimale (en termes de coût et de niveau de sécurité) aux besoins de production de l'organisation et de protection de ses actifs.

1. Stratégie de cybersécurité

La lutte contre la cybercriminalité et toute forme d'intrusion doit s'appuyer préalablement sur la connaissance des acteurs, de leurs motivations et leurs manières d'agir. Cela demande de comprendre entre autres, quelle est leur vision stratégique, quels sont les moyens opérationnels qu'ils utilisent, comment sont-ils organisés. Mais aussi savoir, quelle est la répartition des tâches, de quelle manière leurs agents sont-ils recrutés, comment sont-ils rémunérés, quels sont les processus, quels leurs modèles économiques, comment l'argent du crime est-il blanchi, etc.

La sécurité informatique d'une organisation doit s'appréhender d'une manière globale et stratégique (notion de stratégie de sécurité) et s'appuie sur : la définition d'une politique de sécurité ; la motivation et la formation du personnel ; la mise en place de mesures proactives et réactives ; l'optimisation de l'usage des technologies de l'information et des communications (TIC) ainsi que de celui des solutions de sécurité.

2. Architecture de cybersécurité

L'architecture de cybersécurité reflète l'ensemble des dimensions organisationnelle, juridique, humaine et technologique de la sécurité informatique à prendre en considération pour une appréhension complète de la sécurité d'une organisation. Définir une architecture globale de la sécurité permet de visualiser la dimension générale et la nature transversale de la sécurité informatique d'une entreprise et d'identifier ses diverses facettes et composantes afin de pouvoir les développer de façon cohérente, complémentaire et harmonieuse. Cela facilite l'intégration de mesures, de procédures et d'outils de sécurité.[44]

En RDC, sur l'aspect juridique, le législateur a mis en place en 2023, un organe de sécurité des systèmes informatiques dénommé l'Agence Nationale de Cybersécutité (ANCY). Cet organisme bien que pas opérationnel, il est une avancée majeure pour l'accompagnement des institutions tant publiques que privées en matière de Cybersécurité.

[44]S. GHERNAOUTI, *Cybersécurité sécurité informatique et réseaux, op.cit.,* p.16.

A la lumière de tout ce qui précède,la République Démocratique du Congo, se bat très fortement à l'adaptation du monde technologique. Ceci se matérialise au travers des créations des différents cadres institutionnels des activités numériques et l'élaboration des stratégies y afférentes. La plus lourde tâche demeure l'opérationnalité de ces activités par des organismes en place et la mise en œuvre effective des stratégies dans ce secteur du numérique. Par ailleurs, la criminalité traditionnelle en RDC évolue et s'étend, posant de nouveaux défis pour les services de renseignement. Les attaques cyber sont une réalité. Les moyens et les champs d'action des criminels se diversifient, incluant des activités telles que le trafic de ressources naturelles, la contrebande, et les crimes transfrontaliers.

Les services de renseignement congolaisdoivent, cependant, adapter leurs stratégies pour faire face à ces menaces croissantes. Cela inclut l'utilisation des technologies avancées pour la surveillance et la collecte de données. Mais également lacoopération internationale pour lutter contre les réseaux criminels transnationaux. En outre, il est crucial de renforcer les capacités locales en matière de renseignement et sécurité, en formant les agents notamment ceux de la DTNTIC (Direction des télécoms et des Nouvelles technologies de l'Information et de la communication) etc. ; et en améliorant les infrastructures.

Il en est de même pour les organismes à des fins numériques, notamment le conseil national du numérique (CNN) et l'Agence nationale de développement du numérique (ADN) avec son statut d'un établissement public chargé de la promotion des télécommunications et des technologies de l'information et de la communication, et sa mission qui s'articule autour de la mise en œuvre du Plan National du Numérique en RDC.[45] Ses organismes doivent établir une étroite collaboration avec les autorités du secteur de renseignement pour innover avec les techniques de renseignement à l'ère des avancées technologiques. Ceci aux fins de faire face à l'extension de champs et moyens de criminalité traditionnelle en RDC.

Clément KIVUNA TSHEKO. (INGENII)
Licencié en Droit public International (UPC) système PADEM.
Chercheur en Droit du numérique et dans les domaines d'intervention varié.

BIBLIOGRAPHIE

[45] PLAN NATIONAL DU NUMÉRIQUE - Horizon 2025 - Septembre 2019. p.88.

I. LÉGISLATION CONGOLAISE

1)Textes législatifs

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

2)Textes réglementaires

- Ordonnance n°13-076 du 17 juin 2013 portant organisation et fonctionnement du service de communication et d'information des Forces armées, in J.O.RDC, 22 juin 2013, n° spécial, col.158.
- Ordonnance-Loi n° 23/010 du 13 mars 2023 portant code du numérique, *in J.O RDC*, n° spécial 11 avril 2023.
- Ordonnance-Loi n°23/170 du 15 aout 2023 portant création, organisation et fonctionnement d'un service spécialisé dénommé Conseil National de Cyberdéfense, en sigle « CNC », col.44.
- Décret n°13/017 du 06 juin 2013 déterminant l'organisation et le fonctionnement du Commissariat Général de la Police Nationale Congolaise.

.

II. LÉGISLATION INTERNATIONALE

-Convention IV de La Haye du 18 octobre 1907 concernant les lois et coutumes de la guerre sur terre et son Annexe.

III. OUVRAGES

1) Ouvrages spécifiques

1. CHOPIN O. et OUDET B., *Renseignement et sécurité*, Ed. Armand Collin, Paris, 2023.
2. LEONETTI X., *Guide de cybersécurité*, *Droits, méthodes et bonnes pratiques*, Ed. L'Harmattan, Paris, 2015.
3. GHERNAOUTI S., *Cybersécurité : Analyser les risques, Mettre en œuvre les solutions*, 6e Ed. Dunod, Malakoff, 2019
4. GHERNAOUTI S., *Cybersécurité sécurité informatique et réseaux*, 5ème édition © Dunod, Paris- Malakoff, 2016.
5. K.NDUKUMA ADJAYI, *Droit des télécoms et du numérique,* Ed. L'Harmattan, Paris, 2019, P.35.
6. FILIOL E., et RICHARD P., *Cybercriminalité : Enquête sur les mafias qui envahissent le web*, Ed. Dunod, Paris, 2006.

IV. ARTICLES

1. ARBOIT G. et MATIEN M., « Médias et exploitation politique des services de renseignement », in Annuaire Français de Relations Internationales (AFRI), Ed. Bruyant, Bruxelles, 2015, p.956.
2. HAYEZ P., « Le renseignement facteur de puissance » *in Afri*, vol.4, 2008, p. 520.
3. MASSON M., Le renseignement d'intérêt militaire, « L'ENA hors les murs », n°365, octobre 2006, p. 9
4. PIRON P., la cyberdéfense, nouvelle arme géopolitique « La Jaune et la Rouge », Magazine N°753, p.3.
5. WARUSFEL B., « Le cadre juridique et institutionnel des services de renseignement en France *», in Fondation pour les Etudes de Défense, La Documentation française*, Paris, 1997, p. 20.
6. Weissbrodt D., *« Cyber-Conflict, CyberCrime, and CyberEspionage », University of Minnesota Law School Scholarship Repository*, 2013, vol. 347, p. 354.

V. RESSOURCES EN LIGNE

1) Articles accessibles sur Internet

1. DIOTTE P., « Les quatre grands auteurs de menaces et le cyberespionnage :

   Quand la Chine, la Russie, l'Iran et la Corée du Nord espionnent en ligne », in Revue militaire canadienne, Vol. 20, no. 4, automne 2020, p.32.
2. GHRENASSIA C. et R. BINSARD, « La preuve, le renseignement et le droit », [en ligne] disponible sur : [https://www.dalloz-actualite.fr/], (consulté le 05/08/2024).
3. LAURENT S-Y., « Pour une véritable politique publique du renseignement », Institut Montaigne étude juillet 2014.

2) Pages Web et liens HTML

1. La cyberdéfense, priorité ministérielle et enjeu militaire « ministère des Armées », [en ligne], disponible sur [https://www.defense.gouv.fr/], (consulté le 05/08/2024).
2. Les nouvelles technologies de l'information et de la communication, [en ligne] disponible sur : [Http : //www.certitude-management.com], (consulté le 11 aout 2024).

VI. AUTRES DOCUMENTS

- Présidence de la république : « Stratégie nationale de cybersécurité de la République Démocratique du Congo », rédigé par la commission technique pour la cybersécurité, Kinshasa- juillet, 2022, p.22.

Table de matière