CAHIERS AFRICAINS DES DROITS DE L'HOMME ET DE LA DÉMOCRATIE AINSI QUE DU DÉVELOPPEMENT DURABLE
REVUE AFRICAINE INTERDISCIPLINAIRE

ISSN : 2791-1063 (Imprimé)
ISSN : 2791-1071 (En ligne)

28ème année - Numéro 83 - Volume 1 - Avril-Juin 2024

LA SOUVERAINETE DES ETATS A L'EPREUVE DE LA CYBERGUERRE. POUR QUELLE CYBERDEFENSE CONGOLAISE ?

Par

Georges SUMAILI SHINDANI
Professeur à l'Université Libre de Kinshasa

et

Pathy MUKUNA WA MUKUNA
Apprenant en Relations Internationales à l'Université de Kinshasa

RÉSUMÉ

Le système interétatique né du traité de Westphalie a déterminé les concepts directeurs des relations internationales à savoir : l'équilibre des puissances, l'inviolabilité de la souveraineté nationale et le principe de non-ingérence dans les affaires d'autrui. La période post-guerre froide, voit l'ordre westphalien être remis en cause à l'ère du cyberespace. L'actuel siècle est marqué par la transition numérique des Etats et de leurs domaines de souveraineté ; ainsi, le cyberespace est devenu un champ de confrontation géopolitique et de compétition stratégique entre les Etats et les autres acteurs du cyberespace. Toute cyberattaque entraînant la destruction physique de biens ou la mort pourrait automatiquement être assimilée à une attaque armée susceptible de compromettre la sécurité de l'Etat.

Mots-clés *: Cyberguerre, sécurité, sécurité globale, souveraineté, défense, guerre, cyberdéfense*

ABSTRACT

The interstate system born of the Treaty of Westphalia determined the guiding concepts of international relations: the balance of power, the inviolability of national sovereignty and the principle of non-interference in the affairs of others. The post-Cold War period has seen the Westphalian order challenged in the age of cyberspace. The current century is marked by the digital transition of states and their areas of sovereignty; cyberspace has thus become a field of geopolitical confrontation and strategic competition between states and other cyberspace players. Any cyberattack resulting in the physical destruction of property or death could automatically be assimilated to an armed attack likely to compromise state security.

Keywords*: Cyberwar, security, global security, sovereignty, defense, war, cyberdefense*

I. INTRODUCTION

Depuis les attentats du World Trade Center aux États-Unis, et la libéralisation de l'Internet, la mondialisation a basculé vers la globalisation qui à son tour a bousculé l'équilibre dans l'ordre des choses en relations internationales surtout en ce qui concerne la puissance et de surcroit sur la question de l'importance de la Guerre. Ce questionnement fait suite à l'invasion brutale du cyberespace comme lieu de conflictualité. L'ouverture des frontières, l'immédiateté de l'information, la fluidité des échanges, L'augmentation des flux financiers dans le monde a minimisé la fonction des Etats dans les grandes questions de la stabilité de scène internationale. Les nouvelles technologies de l'information et de la communication ont centralisé la vie internationale.

Le cyberespace pose la question sur l'autonomie stratégique des Etats et sur l'exercice de la souveraineté. A défaut d'une affirmation de puissance et d'une plénitude dans l'exercice de la souveraineté, l'autonomie stratégique des Etats se retrouve limiter avec l'apparition des vers et virus qui désormais se classent au rang des armes classique. Désormais, c'est dans le cyberespace que se jouent les guerres du futur. Les Etats sont dans l'impératif démarche de gagner la guerre du numérique et poursuivre les transformations des champs de la défense et de la sécurité dans le cyberespace en assurant l'autonomie stratégique. Les nouveaux acteurs du cyberespace sans arrogance à gouverner apparaissent, faire concurrence à l'État plus grave, ces nouveaux acteurs non étatiques du cyberespace conçoivent l'Etat comme un acteur dépassé.

II. MÉTHODE ET THÉORIE

Guy Rocher définit la méthode systémique comme étant toute recherche théorique ou empirique qui partant du postulat que la réalité sociale présente les caractères d'un système, interpréter et expliquer les faits sociaux par les lois d'interdépendances qui relient entre eux et qui forment une totalité[1]. Cette méthode considère l'objet de recherche comme un système, c'est-à-dire une réalité sociale. Elle interprète et explique les phénomènes sociaux par les liens d'interdépendance qui les relient entre eux et qui forment une réalité[2].

La formulation adoptée par Hoffman est moins abstraite et moins complexe : « un système international est un réseau de relations entre les unités de base de la politique mondiale ; il se caractérise par l'étendue des objectifs que poursuivent ces unités et des tâches qu'elles accomplissent par les moyens utilisés pour atteindre ces objectifs et exécuter ces tâches. Ce réseau est

[1] ROCHER G., cité par MULUMBATI N., « Manuel de sociologie générale, collection savoir et connaitre », Africa, Lubumbashi, 2001, p.20.
[2] BOLA N., *Science administrative*, cours inédit, G1, RI, FSSAP, ULK, Kinshasa, 2011-2012.

déterminé en grande partie par la structure du monde, par la nature des forces qui œuvrent entre ou au sein des unités principales, et par les capacités, la structure du pouvoir et la culture politique de ces unités »[3]. Un système international, pour Hoffman, est donc identifié à la totalité des relations internationales. En ce qui concerne la notion du système en Relations Internationales, il convient de concevoir les Relations Internationales comme un système, c'est-à-dire un ensemble complexe d'acteurs en interaction dans un environnement donné.

Pour appliquer l'approche systémique, il faut penser circulairement et non linéairement, c'est-à-dire qu'il faut se réaliser que tous les éléments (Acteurs étatiques et non étatiques) sont interconnectés. On ne peut pas comprendre la cyberconflictualité si on le prend d'une façon isolé. Pour qu'elle devienne une réalité dans le système global, il faut comprendre que tous les éléments et acteurs du système agissent dans une interconnexion qui le rend dépendante des uns vis-à-vis des autres. C'est de cette interconnexion que nait aussi le conflit du cyberespace.

Pendant que le monde universitaire se cherchait en méthodologie et en théories, le Cyberespace est devenu un enjeu fortement mobilisateur dans les Relations Internationales. A partir des années 1990, les technologies de l'information et de la communication numérique ont été perçues par les rares chercheurs qui s'y sont intéressés comme ayant des effets structurants sur leur environnement social et politique. Le cyberespace se présente comme un système sociotechnique qui s'est progressivement globalisé au point de devenir un enjeu important pour le système international.

Contrairement aux réalistes, les acteurs d'orientation néolibérale s'entendent pour dire que la mondialisation restreint l'autonomie des Etats en matière de politique macroéconomique[4]. La mondialisation est ce qui caractérise le nouvel ordre mondial depuis la fin de la Guerre Froide. L'ouvrage de James Rosenau[5] est une référence majeure de cette nouvelle pensée. Il a cherché les conditions d'une régulation d'un monde bousculé par les phénomènes transnationaux[6]. Son idée de départ est que la planète est entrée dans une phase chaotique et que les théories classiques des relations internationales ne sont plus en mesure d'expliquer le changement qu'il croit voir s'opérer à l'échelle global. D'abord, que depuis les années cinquante, on

[3] S. Hoffman, International Systems and International Law, World Politics, XIV, octobre 1961, p.207

[4] KEOHANE R.O. et MILNER H.V., *Internationalization and Domestic Politics*, Cambridge University Press, Cambridge, 1996.

[5] ROSENAU J.N., *Turbulence in World Politics: a Theory of Change and Continuity*, Princetown University Press, Princetown, 1990.

[6] ROSENAU J.N., *Along the Domestic-Foreign Frontier. Exploring Governnce in a Tribulent World*, Cambridge University Press, Cambridge, 1997.

assiste à une montée en puissance des individus au sein des sociétés mais aussi dans les affaires internationales.

Avec l'avènement du cyberespace dans la globalisation, une cité globale est en train d'émerger, comme en témoigne les divers mouvements sociaux et politique transnationaux et l'amorce d'un transfert d'allégeance allant de l'Etat vers des regroupements infranationaux, transnationaux et internationaux. Ces allégeances qui sont transférées dans le cadre de la globalisation sont de nature à causer l'érosion de la souveraineté des Etat. Avec la globalisation contemporaine, l'interdépendance est devenue une réalité. Elle est l'effet multiplicateur des nouvelles technologies de communication, de la production et de la consommation de masse.

III. LA SOUVERAINETÉ DES ETATS

Le terme « souveraineté » est issu du latin superanus, superus, «supérieur»[7]. Le mot a fait son apparition au bas moyen âge, vers le milieu du XIIe siècle. Ensuite, la souveraineté « s'est précisée au XVIe et au XVIIe siècles, en rapport direct avec l'apparition et la consolidation de l'Etat au sens propre, moderne du mot. Le mot sert à désigner le statut de celui qui a le pouvoir de gouverner sur un territoire et ses habitants. Une pensée émise en première par Bodin qui avait une conception très limitée ou absolue de la souveraineté. Pour ce dernier, la souveraineté est la puissance absolue et perpétuelle de la République. Il va même encore plus loin en opinant que « la souveraineté n'est limitée ni en puissance, ni en charge ni à certains temps »[8].

Pour Léon Duguit, la souveraineté est un concept embrouillé et obscur ayant subi d'excessives extensions[9], il voit dans la souveraineté un principe totalement vide[10]. Selon Krasner [11], « la souveraineté est érodée par un aspect du nouveau système international qui est la mondialisation. Un même constat semble pouvoir être dressé aujourd'hui, si bien qu'on voit dans la souveraineté un « concept aussi inconsistant qu'incontournable »[12], un « voile dont il nous faut comprendre ce qu'il cache »[13], ce qui n'est pas étonnant pour Stéphane TAILLAT pour qui « la souveraineté est elle-même un concept qui a des

---

[7] REY. A., *Dictionnaire historique de la langue française*, Le Robert, Paris, 1992, p. 2000.
[8] Jean BODIN, *Les six livres de la république*, Paris, Jacques du Puys, 1583, p. 122.
[9] R. CARRÉ DE MALBERG, *Contribution à la théorie générale de l'État spécialement d'après les données fournies par le droit constitutionnel français,* t. I, Librairie du Recueil Sirey, 1920, p. 191.
[10] DUGUIT.L., *Traité de droit constitutionnel* – Tome deuxième : La théorie générale de l'État – Première partie : Éléments, fonctions et organes de l'État, 3e éd., De Boccard, 1928, p. 27.
[11] KRASNER S., *Sovereignty : organized Hypocrisy* , Princetown University Press, Princetown, 1999.
[12] BERNS T., « Souveraineté, droit et gouvernementalité », Arch. phil. Droit 2002, p. 353.
[13] DE SMET F., *Le mythe de la souveraineté – Du Corps au Contrat social*, EME, coll. Politique & culture, 2014, p. 8.

fondements à la fois juridiques et dans la philosophie politique, mais dont la pratique n'a jamais été fixe »[14].

Pour nous, la souveraineté est l'autorisation de bâtir de l'Etat qui lui est conféré par le traité de Westphalie pour ainsi dire par le Droit International public. La souveraineté et la puissance sont le deux facettes de la même pièce, la souveraineté étant le stade de départ et la puissance celui d'arrivé. Nous pouvons même rajouter que la puissance est le stade extrême de la souveraineté.

IV. LES NOUVELLES MENACES CONTRE LA SOUVERAINETÉ

Avant le XXe siècle, la scène internationale n'avait pas connu beaucoup des attaques contre le principe fondamental westphalien, celui de la souveraineté et la centralité de l'Etat. Dans cette logique des choses, l'Etat possédait l'entièreté de l'exercice de la souveraineté avec toutes les capacités de faire face à toutes menaces venant des autres acteurs ou organisme politique et économique en concurrence avec l'Etat. De nos jours, aucun de ses éléments ne fait l'unanimité. En effet, au cours des trente dernières années, partout dans le monde, l'Etat a fait l'objet d'une redéfinition restrictive de ses rôles et de ses pouvoirs ou capacités. Sa capacité de régulation de l'économie, des marchés, des échanges, de ses défendre, de l'information et de la communication, tout comme l'exercice de la souveraineté dans ses dimensions (monétaire, sécuritaire, économique) et son unité sociologique et culturelle s'en sont trouvées amoindries et amputée.

Le cyberespace est devenu ainsi le théâtre d'une nouvelle forme de conflictualité dénommée « cyberconflictualité » dont la cyberguerre occupe le haut de l'échelle des menaces contre la souveraineté des Etats. Le cyberespace se présente comme un espace sans frontière et conflictuel. Les dix dernières années ont démontré que les attaques numériques ont causé des dommages irréparables. Nous en avons pour preuve qu'il y a deux décennies, on ne pouvait être assuré que des acteurs comme Google, Facebook ou Twitter seraient en mesure de défier la souveraineté des États sans s'exposer à de puissantes ripostes. Ces acteurs non étatiques ont atteint la dimension de faire vaciller même le socle de la démocratie, de l'expression de la souveraineté populaire de la super puissance mondiale.

Avec la virtualisation du monde, la guerre a connu une mutation vers la cyberguerre comme nouvelle expression de la conflictualité, de nature très différente des conflits anciens et actuels, symétrique ou beaucoup plus asymétriques. L'arme nucléaire qui servait pour l'affirmation de puissance par

[14] TAILLAT.S., *Cyberguerre - Cyberpaix et la conflictualité*, Séminaire du Collège des Bernardins, Chaire des Bernardins, Paris, 2016, p. 14.

les Etats, se voient concurrencer par les cyberarmes qui ouvrent un nouvel espace stratégique dont l'Etat n'a plus le monopole de la détention ni de l'utilisation. Le caractère massif d'une cyberattaque est capable de paralyser un Etat. Aujourd'hui les cyberattaques militaires peuvent aussi bien frapper des équipements matériels, que des actifs immatériels à des fins de renseignement notamment, ou encore cibler les utilisateurs de ces moyens informatiques. Le cyberespace a transformé la notion de l'État ainsi que celle de la souveraineté.

Ainsi, la définition de Jean Bodin n'est donc plus valable aujourd'hui dans un contexte de la globalisation qui entraine une multiple interdépendance croissante entre les Etats. Ainsi, il nous semble que les relations internationales soient dorénavant mues par d'autres enjeux que l'affirmation de la souveraineté des États par d'autres acteurs non-étatiques.

V. LA CYBERGUERRE

L'adoption du cyberespace comme le cinquième domaine militaire après la terre, la mer, l'air et l'espace par de grandes puissances du cyberespace, a commencé par les États-Unis, le Royaume-Uni et la France. En 2016, l'Organisation du traité de l'Atlantique Nord (Otan) à son tour avait reconnu le cyberespace comme un domaine militaire opérationnel[15]. Alors que les Etats s'accordaient sur la cyberguerre, Martin Libicki dénonçait cette métaphore comme mal adaptée à la compréhension de cet environnement[16]. Le concept même de cyberguerre ne faisait pas consensus dans le monde académique, en dépit de son large succès médiatique et politique. Thomas Rid[17] estime que les opérations menées jusqu'à présent ne relèvent pas de la guerre, définie comme un « acte de force, politique, instrumentalisé et potentiellement létal, mené grâce à un code malveillant », mais ne sont que des versions à peine plus sophistiquées d'activités aussi anciennes que la guerre : l'espionnage, le sabotage et la subversion.

Le cyberespace constitue aujourd'hui une dimension à part entière de l'activité humaine, à l'égal de la terre, de la mer, de l'air et de l'espace. A la différence des autres dimensions, le cyberespace est dématérialisé. Si de nos jours, le cyberespace est le cinquième théâtre de la conflictualité et que dans les quatre premiers domaines, l'armée et la guerre étaient bien présente, il faut affirmer que dans le cyberespace, les armes et la guerre est aussi bien réelle.

Le concept de cyberguerre a été plébiscité à tort par les journalistes et commentateurs d'être une guerre de l'information et mais aussi, par d'autres

[15] Rand Corporation, « Operationalizing Cyberspace as a military domain », juin 2019, en ligne.
[16] LIBICKI M., "Cyberspace is Not a Warfighting Domain", I/S: A Journal of Law and Policy for the Information Society, vol. 8, n°2, 2012, pp. 321-336.
[17] RID. T., "Cyber War Will Not Take Place", Journal of Strategic Studies, 2012, pp. 32-35.

spécialistes (scientifiques et politiques) en relations internationales pour qui la cyberguerre était improbable. Les journalistes utilisent souvent à « contresens le terme "guerre de l'information", à la fois pour mal traduire et pour exciter les foules autour de "guerres" inexistantes. En réalité, en anglais, Information ne se réfère pas aux "nouvelles" (news), mais plutôt qu'aux technologies de l'information, aux processus qui en dérivent et à leurs contenus cognitifs »[18].

C'est aussi l'avis de Frederick Douzet[19] pour qui, la militarisation du cyberespace s'explique en partie par une compréhension plus avancée de l'Internet et des technologies numériques de la part des acteurs de la défense, qui leur a permis de mieux anticiper et faire connaître la menace, et de rapidement allouer des moyens à ce nouveau domaine, contribuant ainsi à définir les priorités de l'État autour des questions de sécurité nationale. Ainsi, pour Daniel Ventre[20], comme pour Olivier Kempf[21], le cyberespace constitue un nouveau milieu, qui se superpose aux milieux traditionnels (terre, mer, air), à l'espace et au nucléaire, ce qui n'implique pas pour autant qu'il domine les autres ou que la « cyberguerre » constitue à elle seule un milieu autonome de la guerre. Bien avant même la guerre en Ukraine, d'après Robert Kaiser, les cyberattaques de 2007 contre l'Estonie avait servi de catalyseur à la matérialisation de la cyberguerre et continuerait d'influer sur la manière dont les États se représenteraient les menaces futures de cyberguerre[22].

Le cyber est désormais partout dans les opérations militaires. Il est au cœur des armements. La seule certitude en la matière est que les cyberopérations font désormais partie de l'arsenal des plus grandes armées et viennent en appui de tous les moyens utilisés pour mener la guerre ; et que le cyberespace est devenu un nouvel espace de confrontation dans les rivalités de pouvoir géopolitiques entre une multitude d'acteurs, entraînant une prolifération des opérations dont les plus avancées viennent généralement des Etats et des acteurs non-étatiques.[23]

Le deuxième point pour laquelle nous voulons nous inscrire en faux, c'est la létalité dans la cyberguerre. Pour bon nombre des chercheurs appartenant à l'ancienne école de la guerre, le critère de la guerre qui demeure est celui de

[18] Laurent Murawiec, Effets spéciaux: la Guerre au XXIème siècle, Odile Jacob, Paris, 2000.
[19] Douzet F. et Géry. A., « Le cyberespace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace », dans *Hérodote*, Éditions La Découverte, N° 177-178, Paris, 2020, pp. 329-350.
[20] Voir les ouvrages de M. Daniel Ventre « Cyberattaque et cyberdéfense » et « Cyberespace et acteurs du Cyberconflit » ainsi que le livre dirigé par M. Daniel Ventre « Cyberguerre et guerre de l'information – stratégies, règles et enjeux » aux éditions Lavoisier.
[21] Voir notamment l'ouvrage co-dirigé par Stéphane Dossé et Olivier Kempf, *Stratégie dans le cyberspace*, Esprit du Livre, 2011.
[22] Kaiser R., "The Birth of Cyber War", Political Geography, vol. 46, 11-20, 2015.
[23] http://www.oai.cairn.info consulté le 23/02/ 2023 à 15h10.

l'existence ou non de morts humaines touchant soit les parties militaires au conflit, soit les populations environnantes (civiles). Et continu de retenir le nombre de mille morts militaires par an, identifié par les polémologues pour marquer le seuil à partir duquel il y a guerre[24]**.** Au sens clausewitzien d'une effusion de sang qui sert à imposer sa volonté à un acteur politique, cela est douteux.

Si hier, les cyberattaques étaient virtuelles, les cyberattaques ont de plus en plus de conséquences dans le monde réel. La technologie inonde le domaine de la défense et ne fait qu'accroître sa dépendance vis-à-vis du cyberespace. Les réseaux et systèmes de communication sont de plus en plus interconnectés. En cas d'infection virale, les répercussions sont rapidement régionales, voire mondiales. Nous affirmons que la cyberguerre peut aussi être définie comme la conduite d'actes de guerre par l'usage stratégique de la force, potentiellement létal, à des fins politiques par le biais d'attaques informatiques.

La mise en réseau des états-majors et l'embarquement d'informatique dans les armes a provoqué une augmentation certaine de l'efficacité. On parle aujourd'hui de systèmes d'armes, de systèmes de commandement informatique (SIC). Et il est vrai que l'efficacité est palpable : avec la précision des missiles ou encore les capacités des avions de chasse moderne, des drones, et autres engins de guerre. Désormais**,** un avion n'est plus un porteur seulement de bombes, c'est aussi un ordinateur qui vole et qui peuvent être dévié vers d'autres cibles et ainsi causer la létalité de la cyberguerre. Les avions de chasse actuels (F-15) peut être la cible des cyberattaques et comme conséquence logique, l'avion pourrait tirer des bombes qui ne tomberaient pas dans le cyberespace, mais dans l'espace physique et causerait des pertes en vies humaines. Désormais, on peut envoyer un code malveillant aux avions qui donnerait de fausses informations qui feront dévier les missiles de leurs trajectoires.

La cyberguerre a d'ores et déjà commencé et pourrait prendre des proportions inattendues dans les années qui viennent. S'il faut manier le terme avec précaution, force est de constater que les outils informatiques font désormais partie intégrante de la plupart des conflits géopolitiques contemporains et conduisent à l'émergence de nouvelles menaces, diffuses et imprévisibles. Les cyberattaques sont difficiles à anticiper, à détecter, à attribuer, à décourager et à contrer. Leur spécificité rend ainsi les paradigmes stratégiques classiques et les règles internationales obsolètes, à l'heure où les États mènent dans le cyberespace des opérations qui flirtent parfois avec les limites de la déclaration de guerre. À l'ère du numérique, alors que la course aux cyberarmes a bel et bien commencé et que ses conséquences sont incertaines, il semble nécessaire de repenser les cadres de la sécurité collective.

[24] http://www.frstrategie.org, consulté le 04 /07/ 2023 à 13h 55'.

VI. LES IMPACTS DE LA CYBERGUERRE SUR LA SOUVERAINETÉ

Lorsque les attaques cybernétiques visent les infrastructures vitales d'un Etats comme les systèmes de santé, des énergies hydrauliques et électriques, de transports, des industries nucléaires, financières et monétaires. Les conséquences ne seront pas qu'au niveau des pertes en vies humaines mais aussi de l'existence même de l'Etat. Au point où on parle désormais d'un « blocus électronique », qui constituerait un acte de guerre au même titre et degré qu'un blocus naval. La cyberguerre est le type d'attaque le plus grave qui mette en jeu la sécurité d'un Etat ou ses intérêts fondamentaux.

Contrairement à un acte d'agression conventionnel (franchissement d'une frontière, invasion d'un territoire, bombardement, etc.), l'acte d'agression informatique a ceci de particulier que sa gravité ne réside pas dans le mécanisme de sa survenance en lui-même (l'infiltration d'un virus ou d'un ver dans un réseau informatique), mais dans ses conséquences potentielles sur la vie de l'état et de la population (perturbation des systèmes de contrôle aérien aboutissant à des accidents, des réseaux hospitaliers conduisant à l'arrêt des appareils médicaux, du système de gestion d'un barrage hydraulique conduisant à l'ouverture intempestive des vannes et à l'inondation d'une zone habitée, neutralisation du réseau informatique par lequel s'opère la mobilisation ou l'approvisionnement des forces armées…).

Le cyberespace est devenu à la fois l'objet, le théâtre et un outil des conflits géopolitiques contemporains. Mais les États s'inquiètent surtout des défis posés à leurs pouvoirs régaliens, dans un contexte de très forte intrication des enjeux politiques, économiques et sécuritaires et de multiplicité des acteurs. Les États craignent en particulier pour leur capacité à assurer la sécurité de la nation et la défense du territoire, notamment en cas d'attaque contre des infrastructures vitales qui pourraient causer des pertes civiles. Le faible coût et la forte accessibilité de la technologie renforcent le pouvoir de petits acteurs, faisant émerger l'idée d'une menace asymétrique diffuse de type terroriste.

En dépit de leur usage dual, ces technologies ont désormais la capacité de perturber très sérieusement ou de détruire l'industrie, l'économie, les infrastructures sociales et de santé publique et l'administration d'un Etat, ainsi que la protection des informations sensibles du point de vue politique, militaire ou économique ; elles permettent donc d'atteindre des objectifs stratégiques, opérationnels et tactiques jusqu'ici à la portée d'opérations militaires.

VII. LA SOUVERAINETÉ DE LA RD CONGO A L'ÈRE DE LA CYBERCONFLICTUALITE : POUR QUELLE STRATÉGIE DE CYBERDÉFENSE CONGOLAISE ?

La République Démocratique du Congo a connu l'apogée des cyberattaques entre 2019 et 2021. Selon notre recherche, nous avons abouti à la conclusion que 31% des infrastructures de l'administration de l'Etat ou loge la souveraineté sont vulnérable et tourne sur des vieux systèmes d'exploitation qui ne jouissent pas des mesures de sécurités ; 40% des terminaux à usage privé sont infectés et 65% du système informatique tant pour les privés et pour l'administration public fait l'objet de plusieurs fuites des données numériques sans que les auteurs ne soient inquiétés[25].

Dans un autre registre, à l'issu des élections présidentielles de 2011 en RD Congo, un compte Twitter avait servi pour annoncer la mise hors service d'une dizaine de sites du gouvernement congolais. Se réclamant du groupe Anonymous, les pirates ont fait planter pendant des heures les sites du ministère du Budget (souveraineté économique), de la Direction générale des impôts, du ministère du Plan. Une action qui plut aux opposants au régime qui en ont en profités pour suggérer aux pirates d'autres cibles qui vont mettre la souveraineté de la RD Congo à rude épreuve. Dans le lot, outre les Banques implantées en RD Congo, on retrouve la base de données et le site web de la Commission électorale nationale indépendante qui fut l'objet d'une cyberattaque, or les élections sont les vecteurs d'expression de la souveraineté populaire d'un Etat.

Si dans certains secteurs d'activité (les banques, les télécoms), la cybersécurité est plus ou moins régulée, la grande majorité des activités, y compris les secteurs du service public, bien qu'ayant une visibilité sur le cyberespace dans certains cas, ne sont pas soumises à des règles de sécurité, même minimales. Ces dernières années, il s'est constaté une forte augmentation des menaces dues aux cyberattaques en République Démocratique du Congo, dans la sous-région et dans toute l'Afrique, des attaques réussies, aux conséquences parfois graves, ont montré que non seulement la fréquence et la complexité des cyberattaques augmentaient, mais encore que celles-ci étaient de plus en plus dirigées contre des États ou des entreprises.

La République Démocratique du Congo est la cible d'attaques informatiques qui portent atteinte à ses intérêts fondamentaux. Les infrastructures critiques sont définies comme l'ensemble des systèmes, actifs, installations ou réseaux qui fournissent des services essentiels au fonctionnement de l'économie et au bien-être de la population. Les

[25] http://www.legavox.fr, consulté le 07/04/2023 à 14h h 00'.

infrastructures critiques représentent la logistique vitale. Selon l'Union Internationale des Télécommunications (UIT), la faible préparation des pays africains à la transition numérique et aux menaces cyber (sabotage des infrastructures publiques, fraude digitale, espionnage et vol des stratégiques, vol de renseignement et intrusion militaire, etc.) aurait le potentiel de fragiliser les systèmes d'information et de nuire aux ambitions du continent d'être le premier marché mondial de l'économie numérique[26].

Les guerres actuelles (numériques) ont trouvé des nouveaux fronts, de ce fait, le cyberespace est ce nouveau théâtre ou les armes conventionnelles ont cédé la place aux nouvelles armes numériques (virus). Par conséquent, les explosions des armes conventionnelles sont désormais remplacé par des pannes informatiques qui peuvent paralyser tous les systèmes existence d'un Etat (aéronefs, électricité, santé, transport, industries, armées, police, etc). Une attaque cyber est symboliquement humiliante pour les Etats, quand l'armée peut constater que les avions ou les drones sont cloués au sol, l'Etat se retrouve défait sans combattre face à un individu qui peut rendre incompétente l'expression de la puissance d'un Etat et au passage sa souveraineté.

De par sa nature transversale, le numérique bouleverse tout particulièrement le concept classique de souveraineté de l'État en modifiant les conditions de son expression et en remettant en question sa légitimité. En effet, le numérique est un marché quasiment monopolisé par les géants numériques américains et les administrations et les organisations congolaises en dépendent fortement. Dans un tel contexte deux enjeux fondamentaux de souveraineté s'identifient. Premièrement les individus connectés qui produisent les données captées par des géants technologiques sans forcément un consentement préalable des utilisateurs. Dans ce premier cas, il relève de la prérogative régalienne de l'État de protéger les citoyens et leurs données personnelles. Deuxièmement, c'est la souveraineté de l'État elle-même qui est en jeu parce qu'agir à l'échelle nationale seulement ne peut constituer une solution efficace

Les données ne doivent plus seulement être comprises comme un sujet juridique et commercial, mais comme un enjeu géopolitique international à part entière. La maîtrise des données est depuis plus d'une décennie devenue un moyen de faire peser les rapports de force en sa faveur, dans un monde quasiment numérisé. Des États et des acteurs privés de l'internet interviennent dans la gouvernance des données. Pour les États c'est un enjeu de souveraineté et de sécurité des citoyens et pour ces géants du web c'est une opportunité de création de valeur à partir des données personnelles.

[26] http://www.presidence.cd/Stratégie nationale de cybersécurité de la République Démocratique du Congo, Commission nationale de la cybersécurité, Kinshasa, 2022.

VIII. POUR UNE CONSTRUCTION DE LA CYBERDÉFENSE

La cyberdéfense désigne l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels[27]. La cyberdéfense est un des moyens de protéger les ressources informatiques et numériques d'un Etat et contribue à la souveraineté numérique. La cyberdéfense constitue l'ensemble des activités que le ministère de la Défense conduit (actions militaires ou non militaires) pour garantir l'efficacité de l'action des forces armées et la réalisation de leurs missions. Elle regroupe la cyberdéfense active des systèmes d'information, la capacité de gestion de la crise cybernétique et enfin la capacité de lutte dans le cyberespace.[28]

La défense numérique n'est pas que militaire parce que mettant en œuvre par les institutions militaires et du renseignement. La cyberdéfense peut prendre plusieurs dimensions (juridique et politique), globalement elle est l'apanage des Etats. La cyberdéfense s'inscrit dans le cadre de la politique étrangère qui englobe les politiques de sécurité et de défense. Comprise comme une approche particulière de la conflictualité, la cyberdéfense est également dépendante des discours et des représentations technoscientifiques liées à la guerre et à la manière de la faire.

La politique de cyberdéfense remplit de nombreuses fonctions. Elle structure l'espace numérique et les jeux d'acteurs qui s'y développent, elle contribue à produire et organiser un corpus normatif, elle affirme une volonté politique et un projet collectif, elle vise à dissuader, le cas échéant, les comportements ou les projets susceptibles de s'y opposer… Il lui revient en particulier d'anticiper et de faire face aux « crises » susceptibles de se produire dans l'espace numérique. Toute politique de cyberdéfense se décline en une série de décisions et d'actions prises par des acteurs hétérogènes dans le domaine de l'espace numérique. La politique de cyberdéfense est donc faite d'activités spécifiques dans un champ complexe d'infrastructures, d'acteurs individuels et collectifs, de logiciels et de contenus. L'analyse de la cyberdéfense ne saurait être conduite sans commencer par une tentative de cartographie de l'espace numérique, tentative toujours délicate du fait de la complexité et de la turbulence qui le caractérisent.[29]

Une politique de cyberdéfense des États doit poursuivre une finalité qui consiste à garantir la souveraineté. La particularité de la politique de cyberdéfense tient à la diffraction de la notion et des acteurs qui entrent en jeu.

---

[27] https://www.ssi.gouv.fr/entreprise/glossaire/c/
[28] http://www.academiedegeopolitiquedeparis.com, consulté le 24/02/2023 à 15h 00.
[29] http://www. dunod.com, consulté le 25/05/2023 à 14h 40.

La cyberdéfense est contraignante pour tous les acteurs du cyberespace (Etats, Non-Etat, entreprise, individu)

La cyberdéfense impose d'abord de resituer l'espace numérique dans un contexte global. Il n'est pas possible aujourd'hui de dissocier de façon très nette les enjeux de défense de ceux de la sécurité. Une cyberattaque de grande ampleur sur des infrastructures nationales est tout aussi préoccupante pour un État que des menaces plus diffuses, comme celle de la propagande qui se joue sur les réseaux sociaux et qui peut, dans les cas les plus extrêmes, conduire à des actes criminels ou terroristes.[30]

VIII.1. Pour une stratégie nationale de la cyberdéfense congolaise

La République Démocratique du Congo n'a pas connu une longue période de paix depuis le génocide au Rwanda, doublé par l'avènement du cyberespace et ses menaces protéiformes sur la souveraineté. La numérisation a donné à la RD Congo et au reste du monde de grandes possibilités de développement et de progrès, mais ont également accru l'exposition à des facteurs qui affaiblissent la souveraineté.

Malgré des progrès incontestables accomplis depuis la mise en place des plusieurs instruments sur le numérique tels que le ministère du numérique, la loi sur le numérique, la commission nationale sur la cybersécurité et le plan national du numérique, la situation de la République Démocratique du Congo au regard de la menace résultant des attaques informatiques reste encore insatisfaisante. En dépit d'un réel effort de rattrapage, la RD Congo accuse encore un important retard concernant les moyens et les effectifs compétents dans la cybersécurité et la cyberdéfense, par rapport à ceux dont disposent les autres Etats comme le Rwanda, l'Angola, la Tanzanie.

Il se pause sérieusement un problème de compétente même des structures censées réguler la communication et la cybersécurité. Le cas de l'ARPTC qui se bute aux fournisseurs d'Internet et communication pour le paiement de la redevance plus 243 et autres griefs. Il persiste un flou sur la structure qui a l'autorité de la cybersécurité et de la cyberdéfense. L'action gouvernementale de la RD Congo ne dispose pas non plus des moyens nécessaires pour donner une plus large diffusion aux actions de sensibilisation, de formation ou de conseil, ni pour mener à l'échelle nationale les activités d'audit et d'inspection auprès des administrations ou des opérateurs d'importance vitale. Le constat sur l'absence d'une synergie entre acteurs publics et privés est flagrant, qu'il s'agisse des entreprises ou des opérateurs d'importance vitale, reste très insuffisante, alors qu'un partenariat étroit serait indispensable.

[30] http://www. dunod.com, *op. cit.*

La sécurité des systèmes d'information n'est pas toujours considérée comme une priorité par les différents ministères. Si certains ministères, comme le ministère de la défense, ont pris des mesures pour renforcer la protection de leurs systèmes d'information, beaucoup de ministères demeurent encore peu sensibilisés aux menaces liées aux attaques contre les systèmes d'information. Très peu de ministères en RD Congo disposent d'une véritable politique de cybersécurité et d'ailleurs très peu des ministères ont un service de cybersécurité ou un poste d'expert en la matière. Cette procrastination gouvernementale à l'ère de la cyberconflictualité est un risque majeur d'autant plus que les Etats qui excellent dans ce domaine sont en grande partie les Etats limitrophes. On en déduit que la RD Congo accuse un retard énorme sur le combat de la cybersécurité, de la cyberguerre et du cyberespionnage.

Les systèmes informatiques utilisés par les administrations présentent en réalité de nombreuses vulnérabilités. Or la vulnérabilité est la première brèche pour une cyberattaque. Jusqu'en plein 21e Siècle, la cybersécurité est perçue par les responsables ministériels et les utilisateurs comme une contrainte inutile et coûteuse. Elle n'est pas suffisamment prise en compte dans les projets informatiques des ministères, qui ont tendance à minorer l'importance de cette question et à ne pas prendre en considération les avis des responsables de la sécurité des systèmes d'information. De nombreux ministères ne connaissent même pas la cartographie de leurs propres réseaux et ignorent souvent la finalité de leurs propres systèmes d'information. Or, comment peut-on prétendre assurer une protection de ses systèmes informatiques, si l'on ne sait même pas localiser précisément l'un de ses ordinateurs qui a été infecté à la suite d'une attaque informatique ou si l'on ignore à quoi sert son serveur informatique ?

Le système d'information et de communication ont désormais un rôle central dans la dépendance de la RD Congo aux nouvelles technologies gage du développement. Ainsi, la cyberdéfense représente un enjeu de sécurité nationale. Faire de la cyberdéfense et de la protection des systèmes d'information est une priorité nationale, qui doit être porté au plus haut niveau de l'Etat.

La nouvelle stratégie de cyberdéfense vise à renforcer la résilience de la Défense congolaise en protégeant ses moyens et ses capacités contre les activités cybernétiques malveillantes. Cette stratégie se donne comme objectif le développement de capacités de cyberdéfense pouvant être utilisées dans un contexte national et international. Les menaces pour les intérêts vitaux de la RD Congo ne s'arrêtent pas à la frontière physique mais aussi numérique. Le cyberespace comme nerf du système international est vital pour les Etats, ainsi, la sécurité est essentiel pour le bon fonctionnement et pour la résilience de la dynamique nationale. L'objectif de notre stratégie est que la RD Congo dispose d'une des défenses les plus sûres en matière de cyberdéfense, et qu'il développe une expertise et des capacités. La stratégie se concentre sur quatre objectifs.

Au niveau national, il faut mettre en place une Direction de la cyberdéfense qui doit faire partir du Comité interministériel de coordination pour la prévention et la cybersécurité composé des ministères (Affaires étrangères, Défense, commerce extérieurs, Intérieur et sécurité). Cette stratégie permettra à la Défense congolaise de faire mûrir ses capacités, de contribuer davantage aux initiatives nationales de cybersécurité et de renforcer la résilience des infrastructures nationales. Les cyberattaques étant un phénomène international et transnational, la nouvelle stratégie doit intégrer les engagements de la RD Congo envers les organisations internationales, en veillant à ce que le pays assume sa part de responsabilité dans les efforts et les risques inhérents à la défense. La cyberdéfense de la RD Congo étant en construction a besoin de mûrir. Elle doit se faire une place dans les forces armées de la RD Congo tout en développant des capacités de base de la cyberdéfense.

Les objectifs stratégiques pour la mise en œuvre de cette stratégie couvrent donc un large éventail de facteurs :

1. Les ressources humaines

L'homme demeure la ressource centrale dans la construction de la cyberdéfense, ainsi, il faut une ressource humaine instruite à la cybernétique**.**

1.1. Personnel de défense bien informe et expérimenté

- Il faut impérativement établir et promouvra une formation interne en matière de cybersécurité et sensibiliser à l'importance d'intégrer la cybersécurité dans les processus existants au niveau du système éducatif.
- L'Etat enverra du personnel pour participer à des exercices et des formations nationaux et internationaux sur la cyberdéfense. Les aspects cybernétiques seront intégrés dans les exercices militaires et pris en compte dans les opérations militaires.

1.2. Mise en place et renforcement des principaux organes de cyberdéfense

La cyberdéfense exige un renforcement des capacités des structures et nécessite une grande ressource humaine, mais aussi la création des unités de cyber-réserve national.

2. Renforcement des compétences nationales non militaires/non liées à la défense en matière de cyberdéfense

2.1. Une cyber-coopération nationale et internationale forte

Le cyberespace n'a pas de frontière ainsi, la RD Congo doit s'efforcer au niveau national et international, de respecter l'ordre international fondé sur des règles, de remplir les engagements pris, entre autres, sous les auspices de l'Union Africaine et de l'Organisation des Nations Unies.

2.2. Identification des besoins et capacités mutuels et des facteurs favorables

Il faut plusieurs missions d'enquêtes sur les éventails des portails numériques de la RD Congo et leurs capacité de défense sectorielle mais aussi, établir le montage de l'industrie de la cyberdéfense et dresser le catalogue des portails numériques et identifier les besoins futurs. Ce qui aura aussi un impact sur les entreprises locales à maitriser le marché international de la cyberdéfense en vue de se construire un monopole dans la cyberdéfense.

2.3. Échange continu d'expertise et de ressources

La RD Congo doit participer au partage international de renseignements sur les menaces afin d'améliorer la connaissance de la situation avec et entre les Alliés et partenaires Africains et d'ailleurs.

3. Cyberdéfense intégrée dans l'ensemble des activités, des moyens et de la culture de la défense congolaise

3.1. La cybersécurité ancrée dans la culture organisationnelle

La Défense congolaise mettra en œuvre les meilleures pratiques et lignes directrices de l'industrie et des organisations internationales pour intégrer la cybersécurité dans la culture organisationnelle. La Défense congolaise introduira également une identité visuelle de cyberdéfense.

3.2. Gouvernance, mise en œuvre et exécution

Grâce à un cadre de gouvernance, de mise en œuvre et d'évaluation, l'Etat doit assurer l'intégration des meilleures pratiques en matière de cybersécurité par la mise en œuvre d'un Système de Management de la Sécurité de l'Information. En outre, la Défense congolaise doit mettre en œuvre des projets, des exercices d'entraînement et contribuer aux opérations dans le cyberespace. L'Armée congolaise doit chercher en permanence à améliorer la résilience du cyberespace, de son personnel, de ses infrastructures, de ses capacités et de ses systèmes.

IX. CONCLUSION

La globalisation transforme en profondeur les fondements mêmes du système international. La distribution de la puissance mondiale se modifie et les États se voient concurrencés, dans leurs stratégies, par de nouveaux acteurs puissants. La globalisation structure donc profondément l'évolution de la sécurité internationale. Elle constitue l'un des changements les plus importants intervenus depuis la fin de la guerre froide. L'actualité nous présente chaque jour des États incapables d'anticiper ou répondre à des cyberattaques. Cette incapacité Un tel événement porte atteinte à la souveraineté**.**

Véritable rupture en termes de technologie et d'emploi de la force, les cyberarmes ont bouleversé les modalités de la guerre sans en renouveler profondément les principes. Il se constate une multitude d'acteurs étatiques et non-étatiques, masqués ou non, organisations terroristes ou criminelles tels sont les risques du cyberespace. Une zone grise, un brouillard, dont les effets sont, eux, bien réels, parfois dévastateurs. Le combat dans le cyberespace est de nature asymétrique, hybride, parfois invisible et en apparence indolore. Pourtant, l'emploi des cyberarmes sont susceptible de porter gravement atteinte aux capacités et aux intérêts souverains des États.

Dans la cyberguerre militaire, il existe des implications physiques et technologiques. Les systèmes électroniques sont, la plupart du temps, compromis suite à l'identification et l'exploitation de vulnérabilités humaines ; cette démarche leur permet d'accéder aux systèmes physiques eux-mêmes. Le monde civil est différent, bien que plus large, un ennemi puisse frapper sa cible sans jamais quitter son bureau. Les futures guerres seront incomparables par rapport aux conflits passés. Les différentes nations sont aujourd'hui soumises à une course aux armements qui se dirige vers des machines autonomes régies par une intelligence artificielle tout en ayant des programmes susceptibles de détruire des infrastructures à l'aide d'une seule ligne de code.

La cyberdéfense est un enjeu majeur dans le monde d'aujourd'hui, et la République Démocratique du Congo ne fait pas exception. En tant que pays en développement, il est crucial pour la RDC de prendre des mesures afin de garantir sa souveraineté numérique et de tirer pleinement parti des avantages offerts par les technologies de l'information et de la communication. Dans le contexte spécifique de la RDC, plusieurs défis doivent être relevés pour assurer une véritable cyberdéfense. Tout d'abord, il est essentiel d'améliorer l'accès à Internet dans tout le pays afin que tous les citoyens puissent bénéficier des opportunités qu'il offre. Cela nécessite des investissements importants dans l'infrastructure réseau ainsi que dans la formation aux compétences digitales. Ensuite, il faut mettre en place une législation solide pour encadrer l'utilisation des technologies digitales et protéger les droits fondamentaux tels que la vie privée et la liberté d'expression en ligne. La création d'une agence nationale chargée de superviser ces questions pourrait jouer un rôle clé dans ce domaine.

BIBLIOGRAPHIE

I. Ouvrages

- BODIN Jean., *Les six livres de la république*, Jacques du Puys, Paris, 1583.
- CARRÉ DE MALBERG R., *Contribution à la théorie générale de l'État spécialement d'après les données fournies par le droit constitutionnel français,* Librairie du Recueil Sirey, Paris, 1920.
- David SANGER, *Confront and Conceal. Obama's SecretWar and Surprising Use of American Power*, Broadway Books, New York, 2012.
- DUGUIT Léon, *Traité de droit constitutionnel* – Tome deuxième : La théorie générale de l'État – Première partie : *Éléments, fonctions et organes de l'État*, 3e éd., De Boccard, 1928.
- KRASNER Stephen., *Sovereignty : organized Hypocrisy*, Princetown University Press, Princetown, 1999.
- MURAWIEC. Laurent., *Effets spéciaux: la Guerre au XXIe siècle*, Odile Jacob, Paris, 2000.
- REY. Alain., *Dictionnaire historique de la langue française*, Le Robert, Paris, 1992.
- KEOHANE R.O. et MILNER H.V., *Internationalization and Domestic Politics,* Cambridge University Press, Cambridge, 1996.
- ROSENAU J.N., *Turbulence in World Politics: a Theory of Change and Continuity,* Princetown University Press, Princetown, 1990.
- ROSENAU J.N., *Along the Domestic-Foreign Frontier. Exploring Governance in a Tribulent World*, Cambridge University Press, Cambridge, 1997.

II. Revues et articles

- BERNS.T., « Souveraineté, droit et gouvernementalité », Arch. phil. Droit 2002.
- BOCKEL.J-M., « La cyberdéfense : un enjeu mondial, une priorité nationale ». Commission des affaires étrangère, de la défense et des forces armées du Senat, Paris, 2012.
- BOYER.B., « La cyberguerre ou le mythe du blitzkrieg numérique », Géopolitique de l'information, Les grands dossiers n°2, Diplomatie, 2011.
- DE SMET.F., « Le mythe de la souveraineté – Du corps au contrat social », EME, coll. Politique & culture, 2014.
- DOUZET. Frederick. et Géry. Aude., « Le cyberespace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace », dans Hérodote, Éditions La Découverte, Paris, 2020, N° 177-178.
- Kaiser R., "The Birth of Cyber War", Political Geography, vol. 46, 11-20, 2015.
- LIBICKI. Martin, "Cyberspace is Not a Warfighting Domain", I/S: A Journal of Law and Policy for the Information Society, vol. 8, n°2, 2012.

- RID. Thomas, "Cyber War Will Not Take Place", Journal of Strategic Studies, 2012.
- DOSSE Stéphane et KEMPF. Olivier., "Stratégie dans le cyberspace", Esprit du Livre, 2011
- MULUMBATI N., « Manuel de sociologie générale, collection savoir et connaitre », Africa, Lubumbashi, 2001.
- HOFFMAN Stanley, "International Systems and International Law", World Politics, XIV, octobre 1961.

III. Autres documents

- BOLA N., *Science administrative*, cours inédit, G1, RI, FSSAP, ULK, Kinshasa, 2011-2012.
- Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, nov. 2011.
- Rand Corporation, « Operationalizing Cyberspace as a military domain », juin 2019.
- Stratégie nationale de cybersécurité de la République Démocratique du Congo, Commission nationale de la cybersécurité, Kinshasa, 2022.
- TAILLAT Stéphane., *Cyberguerre - Cyberpaix et la conflictualité*, Séminaire du Collège des Bernardins, Chaire des Bernardins, Paris, 2016.

IV. Webographie

- https://www.ssi.gouv.fr/entreprise/glossaire/c/, consulté le 20/03/2024
- http://www.oai.cairn.info, consulté le 23/02/2023 à 15h 10'
- http://www.frstrategie.org, consulté le 04 /07/2023 à 13h 55'
- http://www.legavox.fr, consulté le 07/04/2023 à 14h h 00'
- http://www.presidence.cd
- http://www.academiedegeopolitiquedeparis.com, consulté le 24/02/2023 à 15h 00'
- http://www. dunod.com, consulté le 25/05/2023 à 14h 40'