Les répercussions du cyberterrorisme sur la paix et la sécurité internationales

Dr. Yasmine Abdel Moneim

Résumé

Le cyberespace est un nouveau lieu d'échanges et d'affrontements entre les différents acteurs de la société internationale qui témoigna un recul de la souveraineté étatique. Menacé par plusieurs risques transnationaux, il est devenu actuellement au centre des intérêts des chercheurs et des responsables politiques et militaires puisqu'il est lié à la sécurité nationale des États et a ainsi des répercussions sur la paix et la sécurité internationales.

Le cyberterrorisme, étant un de ces risques alarmants, fait partie des « *attaques asymétriques* » où la partie faible militairement peut bénéficier de la baisse des coûts des attaques cybernétiques en vue de réaliser des objectifs idéologiques et politiques au lieu de mener une guerre conventionnelle. Les avantages qu'offre le cyberterrorisme par rapport au terrorisme classique ont permis de mener des attaques à distance sans aucune nécessité d'intervention physique sur le territoire d'un autre État, et représentant ainsi une atteinte à sa souveraineté territoriale. Les cyberterroristes peuvent bénéficier également de l'anonymat et de l'impré visibilité des attaques ainsi que de l'absence de règles juridiques internationales qui peuvent être appliquées vis-à-vis de ces attaques terroristes.

Bien que le cyberterrorisme reste une menace potentielle et éventuelle, une collaboration à l'échelle mondiale de la part des organisations internationales, ainsi qu'une coopération entre les systèmes juridiques nationaux sont essentielles pour garantir la paix et la sécurité internationales.

The impacts of Cyberterrorism on international peace and security

Summary

The cyberspace is a new space of exchanges and conflicts between the various actors of international society that attests a decline in state sovereignty. Threatened by several transnational risks, the cyberspace has currently become a centre of interests for researchers, political and military leaders as it affects the national security of states and thus has implications for international peace and security.

yberterrorism, being one of the alarming risks posed in cyberspace, is part of "*asymmetric attacks*" where the weaker military party can benefit from the low cost of cyberattacks to achieve political and ideological goals instead of conducting a conventional war. The advantages that offers the cyberterrorism compared by the conventional (classical) terrorism have allowed remote attacks without any need for physical intervention on the territory of another state and thus risks violating its territorial sovereignty. The cyberterrorists can also benefit from the anonymity and unpredictability of attacks as well as the absence of

international legal rules that can be applied to these attacks.

Since cyberterrorism remains a potential and significant global threat, it requires a global collaboration from international organisations as well as cooperation between national legal systems to maintain international peace and security.

Les répercussions du cyberterrorisme sur la paix Et la sécurité internationales

Introduction

1 - La conceptualisation du cyberterrorisme

A - Définition du cyberterrorisme

1 - Le terrorisme

2 - Le cyberespace

3 - Le cyberterrorisme

B - Les autres concepts qui sont en relation

1 - Cyberattaques

2 - Cybercriminalité

3 - Cyberguerre (Cyberwarfare)

4 - L'hacktivisme

5 - Cyberespionnage

II - Le changement du rapport de force sur la scène internationale

A - L'apparition de nouveaux acteurs non étatiques

B - La force électronique (Soft power) via la force militaire

III - Les impacts de la détention de la force électronique

A - Apparition des Cyberarmes et la course aux armements

B - Les stratégies de cyberdéfense relatives à la lutte contre le cyberterrorisme

IV - La recherche de la paix dans le cyberespace

A - Rôle du droit international

B - Réaction des États

Conclusion

Introduction

La paix et la sécurité internationales ont été considérées pour longtemps comme étant deux piliers primordiaux pour la stabilité de la société internationale et une garantie pour son développement et sa prospérité. Or, ces deux piliers ont été menacés à maintes reprisesà cause des conflits internationaux ou des conflits internes. Ces menaces fréquentes ont exigé une action internationale unifiée de la part de différents acteurs internationaux, et notamment les organisations internationales, plus précisément les Nations Unies.

Pourtant, la « révolution technologique »[1] et particulièrement la «révolution numérique »qui a touché le monde entier, ainsi que la mondialisation ont conduit à un changement radical dans les types de menaces traditionnelles visant la société internationale et affectant profondément la paix et la sécurité internationales. Un bon nombre de ces menaces est lié au

---

(1) Elle est perçue comme étant la troisième révolution industrielle.

cyberes pacesous le nom des « cybermenaces ». Même si la plupart de ces cybermenaces ne sont pas nouvelles, car elles existaient déjà dans les autres espaces (terre, mer, air), sauf qu'elles disposent de nouvelles dimensions les rendant particulières. Ces menaces se voient disperser dans le cyberespace de manière plus simple et plus rapide en raison de la spécificité de ce milieu et des avantages qu'ils présentent comme l'anonymat et l'imprévisibilité des attaques, la limitation de la souveraineté étatique dans le cyberespace, ainsi que l'absence de règles juridiques internationales qui peuvent être appliquées vis-à-vis de ces attaques. Le faible coût[1] de ces cybermenaces fait qu'ellesne sont plus commises uniquement par des acteurs étatiques classiques, mais de nouveaux acteurs apparaissent sur la scène internationale, menant à un bouleversement profonddans les rapports de force existants.

Notre préoccupation dans cette étude portera particulièrement sur une des menaces de plus en plus alarmante sur la scène internationale qui est le phénomène du cyberterrorisme. Cette menace qui

---

(1) Les moyens à utiliser pour mener des attaques cybernétiques sont relativement moins coûteux, un ordinateur et une connexion internet suffisent et ils sont beaucoup moins chers que des armes ou des explosifs.

dépend, non plus de la force militaire traditionnelle, mais de la force électronique « *Soft power* » [1], utilise les différentes formes technologiques pour influencer et séduire ses futurs militants tout en s'appuyant sur des moyens idéologiques, culturels ou religieux. Les cyberterroristes peuvent utiliser le cyberespace soit pour mener directement des cyberattaques terroristes ou pour conduire des actes terroristes classiques sur le terrain via Internet.

Notre problématique se focalise sur la question des répercussions du cyberterrorismesur la paix et la sécurité internationales. Cette question est liée au fait que le cyberterrorisme va permettre aux acteurs non étatiques de détenir une force asymétrique qui leur aide àmener de nouveaux types d'attaques. Ce changement a conduit à une modification radicale, vu mêmeune révolution, dans les relations internationales.

---

[1] Ce concept fut sa première apparition avec Joseph Nye en 1990 dans son livre « Bound to Lead » (Le leadership américain). Il définit le « soft power » comme étant la capacité ou la puissance d'influencer le comportement d'un autre État par la séduction plutôt que par la coercition ou la force. Joseph Nye,*Bound to Lead: The Changing Nature of American Power*, New York, Basic Books, 1990. Ce concept a été développé par l'auteur en 2004 pour décrire le cas où le soft power est utilisé pour permettre à un État d'obtenir ce qu'il veut sans force "Co-opt people ratherthancoercethem". Joseph Nye, *Soft Power: The Means to Success in World Politics*, New York , Public Affairs, 2004, p. 5.

Pour mieux comprendre cette problématique, il est évident d'aborder en premier lieu la conceptualisation du cyberterrorisme en étant un des types du terrorisme classique qui a entrainé par conséquentun changement dans les rapports de force sur la scène internationale. En deuxième lieu, on examinera les impacts de la détention de la force électronique. Enfin, il sera pertinent de connaîtrele rôle du droit international et des États dans la recherche de la paix dans le cyberespace.

1 - La conceptualisation du Cyberterrorisme

Il - faut bien admettre que le monde virtuel n'est que la réflexion du monde réel, et que la plupart des dangers et des menaces qui perturbent le monde réel se trouve aussi dans le monde virtuel, presque de la même ampleur. Cela veut dire que le fait de se trouver devant un phénomène du cyberterrorisme est à vrai dire, le résultat du développement du phénomène du terrorisme en général.

Le cyberterrorisme est un terme récent qui cause beaucoup de polémique pour plusieurs raisons. Déjà, il n'existe pas une définition consensuelle pour le phénomène du terrorisme classique et par conséquent la conceptualisation du cyberterrorisme est presque difficile. En plus, ce phénomène engendre une certaine

confusion avec les autres attaques qui arrivent au cyberespace. Des auteurs considèrent même le cyberterrorisme avec ses attaques terroristes dans le cyberespace comme étant à la fois, une catégorie du Cybercrime et de terrorisme[910], en plus d'être un mauvais usage des technologies del'information. Il est donc important de définir premièrement le conceptdu cyberterrorismepuis expliquer la distinction avec les autres termes qui y sont liées.

A - Définition du cyberterrorisme

Le concept du cyberterrorisme est né de la convergence entre le terrorisme classique et le cyberespace. Une compréhension du phénomène du terrorisme en premier lieu est essentielle avant de l'intégrer à la technologie et à l'informatique dans le cyberespace.

1 - Le terrorisme

Le concept u terrorisme a été développé de manière exceptionnelle et contradictoire depuis son apparition et

---

(1) Stein Schjolberg, «*Terrorism in Cyberspace – Myth or reality?* », article présenté au NATO Advanced Research Workshop on Cyberterrorism, Bulgaria, Sofia (October 2006), et au International Criminal Law Network (ICLN), 4th Annual Conference: Effective Counter-Terrorism and the Rule of International Law, The Hague, The Netherlands, December 2005, p. 2.

jusqu'à nos jours car le concept est équivoquepuisqu'il *« désigne en même temps une technique de combat, un type d'action politique violente, et porte un jugement moral »*[(1)]. Loin d'avoir un consensus universel sur une définition du terrorisme, ce concept a été lié aux développements politiques et idéologiques des différentes sociétés.En plus, d'autres actes de violence dans des domaines variés ont emprunté ce concept comme c'est le cas dans le cyberterrorisme, l'Eco-terrorisme, le bio-terrorisme...

Bien que le phénomène du terrorismeexiste depuis la création des sociétés, le concept du terrorisme lui-même est apparu pour la première foisde manière significative durant la révolution française[(2)] pour désigner la terreur Robespierristeen 1793-1794[(3)]. En ce temps, la terreur a été conçue comme un moyen de violence utilisé pour atteindre un objectif politique à

---

(1) Jean-François Gayraud et David Sénat, *Le terrorisme*, coll. Que Sais-Je ?, Paris, Presses Universitaires de France (PUF), 2002, p. 22.

(2) Il est dit même que la première république française est née par la terreur. C'est ainsi que Robespierre et ses partisans (les Montagnards) ont établi un régime de dictature caractérisé par la terreur pour, selon eux, protéger les principes de liberté. Ils étaient considérés comme des terroristes car ils ont eu recours à la violence pour atteindre leurs objectifs politiques.

(3) Marc Jacquemain, « *Terrorisme, terroriste* », no. 63, Printemps 2007, Quaderni, Nouveaux mots du pouvoir : fragments d'un abécédaire, p. 89. Doi : 10.3406/quad.2007.1794.

travers la résistance et l'émeute (viades attentats, de meurtres ou d'assassinats ...). Il était en relation avec la terreur révolutionnairequi « *a voulu fonder de nouvelles valeurs en ouvrant un cycle de vengeance publique* »[(1)].

Après la révolution, le terme du terrorisme est apparu en 1795 dans un œuvre du philosophe Emmanuel Kant intitulé « *Projet de paix perpétuelle* »dont il a essayé dedéfinir la terreur en étant « *celle qu'exerce l'obstination du pouvoir existant à maintenir sa contrainte, son refus de droit, son acharnement à réduire l'homme aux seules dispositions égoïstes, sa volonté de lui interdire tout progrès* »[920].

Plus tard, le Dictionnaire de l'Académie française définit le terrorisme comme « *un régime de terreur politique, c'est-à-dire qui use d'une rigueur impitoyable et inspire une grande crainte* »[(3)]. À cette époque, le terrorisme était alors conçu comme un mode d'exercice du pouvoir et pas un moyen de contestation ou d'opposition.

---

(1) Sophie Wahnich, « *Terreur Révolutionnaire et terrorisme. Rémanence rétinienne et troubles de la vision* », *Lignes*, vol. 2, n° 8, 2002, p. 165. DOI 10.3917/lignes1.008.0147.

(2) Emmanuel Kant, *Projet de paix perpétuelle*, traduit par Karin Rizet, coll. Mille et Une Nuits, n° 327, Paris, 2001.

(3) Dictionnaire de l'Académie française, supplément, an VII, 1798, p. 775. Cité par Marie-Hélène Gozzi, *Le terrorisme*, Paris, Ellipses, 2003, p. 8.

Depuis ce temps, le phénomène du terrorisme n'a cessé de se développer de manières différentes, et notamment durant le XXe siècle en fonction du changement des intérêts politiques et idéologiques. Il a été connu comme acte d'agression contre un Étaten lui causant la terreur et l'instabilité par des groupes terroristes. De ce fait, le terrorisme sort du cadre précis de la guerre conventionnelle et suscite un débat international autour de sa définition. La doctrine et la pratique internationales témoignent une divergence entre les multiples tentatives de définition. Or, plusieurs approches du terrorisme sont souvent avancées.

Il y a une approche qui voit que le terrorisme vise en premier lieu et exclusivement la propagation de la terreuret des effets psychologiques négatifs. Il consiste à « *tuer délibérément des innocents pris au hasardafin de semer la crainte dans une population et de forcer la main à ses dirigeants politiques* »[1]. De cela, une « *action violente est dénommée terroriste lorsque ses effets psychologiques sont hors de proportion avec ses résultats purement physiques* »[2].

---

(1) Michael Waltzer, *De la Guerre et du Terrorisme*, Paris, Bayard, 2004, p. 35.

(2) Raymond Aron, *Paix et guerre entre les nations*, Paris, Calmann-Lévy, 1962, p. 176.

Une seconde approche avance une définition axée sur les buts politiques du terrorisme qui vise avant tout, pas la propagation de la terreur,mais la réalisation d'une finalité politiqueà travers des actes terroristes puisqu'il est « *l'usage ou la menace de l'usage de la force dans le but de provoquer des changements politiques* »[1].

Quant à la troisième approche[2], elle soutient une idée mixte du terrorismequi, selon elle, vise à la fois la réalisation d'un but politique (finalité politique) à travers la propagation de la terreur[3] (effets psychologiques). L'acte terroriste est qualifié comme un

---

(1) Brian Jenkins, *International Terrorism : A New Kind of Warfare*, Santa Monica, Rand Corporation, 1974, p. 37.

(2) Selon cette approche, le terrorisme est « *la création délibérée de la peur, ou son exploitation, par la violence ou la menace de violence, dans le but d'obtenir un changement politique. Il est spécifiquement destiné à produire des effets psychologiques qui touchent un cercle plus large* ». Bruce Hoffman, *Inside Terrorism*, New York, Columbia University Press, 2006, pp 40, 41.

(3) Alex Schmid et Albert Jongman, *PoliticalTerrorism : A new guide to actors, authors, concepts, data bases, theories, and literature*, London, Transaction Publishers, 2005. Ces deux auteurs néerlandais ont mené une étude sur le terrorisme et ont analysé presque 109 définitions du concept de sources variées avant d'arriver à leur définition. Selon eux, le terrorisme est « *une méthode répétée d'action violente inspirant l'anxiété, la peur, et qui est employée par des individus, des groupes, (semi-) clandestins ou des acteurs étatiques pour des raisons particulières, criminelles, ou politiques où - au contraire de l'assassinat - la cible initiale de l'acte de violence ne représente que la secondaire et non la cible principale. La cible initiale de l'acte de violence est généralement choisie au hasard (opportunité) ou de manière sélective (symbolisme) parmi une population donnée et sert à propager un message* ».

acte politique qui viseà « *déstabiliser un gouvernement ou un appareil politique, où les effets psychologiques recherchés sont inversement proportionnels aux moyens physiques employés et dont la cible principale, mais non exclusive, est la population civile* »[1].

En ce temps, les Nations Unies, dans un rapport de son secrétaire général, ont essayé de mettre en place une définition du terrorisme en étant tout acte, outre ceux déjà visés par les conventions en vigueur, commis dans l'intention de causer la mort ou des blessures graves à des civils ou à des non combattants, dans le dessein d'intimider une population ou de contraindre un gouvernement ou une organisation internationale à accomplir un acte ou à s'abstenir de le faire[2].

Cependant, cette définition est limitée et ne couvre pas toutes les situations qui peuvent être qualifiées de terrorisme.

Avec le développement de la technologie et l'apparition de nouveaux types d'armes, le concept du terrorisme a connu beaucoup de changements dans sa

---

(1) Arnaud Blin, *L'histoire du terrorisme de l'antiquité à Al-Qaïda*, Paris, Bayard, 2006, p. 82.

(2) Rapport du secrétaire général des Nations unies *« pour une liberté plus grande : développement, sécurité et respect des droits pour tous »*, Doc off AG NU, 59e sess, Doc NU A/59 (2005).

perception, ainsi que des variations liéesaux fins politiques, idéologiques, religieux, ou culturels des groups qui le définissent, sans nier le fait qu'il menace la paix et la sécurité internationales[1]. Les attentats du 11 septembre 2001 ont constitué un point marquant dans l'histoire internationale et surtout dans le changement inattendu des techniques et de stratégies du phénomène du « terrorisme ».Cela a conduit à une certaine confusion en ce qui concerne la qualification de certains actes et quels liens présentent-t-ils avec le terrorisme. Par exemple, quel est le trait qui distingue les mouvements de libération, actes de résistance,guérilla, crimes politiques, le nationalisme ou même les manifestations duphénomène duterrorisme ? La plupart de ces actes sont aussiaccompagnés d'un certain degré de terreur et de violence. En plus, d'autres questions surgissent comme celle de la légitimité de l'acte (violence légitime contre violence illégitime) et qui décide de telle légitimité ?[2]

---

(1) Le conseil de sécurité a affirmé que « *les actes de terrorisme international constituent l'une des menaces les plus graves à la paix et à la sécurité internationales au 21ème siècle* ». Rés. CS 1377, Doc. off CS NU, 2001, 4413e séance, Doc. NU S/RES/1377.

(2) Est-ce que les bombardements atomiques de Hiroshima et Nagasaki ont été tolérés (légitimes), tandis que les actes du 11 septembre sont considérés comme du terrorisme ?

À mon avis, la référence au « terrorisme » a été différemment perçue selon les intérêts[1] et le contexte politique et stratégique ainsi que les rapports de force en jeu. La qualification des groupes et leurs actes était relative. Le fait de désigner un acte de violence comme du « terrorisme » est lié, dans la plupart des cas, à la volonté politique du régime ou du pouvoir politique en place qui dépend deses intérêts ou des buts qu'il veut réaliser. Dans ce sens, il va désigner du « terrorisme » les actes commis par des groupes contre lesquels il éprouve un mécontentement ou un désaccord, et il va les percevoir comme « actes de violence » une fois que ces actes proviennent des groupesavec lesquels il maintient de bonne relation[2]. La question de la désignation est donc purement politique[1].

---

[1] Le mouvement Al Qaeda fut créé et financé par les États-Unis durant la première guerre d'Afghanistan pour lutter contre l'invasion soviétique. Après la fin de la guerre, le mouvement a décidé de poursuivre le djihâd contre l'occident et a changé radicalement sa stratégie. Depuis, l'occident, et surtout les États-Unis, le considère comme un groupe terroriste une fois que les intérêts entre eux ont changé.

[2] Cela veut dire que les personnes ou les groupes qui commettent des actes de violences sont combattants et terroristes en même temps, « one man's terroristisanother man's freedomfighter ». Par conséquent, un régime va considérer ses opposants comme des terroristes dès qu'ils s'opposent ouvertement et sévèrement à ses politiques. Les exemples sont beaucoup, les attentats du 11 septembre, les combattants tchétchènes, qui étaient considérés à la fois comme des terroristes (vis-à-vis du gouvernement de Moscou) et des résistants (selon la communauté internationale), les fusillades répétées dans les écoles américaines, les actes palestiniens contre l'occupation

En conclusion, « *l'appréhension de la notion de terrorisme pose problème, elle est tellement chargée des valeurs négatives que son usagemême entre dans l'affrontement des propagandes politiques* »[2].

2 - Le cyberespace

Le cyberespace est apparu au début dans le domaine militaire avant d'être largement exploité et utilisé dans le domaine civil dans plusieurs activités surtout les activités commerciales. Cet espace se base essentiellement sur des différents outils technologiques[3]. Il est devenu à la fois en peu de temps, un véritable espace d'échanges et d'affrontements entre plusieurs acteurs.

Malgré l'importance du cyberespace, aucune définition normative et consensuelle n'a été avancée dans un texte juridique international[4]. Cela peut être

---

israélienne ou la guerre en Irak, la tentative d'assassinat du Jean Paul II ou l'assassinat de Rafic Hariri (l'ex-premier ministre libanais).

(1) Dans ce cas, « *l'agresseur n'est pas défini par son action mais par sa désignation comme tel par ses opposants* ». Olivier Kempf, *Le cyberterrorisme : un discours plus qu'une réalité*, Hérodote, vol. 1, n° 152-153, 2014, p. 84. DOI 10.3917/her.152.0082.

(2) Christian Mellon, *Éthique et violence des armes*, Paris, Assas Éditions, 1995, p. 25.

(3) L'internet est considéré comme un des outils les plus utilisés dans le cyberespace, bien qu'il ne soit pas le seul. D'autres formes de technologies constituent l'ensemble du cyberespace.

(4) Le terme « Cyberespace » est apparu pour la première fois en 1984 dans un roman de science-fiction « *Neuromancer* » de William Gibson.

liée au fait que le cyberespace est un nouvelespace difficile de le cartographier, de l'appréhender ou de le délimiter en raison de sa déterritorisation.

Face à une multiple tentative de définition, on remarque que l'idée de ne s'intéresser qu'à la virtualité du cyberespace conduit à une compréhension erronée de cet espace. En fait, le cyberespace est composé de trois couches interdépendantes : la première couche est physique et elle contient les infrastructures techniques des réseaux (les matériels et les câbles installés sur le territoire de l'État)[1]. La deuxième couche englobe l'infrastructure logique qui est les logiciels et les protocoles de données qui assurent la transmission des informations. Cette couche est normalement la cible des attaques informatiques. Quant à la troisième couche

---

Il a décrit le cyberespace comme étant « *une hallucinationconsensuelle vécue quotidiennement en toute légalité par des dizaines de millions d'opérateurs, dans tous les pays, par des gosses auxquels on enseigne les concepts des mathématiques... Une représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain. Une complexité impensable. Des traits de lumières disposés dans le non-espace de l'esprit, des amas et des constellations de données. Comme les lumières de villes, dans le lointain* ». William Gibson, *Neuromancien*, 2e éd, traduit par Jean Bonnefoy,coll SF, Paris, « J'ai lu », 1988, p. 64. (Édition américaine : *Neuromancer*, 1984).

(1) Cette couche « *est soumise aux contraintes de la géographie physique et politique* ». Frédérick Douzet, « *La géopolitique pour comprendre le cyberespace* », Hérodote, La Découverte, vol. 1, n° 152-153, 2e trimestre 2014, p. 6. DOI : 10.3917/her.152.0003. Cette couche fait l'objet de beaucoup de mesures de sécurité pour lui assurer une protection de haut niveau.

cognitive, elle relève des programmes et des applications. Les trois couches sont liées, l'attaque que subit la couche logique influe sur les deux autres.

En conséquence, le cyberespace est un espace étroit et immense d'interactions virtuelles, possédant de grandes potentialités. D'où viendra la difficulté de contourner ses frontières et de le gérer dans sa globalité. Cette difficulté mène à une remise en cause de l'autorité des États[1] et à un recul de sa souveraineté qui freine ses capacités de coercition en présence des acteurs difficiles de les désigner. La croissance des tensions entre les différents pays a conduit au transfert des conflits politiques, économiques et militaires des champs de bataille classique au cyberespace.

3 - Le cyberterrorisme

Le phénomène du cyberterrorisme se caractérisepar la rencontre entre le terrorisme traditionnel et l'utilisation de la technologie d'informations et de communication (TIC) dans le cyberespace. Il est une forme développée du terrorisme classique. On pourra dire que l'apparition réelle du concept du cyberterrorisme a été introduite en1996 par

---

[1] Pour plus d'informations sur la question du rôle de l'État dans la règlementation du cyberespace, voir : Cyril Rojinsky, «*Cyberespace et nouvelles régulations technologiques* », Dalloz Chron., 2001, pp. 844-852.

Barry Collin qui la définit comme étant la « *convergence du monde physique et du monde virtuel* »[1]. Il est « *le pendant des actes de terrorisme classique, mais dans le cyberespace* »[2].

Cependant, jusqu'à nos jours, il n'existe pas une définition consensuelle du phénomène du cyberte rrorisme. Certains auteurs[3] optent pour une définition axée sur le commettant(l'auteur) des actes :les cyberte rroristes. Et donc, le cyberterrorisme est tout acte mené dans le cyberespace par des terroristes. Or, cette définition est limitée et ne reflète pas clairement la vérité du phénomène.

Pour cette raison, d'autres auteurs préfèrent se baser principalement sur le lieu ou l'espace où se passent les cyberattaques terroristes :le cyberespace. Selon eux, le cyberterrorisme est tout acte terroriste qui se passe

---

(1) Barry Collin, « *The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge*», *11th Annual International Symposium on Criminal Justice Issues*. Barry Collins, « *The Future of Cyberterrorism*», Crime and Justice International, vol. 13, n° 2, March 1996, pp. 15-18.

(2) Pour cette définition, voir: Franklin D. Kramer, Stuart H. Starr et Larry K. Wentz, *Cyberpower and national security,* 1st ed., Washington D.C., National Defense University Press: Potomac Books, 2009.

(3) Encesujet, voir: Steven Furnell et Matthew Warren, « *Computer Hacking and Cyber terrorism: the Real Threats in the New Millennium?* », Computers and Security, vol. 18, n° 1, 1991, pp. 30- 32; Maura Conway, «*Terrorist "use" of the Internet and Fighting Back*», Information and Security: An International Journal, vol. 19, 2006, pp. 9-30.

au/ou à travers le cyberespace[1]. Cette définition, ayant basée uniquement sur le lieu des attaques, néglige ou confond entre les différentes formes des cyberattaques (cybercriminalité, cyberespionnage, cyberguerre.....) puisqu'elles arrivent toutes au cyberespace.

Pour essayer d'adopter une définition qui encadre ce phénomène, le cyberterrorisme peut être défini comme Une attaque informatique ou menace d'attaque informatique entrainant d'importants dégâts conduite par des acteurs nonétatiques contre des systèmes d'information pour intimider ou contraindre des gouvernements ou sociétésdans le cadred'objectifs d'ordre politique ou sociaux[2].

De ce sens, le cyberterrorisme peut être vu comme « *une attaque préméditée etpolitique motivée contre les systèmes d'information, programmes informatiques et données par des sous-groupes nationaux ou agent*

---

(1) Olivier Kempf, *Supra* note 22, p. 83.

(2) Encesens, Dorothy Denning, *A view of Cyberterrorism Five Year Later*, Readings in Internet Security: Hacking, counterhacking, and Society (K. Himma ed.), Boston, Jones and Bartlett Publishers, 2006. Cité par, Alix Desforges, «*Cyberterrorisme : quel périmètre ?* » IRESM, no. 11, décembre 2011, p. 5. "*Cyberterrorism is generally understood to refer to highly damaging computer-based attacks or threats of attack by non-state actors against information systems when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social*".

clandestin de laquelle résulte des actes de violence contre des cibles non combattantes»[1]. Il peut être considéré comme une « *activité criminelle qui s'applique à une pluralité d'actions et à des objectifs multiples* »[2].

Un rapport du Conseil de l'Europe[3], daté du 8 juin 2015, a résumé la situation en affirmant que le cyberterrorisme comporte deux éléments : un élément objectif qui est la « *perpétration d'une infraction informatique* » et un élément subjectif relatif aux « *motivations et intentions de l'auteur*». L'absence de l'élément subjectif fait que l'acte commis ne peut être qualifié du cyberterrorisme mais il sera simplement une « *atteinte à la législation contre la cybercriminalité* ».

Le fait donc de qualifier certains genres de perturbations ou de menaces informatiques dans le cyberespace comme terrorisme a été critiqué par plusieurs auteurs. Ils les considèrent comme des cyberattaques et nient donc leur relation avec le terrorisme en raison de l'absence des pertes humaines

---

(1) Mark Pollitt, «*Cyberterrorism: Fact or Fancy?* », Computer Fraud and Security, no. 2, 1998, pp. 8-10.

(2) Marie Stella, « *La menace déterritorialisée et désétatisée : le cyberconflit* », Revue internationale et stratégique, vol. 1, n° 49, 2003, p. 169. DOI 10.3917/ris.049.0165.

(3) Hans Franken, *Renforcer la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur Internet*, Conseil de l'Europe, Rapport de la commission de la culture, de la science, de l'éducation et des médias, Doc. 13802, 8 juin 2015, p. 7.

considérables ou de leur incapacité à propager la terreur et la peur, deux critères qui distinguent le phénomène du terrorisme.

Selon nous, le cyberterrorisme est une opération qui se passe à travers des attaques informatiques faites via l'ordinateur contre un système informatique ou des données vitales d'une institution ou d'une infrastructure stratégique, pour causer des perturbations ainsi que des dommages graves (économiques, sociaux,...) en vue de la réalisation des buts politiques, religieuses ou idéologiques. Par conséquent, pour être qualifiée du cyberterrorisme, la cyberattaque doit être suffisamment grave et d'une ampleur comparable à celle causée par les attaques terroristes classiques pour susciter la peur et la terreur en engendrant des pertes considérables[1]. Uniquement les cyberattaques ayant un impact considérable et créent des dégâts importants font partie du cyberterrorisme, tandis que, les attaques qui « *perturbent des services non essentiels ou représentent avant tout un désagrément coûteux ne sont pas considérées comme actes terroristes* »[2].

---

(1) Pour plus d'informations sur les effets psychologiques du cyberterrorisme, voir : Michael L. Gross, Daphna Canetti et Dana R. Vashdi, « *Cyberterrorism : itseffects on psychologicalwell-being, public confidence and political attitudes* », Journal of Cybersecurity, vol. 3, n° 1, 2017, pp. 49- 58. DOI : 10.1093/cybsec/tyw018.

(2) Dorothy Denning, « Cyberterrorism », témoignage devant le Comité de surveillance du terrorisme, Commission des forces armées,

En se basant sur cette logique, un bon nombre des auteurs avancent que ce phénomène du cyberterrorisme n'est pas encore arrivé en niant, à notre avis, les attentats du 11 septembre 2001 aux États-Unis. Cet avis, n'est pas tout à fait acceptable. Un acte terroriste classique peut engendrer la perte de la vie àun grand nombre de victimes, mais, il peut aussi frapper un nombre limité d'individus. On doit donc se rendre compte, pas seulement de l'impact des actes commis, mais également des motivations et des intentions des attaquants.

B - Les autres concepts qui sont en relation

Le développement du cyberespace a entrainé des confrontations idéologiques, politiques, économiques et militaires. Ces confrontations ont dévoilé, entre autres, la « vulnérabilité » du cyberespace et les systèmes de protection existants. Beaucoup de termes sont ainsi utilisés pour décrire ces confrontations, citons par exemple, les cyberattaques, la cybercriminalité, la cyberguerre, l'hacktivisme et le cyberespionnage.Bien qu'il existe certains critères qui les distinguent, comme l'intention des attaquants et les objectifs à réaliser, un

Chambre des représentants des États-Unis, 23 mai 2000, www.stealthiss.com/documents/pdf/cyberterrorism.pdf.

bon nombre des auteurs ne trouvent pas une véritable différence entre eux.

Avec le brouillard terminologique existant autour de ces phénomènes, et pour éviter toute confusion conceptuelle, il est utile de distinguer brièvement ces différentes confrontations dans le cyberespace.

1 - Cyberattaques

Les cyberattaques peuvent être définies comme : La conduite, par un État ou par des agents ou des entités dontles actions peuvent êtreattribuéesà cet État, de mesures coercitives informatiques destinées, en tirant parti de l'interconnexion des réseaux informatiques d'un autreÉtat, àsévèrement perturber ou à endommager les structures essentielles de cedernier, qu'elles soient militaires, financières, sanitaires ou sociales[1].

Certains auteurs insistent sur le but politique des cyberattaques.[2] Bien que les cyberattaques arrivent dans le monde virtuel, ses conséquences influent le monde réel.

---

[1] Loïc Simonet, « *L'usage de la force dans le cyberespace et le droit international* » Annuaire français de Droit International, vol. 58, 2012, p. 122. DOI: 10.3406/afdi.2012.4673.

[2] The cyber-attack « *consists of any action taken to undermine the functions of a computer network for a political or national security purpose*». Oona A. Hathaway, « *The Law of Cyber-Attack*» California Law Review , vol. 100, 2012, p. 826.

À mon avis, les cyberattaques peuvent être de nature différentes et pour des objectifs variés. De cela, tous les actes illégaux ou violents qui perturbent la sécurité du cyberespace sont considérés comme cyberattaques. Reste donc de connaître la nature et les buts de chacun pour pouvoir bien la catégoriser (cyberguerre, cybercriminalité, cyberespionnage, ou cyberterrorisme).

2 - Cybercriminalité

Comme les autres termes, il n'existe pas une définition universelle pour la cybercriminalité. En Europe, les États utilisent des notions proches de ce terme comme les délits informatiques, la criminalité informatique ou les crimes informatiques. La cybercriminalité peut être conçue comme l'ensemble des infractions commises à travers ou contre un réseau informatique. Son but principal est l'enrichissement illégalà travers la réalisation des gains et des profits financiers à travers des opérations illégales sans avoir aucunes raisons politiques ou idéologiques.

Certainement, la cybercriminalité est un concept large qui couvre une multitude des actes et des infractions illicites commis par l'intermédiaire ou contre des réseaux informatiques. De ce fait, le cyberterrorisme

peut faire partie de ces infractions illicites mais ayant des objectifs idéologiques ou religieuses.

3 - Cyberguerre (Cyberwarfare)

La différence entre la cyberguerre et le cyberterrorisme est la mêmeque celle entre la guerre et le terrorisme classique.

La cyberguerre se passe principalement dans le cyberespace en utilisant des cyberarmes durant une guerre conventionnelle. Elle peut être considérée comme une agression armée dans le cyberespace, puisqu'elle est « *la conduite, dans un contexte de conflit armé, d'activités militairesà l'aide de moyens et de méthodes numériques dans le cyberespace* » comprenant « *aussi bien des activités offensives que défensives des infrastructures informatiques* »[1]. Elle est dans ce cas, une composante ou une tactique de la guerre conventionnelle mais dans le cyberespace ayant pour but de saboter ou d'endommager les systèmes d'informations et de renseignements militaires de l'adversaire pour perturber ou affaiblir ses capacités militaires sur le terrain.Cette possibilité a été conçue lors du conflit qui a

---

(1) Evelyne Akoto « Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public? », Revue de droit d'Ottawa, Première partie, vol. 46, no. 1, 2015, p. 9. <http://www.rdoolr.uottawa.ca/subsite/olr/>. <hal-01244603>

opposé la Russie et la Géorgie en 2008. Cependant, des auteurs admettent la possibilité d'avoir une cyberguerre « *en dehors de tout conflit armé, dans des périodes ne correspondant ni à la guerre ni à la paixmais setrouve « somewherebetween»* »[1].

De ce fait, les règles de droit qui doivent êtreappliquées dans les situations de la cyberguerre sont différentes selon le contexte de ces actes. Alors, si les cyberattaques ont été arrivées dans le cadre d'un conflit armé, les règles de Droit international humanitaire régissent l'affaire. En dehors de cette situation, la désignation des règles applicables se révèlent compliquée et perplexe.

4 - L'hacktivisme

L'hacktivisme désigne l'alliance du piratage informatique et de l'activisme politique.Elle vise la perturbation ou le dysfonctionnement de certains sites pour réaliser des buts politiques mais sans causer de la terreur. En d'autres termes, c'est utiliser le cyberespace pour se protester. Les hacktivistes se différencient des hackers qui ne visent pas des objectifs politiques, mais, ils mènent des opérations contre des sites internet

---

[1] Clémentines Bories, « *Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point* », Revue des droits de l'homme, vol. 6, 2014, p. 2. DOI : 10.4000/revdh.984.

stratégiques en vue de perturber son bon fonctionnement.

L'hacktivisme et le cyberterrorisme ne sont pas similaires[1], ils se distinguent selon l'intention et les buts recherchés. Le but principal ducyberterrorisme est de semer la terreur et de causer des dégâtsconsidérables pour des raisons plutôt idéologiques ou politiques, tandis que l'hacktivisme, qui est aussi politiquement motivé, ne vise pas ni la terreur ni la mort des individus[2]. Toutefois, la frontière entre cyberterrorisme et hacktivisme est parfois poreuse[3], Les groupes terroristes peuvent recruter des hackers doués ou les rallient à leur cause, ou lorsque les hacktivistes décident d'intensifier leurs actions en attaquant les systèmes qui contrôlent les composants critiques de l'infrastructure nationale, comme les réseaux électriques et les services de secours[4].

---

(1) Pour plus d'informations sur la différence entre ces deux phénomènes, voir : Dorothy Denning, « *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for InfluencingForeign Policy* », Global ProblemSolving Information Technology and Tools, (December 1999). https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorim-the-internet-as-a-tool-for-influencing-foreign-policy-2/.

(2) Gabriel Weimann, « *Cyberterrorism: How Real Is the Threat?* », Studies in Conflict & Terrorism, vol. 28, 2005, p. 136, DOI: 10.1080/10576100590905110.

(3) John Klein, « *Deterring and Dissuading Cyberterrorism* », Journal *of Strategic Security*, vol. 8, n° 4, 2015, p. 24. DOI : http://dx.doi.org/10.5038/1944-0472.8.4.1460.

(4) Gabriel Weimann, *Supra* note 43, p. 137.

5 - Cyberespionnage

Le cyberespionnage, étant une des cybermenaces, entre dans la catégorie des cyberattaques persistantes (APT : Advanced Persistant Threat). Il vise à récolter des informations confidentielles à travers des virus « dormants » pour ne pas être repérés, ou par des malwares insérés dans des systèmes d'information et de communication. La complexité de cette opération fait que ce travail couteux est dans la plupart des cas, une affaire d'État. Le cyberespionnage d'État est la forme la plus répandue sur la scène internationale depuis la guerre froide.

En 2012, l'alarme a été sonnée pour détecter FLAME qui est considéré comme un des plus sophistiqués malware[(1)]. Ce logiciel a été considéré vingt fois plus puissant que le ver STUXNET. Les révélations d'Edward Snowden sur les programmes de surveillance de l'Agence Nationale pour la sécurité (NSA :National Security Agency) ont montré la capacité américaine à espionner et à collecter des informations confidentielles.

---

(1) Il s'agit d'un logiciel malveillant destiné à des fins d'espionnage informatiques « *visant à infiltrer un ordinateur à l'insu de son utilisateur pour en prendre le contrôle, collecter des informations ou effacer des fichiers* ». Jean-Marie Bockel, Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense, le Sénat, Session extraordinaire, 2011-2012, p. 16.

En conclusion, on peut dire que ces différentes notions présentent entre eux des points de ressemblance, pourtant, ils existent certaines nuances qui aident à éliminer la confusion et permettent une vraie qualification des actes qui surviennent dans le cyberespace. Cela est évident dans la mesure où il nous permet de bien déterminer les règles juridiques applicablesàchaque cas. À notre avis, une étude objective de l'identité des auteurs des actes, leurs intentions, leurs motivations ainsi que leurs objectives permettent de redresser une ligne frontalière entre les différentes notions. On ne doit pas aussi négliger l'impact des attaques ou leur étendue comme critères importantspour cette qualification. Les cyberagresseurs peuvent certainement recourir aux mêmes techniques pour attaquer leur adversaire, mais, leurs intentions ne sont pas les mêmes. Cela nous rappelle du cas de l'Estonie qui a subi, en 2007, des cyberattaques qui ont paralysé le pays pendant plusieurs jours. Les avis étaient partagés, à tort ou à raison, sur la nature et la qualification de ces actes, s'agissaient-ils d'un cyberterrorisme, d'une cyberguerre ou simplement d'une cyberattaque de grande ampleur. Pourtant, toutes les opinions étaient d'accord sur le fait que ces cyberattaques avaient des raisons politiques.

II - Le changement du rapport de force sur la scène internationale

La technologie a permis un développement dans presque tous les domaines pacifiques et non pacifiques. Comme elle avait des avantages, elle a aussi engendré beaucoup de problèmes qui se tissent avec le recours massif et la dépendance accrue vis-à-vis de l'informatique, ce qui a conduit à l'abolition des frontières et des barrières traditionnelles.

L'utilisation non pacifique du cyberespace nous a mené à la « terreur informatique » ou plus précisément la « Cyber-terreur ». Cet état a été caractérisé par des cybermenaces qui dépendent, non plus de la force militaire traditionnelle, mais de la force électronique « Soft power ». Ila permis un certain déséquilibre et un véritable changement dans les rapports de force traditionnels sur la scène internationale. C'est ainsi que de nouveaux acteurs non étatiques ont vu le jour marquant une rupture avec la perception classique du concept de la force en permettant une diffusion du pouvoir[1] de manière disproportionnée. Cette diffusion est nouvelle et différente de ce qu'arrivait auparavant sur la scène internationale qui assistait uniquement à un

[1] Joseph S. Nye, *Cyber power*, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010, p. 19.

transfert du pouvoir d'un État dominant à un autre[1]. Le rôle de l'État a été réduit en faveur des autres acteurstémoignait ainsi un déclin de l'État souverain. Il n'est plus le seul possédant des informations ni le seul responsable de sa diffusion ou de son contrôle.

L'étude du phénomène de cyberterrorisme exige donc une compréhension minutieuse des différents acteurs existants dans le cyberespacece qui nous aide à comprendre l'influence de leur présence sur la mutation des rapports de force.

A - L'apparition de nouveaux acteurs non étatiques

La question de la sécurité internationale et les menaces qui y sont liées ne sont plus attachée uniquement à la responsabilité des États. D'autres acteurs y sont impliqués de manière directe ou indirecte, positivement ou négativement.On distingue principalement deux types d'acteurs : les acteurs étatiques classiques et les acteurs non étatiques.

Pour les Acteurs étatiques classiques, il faut admettre que les États étaient les premiers acteurs à utiliser le cyberespace. Au début, leur principale utilisation était dans le domaine militaire avant de

---

[1] *Ibid* , p. 1. "*Power transition from one dominant state to another is a familiar historical event, but power diffusion is a more novel process*".

s'étendre aux domaines civils. En ce temps, beaucoup desÉtats ont eu recours essentiellement au « Cyberespionnage » via leurs « services du renseignement ». Le but était lié dans la plupart des cas à des enjeux sécuritaires puisque ce sont surtout les défis stratégiques et sécuritaires qui peuvent pousser un État à se riposter via le cyberespace. Cela ne nie pas le fait que les États avaient également des enjeux politiques, économiques et commerciaux dans le cyberespace.

Les Étatspouvaient mener des cyberattaques offensives ou défensives, en vue de se protéger ou pour affaiblir leurs adversaires par saboter, perturber ou paralyser ses capacités technologiques, comme c'était le cas du ver *Stuxnet*[1]. Ces attaques pouvaient êtrecomplémentaires à une guerre conventionnelle ayant pour cibles des infrastructures militaires ou

---

(1) Cette cyberattaque est arrivée en 2010 contre les centrifugeuses iraniennes de Natanz à travers le lancement d'un ver Stuxnet (il faisait partie du programme secret américain *Olympic Games*). Cette opération a été décidée en 2006 ayant pour objet le sabotage du programme nucléaire iranien. La fabrication du virus a pris trois ans puis il a été inséré dans la centrale. Il a resté un an caché, en induisant des dégâts considérables, avant d'être découvert par les iraniens. Les révélations du journaliste américain *David E. Sanger* a dévoilé l'implication et la responsabilité des services de renseignement américains et la collaboration de l'armée israélienne dans cette affaire. David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, New York, Crown Publishing Group, 2012.

civilesrenfermant le cyberespace comme théâtre d'opérations. Une large partie de ces cyberattaques étatiques viennent particulièrement de trois pays à savoir, les États-Unis, la Russie et la Chine.

La qualification de certains États comme des « cyberterroristes » peut être utilisée par les adversaires contre les États qui ne respectent pas les principes de la démocratieou les droits de l'homme selon l'appréciation (perception) occidentale. Ex. Corée du Nord ou l'Iran.

En ce qui concerne les acteurs non étatiques, ils participent activement aux activités cybernétiques soient pour des raisons pacifiques ou non pacifiques. Leur existence dans le cyberespace fut le résultat de plusieurs raisons liées principalement au fait que le cyberespace n'a pas de frontières physiques et que les États n'arrivent pas à le contrôler complétement. Il jouit à cet égardd'une facilité d'accès qui donne à ces acteurs une rapidité et une simplicité dans « *la mobilisation des civils* » et les aide à « *devenir des cyberagents au service de causes particulières* ».[1] Leur recours massif à l'usage de la technologie numérique dans le cyberespace et leur manipulation de la nouvelle technologie à leurprofit ont

[1] Solange Ghernaouti-Hélie, « *Menaces, conflits dans le cyberespace et cyberpouvoir* », Sécurité et stratégie, vol. 3, n° 7, 2011, p. 65. DOI 10.3917/sestr.007.0061.

conduit à une vague d'attaques imprévisibles et anonymes.

Ces acteurs peuvent être des groupes terroristes islamistes (ayant une idéologie religieuse erronée), des groupes politiques[1], groupes militants, des hacktivistes, ou même des individus indépendants (hackers). Les moyens utilisés par les cyberterroristes sont identiques à ceux utilisés par les hackers ou les cybercriminels[2], mais motivés par une certaine idéologie et des raisons politiques. Les cyberterroristes peuvent recourir aux hackers ou des cybercriminels s'ils jugent nécessaire et utile pour soutenir leur stratégie terroriste.

L'asymétrie du cyberterrorisme donne un grand avantage à ces acteurs pour mener à bien leurs activités, puisque cette asymétrie « *quelle que soit sa forme, est le privilège du faible, qui cherche à vaincre le plus puissant* »[3]. Ces acteurs asymétriques « *disposent de*

---

[1] Ces groupes politiques ont choisi de recourir au terrorisme pour réaliser des buts politiques, en bénéficiant d'une certaine clandestinité intensifiée dans le cyberespace. On peut citer par exemple : Tigres tamouls, indépendantistes birmans…. Olivier Kempf, « *Le cyberterrorisme : un discours plus qu'une réalité* », Hérodote, vol. 1, n° 152-153, 2014, p. 84. DOI 10.3917/her.152.0082.

[2] Les cyberterroristes peuvent recourir à la cybercriminalité à travers des cyberattaques illégales qui visent le financement de leurs activités.

[3] Barthélemy Courmont, « *L'émergence de nouveaux acteurs asymétriques* », Revue internationale et stratégique, vol. 3, n° 51, 2003, p. 84. DOI 10.3917/ris.051.0081.

moyens disproportionnés et d'objectifs militaires et politiques divergents »[1]. Pour étudier par exemple, les attaques menées par les groupes djihadistes dans le cyberespace, certains auteurs écartent le terme cyberterrorisme en faveur des termes e-djihad ou cyber-djihad[2]. Cette qualification marque l'utilisation prépondérante de l'internet par ces groupes terroristes précisément.

Si les cyberterroristes n'ont pas encore mené des cyberattaques terroristes graves, ils investirent le cyberespace pour se financer, recruter leurs militants et/ou faire de la propagande en vue de diffuser leur idéologie qui n'est plus limitée à l'aspect national, mais elle vise également des militants multinationaux ou transnationaux. Ils utilisent le cyberespace autant pour se coordonner via le cyberplanning[3] en bénéficiant des réseaux sociaux et des sites internet.

---

(1) Sophia Clément-Noguier, « *Sécurité du fort contre asymétrie du faible* », Revue internationale et stratégique, vol. 3, n° 51, 2003, p. 89. DOI 10.3917/ris.051.0089.

(2) En ce sujet, voir : Jean Pierre Filiu, *Les dynamiques du cyberjihad*, Paris, Questions Internationales, n° 47, janvier 2011. Benjamin Davis, « *Ending the Cyber Jihadi: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber governance* », *Commlaw Conspectus*, vol. 15, 2006, pp. 119-186.

(3) Le cyberplanning est la coordination numérique d'un plan intégré, « *it refers to digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed. It can include cyberterrorism as part of the overall plan* ». Timothy Thomas,

B - La force électronique (Soft power) via la force militaire

Au début de l'invention des ordinateurs fixes, le risque d'une éventuelle attaque informatique n'existait pas. Le seul danger était de mettre un programme malveillant sur un support matériel (disquette ou CD) et de l'insérer dans l'ordinateur. Le problème des attaques électroniques est apparu avec le développement du secteur des technologies de l'information et des communications (TIC) en raison de l'interconnectivité des appareils à l'internet.Ce développement a fait que « *les cybertechniques constituent une nouvelle manière d'appliquer les outils fondamentaux du pouvoir national – persuasion, coercition et récompense* »[(1)].

L'apparition de la force technologique a conduit à une redistribution des rapports de force entre les différents acteurs de la communauté internationale. Les acteurs étatiques ne sont plus les seuls détenteurs de la force, leur monopole en ce sens a été réduit en faveur d'autres acteurs non étatiques qui partagent une partie de cette force.

«*Al Qaeda and the Internet: The Danger of "Cyberplanning»*, Parameters, Printemps 2003, p. 113.

(1) James A. Lewis, « *Étude préliminaire sur les analyses en cybersécurité : L'affaire Snowden comme étude de cas* », Hérodote, La découverte, vol. 1, n° 152-153, 2014, p. 32.

Les acteurs étatiques et non étatiques ont augmenté leurs capacités défensive et offensive dans le cyberespace par un recours accru à la cybermilitarisation ce qui menace violemment la sécurité internationale et contredit le principe de l'utilisation de l'espace à des fins pacifiques. En même temps, la course au cyberarmement «*fragilise le pouvoir de dissuasion de l'arme nucléaire et rend la possibilité d'une confrontation plus probable* », puisque « *la dissuasion nucléaire repose sur la transparence et la croyance partagée entre les acteurs que les systèmes de chacun fonctionneront, ainsi aucun n'a intérêt à prendre le risque d'une première frappe* »[1]. Le privilégie plutôt avantageux des Cyberarmes est qu'ils sont imprévisibles et inattendus, ils peuvent réaliser les objectifs espérés tout en restant discrète et anonyme.

III - Les impacts de la détention de la force électronique

Le développement rapide des cybertechnologies a montré la vulnérabilité des institutions et des systèmes d'informations, et a en même temps révélé la défaillance des systèmes juridiques nationaux et internationaux et

---

[1] Emmanuel Meneut, « La cyberguerre et la structuration des relations internationales : Le cas Nord-Coréen », IRIS Asia Focus, n° 54, Décembre 2017, p. 14.

leur incapacité à arrêter les abus et les menaces provenant de son utilisation.

Les cyberattaques sont devenues des formes d'affrontements indirects entre les États où le cyberespace a été transformé en un vrai théâtre d'opération.La plupart de ces cyberattaques, y compris le cyberterrorisme, font partie des « *guerresasy métriques* »[1] qui n'exigent pas de vraies armes matérielles et n'appliquent pas le « *principe de l'égalité des armes*»[2]. Cela a conduit à la détention de la fore électronique qui a poussé les Étatsplus précisémentà penser autrement en s'impliquant dans une course au cyberarmement.

Toutefois, les défis, déjà expliqués, que représente le cyberespace entravent parfois l'efficacité des mesures étatiquès prises, ainsi que toute planification stratégique. Le danger que représente par exemple une attaque terroriste contre des centrales nucléaires est préoccupant à cause de la dépendance des installations nucléaires aux systèmes d'informations et à l'internet.

---

[1] Ce type de guerre est marqué par un déséquilibre soit stratégique, militaire, politique ou économique entre les parties concernées. Dans ce type de guerre, tous les moyens, licites ou illicites sont envisagés.

[2] Toni Pfanner, « *Les guerres asymétriques vues sous l'angle du droit humanitaire et de l'action humanitaire* », Revue Internationale de la Croix-Rouge, vol. 87, 2005, p. 260.

A - Apparition des Cyberarmes et la course aux armements

Il est clair que « *les conflits du cyberespace ne peuvent être dissociés des conflits réels et des autres moyens d'action* »[1] qui se passent dans les autres espaces. Face à des cyberattaques de plus en plus sophistiquées et agressives, les Étatsse sont rendu compte de la nécessité de se protéger via des mesures stratégiques offensives et défensives. Cette nécessité a été traduite par une volonté grandissante deposséderla force électronique caractérisée par le recours massif des différents acteurs de la communauté internationale, et surtout les États, à la détention des armes électroniques « les Cyberarmes ». Ces cyberarmes[2] sont perçues comme des outils informatiques ayant un pouvoir destructif imprévisible capable de perturber, paralyser ou déstabiliser des infrastructures vitales ou des systèmes d'informations liés à la gestion de l'État ou à sa sécurité tout en restant anonyme pour lui causer des dommages fonctionnels ou techniques comme par

---

(1) Frédéric Douzet, Alix Desforges et Kevin Limonier, « *Géopolitique du cyberespace : « territoire », frontières et conflits* », Fronts et frontières des sciences du territoire CIST proceedings, 2014, pp. 176-177. HAL Id: hal-01353455.

(2) Pour d'autres définitions de cyberarmes, voir : Thomas Rid et Peter McBurney, « *Cyber-Weapons* », RUSI Journal, vol. 157, n° 1, 2012, pp. 6-13. DOI : 10.1080/03071847.2012.664354.

exemple, les virus, les chevaux de Troie, les codes, etc.....De cela, elles parviennent à « *atteindre des objectifs stratégiques, opérationnels et tactiques jusqu'ici à la portée d'opérations militaires* »[1]. La partie la plus faible peut recourir aux cyberarmes pour compenser sa faiblesse militaire ou stratégique, même si ces cyberarmes ne sont pas licites. À cet égard, certains pays développés ont conclu des contrats de partenariat avec des grands groups de défenses spécialisées pour doter leur arsenal militaire des cyberarmes, comme le partenariat entre les États-Unis et Northrop Grumman, General Dynamics, Lockheed Martin ou Raytheon[2].

Pour faire face aux critiques grandissantes liées au cyberarmement, les pays ont avancé un justificatif, plus ou moins, réel pour développer leur arsenal cybernétique qui se manifeste dans sa volonté de « lutter contre le terrorisme ». Cette justification est devenue l'argument qui légalise toute opération étatique, légitime ou pas, dans le cyberespace. Mais, légale ne veut pas dire

---

[1] Loïc Simonet, « *L'usage de la force dans le cyberespace et le droit international* », Annuaire français de Droit International, vol. 58, 2012, p. 123. Doi : 10.3406/afdi.2012.4673.

[2] Ce sont des grands groupes de défense qui font partie des dix premiers groupes mondiaux. Les États-Unis ont conclu des contrats de fourniture avec ces groupes en vue de développer son arsenal militaire.

nécessairement légitime[1].Ces pays admettent que défendre le terrorisme signifie le recours à une limitation des libertés, voire même une atteinte à la vie privée des individus. Cette atteinte peut transformer la lutte pour la « *bonne cause* » (la lutte contre le terrorisme) en une *mode totalitaire* qui restreint les droits de l'homme et surtout la liberté d'expression. Or, cette liberté qui « *n'est pas un droit absolu* » peut être« *restreinte, sous réserve de respect de critères de légalité, de nécessité, de proportionnalité et de non-discrimination strictement interprétés, lorsque cette liberté est utilisée pour inciter à la discrimination, à l'hostilité ou à la violence* »[2].

En raison de la dangerosité des cyberarmes et en vue de restreindre, voir arrêter, la course au cyberarmement, il est nécessaire d'adopter une convention internationale qui vise la pacification du cyberespace[3] en proposant un cadre juridique qui contrôle les activités cybernétiques des États. Cette

---

(1) La légalité s'apprécie en fonction du droit positif, tandis que la légitimité est plus large, puisqu'elle se mesure à la lumière de la culture dans une société.

(2) Guide de L'Office des Nations Unies contre la drogue et le crime (ONUDC) sur *l'Utilisation de l'Internet à des fins terroristes* (outil d'assistance technique), 2014, p. 14.

(3) Pour plus d'informations sur cette convention, consulte : Edward M. Roche et Michael J. Blaine, «*International Convention for the Peaceful Use of Cyberspace* », Orbis: Journal of World Affairs, vol. 58, n° 2, Spring 2014, pp. 282- 296.

convention, à vocation universelle, doit régir toutes les questions liées à l'utilisation du cyberespace à des fins pacifiques. En plus, des sanctions en cas du non-respect des États de leurs obligations prévues doivent être envisagées dans cette convention. Pourtant, un problème pourra surgir dans le cas d'adoption de telle convention lié aux acteurs non étatiques. Il est clair qu'une convention internationale engage uniquement les États. Il reste donc à réfléchir à une politique internationale unifiée pour faire face aux utilisations non pacifiques de ces acteurs.

B - Les stratégies de cyberdéfense relatives à la lutte contre le cyberterrorisme

Le danger des différentes cyberactivités prend de plus en plus d'ampleur. Dans plusieurs situations, les États ne pourraient pas se protéger des cyberactivités provenant des serveurs installés à l'étranger puisque la cybertechnologie obéit à la déterritorisation[1] de l'espace virtuel. Même si certaines législations nationales prévoient des actions contre un serveur situé dans un autre État, son application effective et réelle nécessite une coopération juridique et des accords conclus avec

[1] En ce sujet, voir : Marie Stella, « *La menace déterritorialisée et désétatisée : le cyberconflit* », Revue internationale et stratégique, vol. 1, n° 49, 2003, pp. 165- 171. DOI 10.3917/ris.049.0165.

cet État. La difficulté s'amplifie encoreavec le développement évolutif des menaces et l'imprévisibilité des attaques qui rendent les Étatsincapables à empêcher de telles attaques. Pourtant, ils peuvent au moins diminuer l'étendue et les effets des attaques à travers leurs stratégies de cybersécurité.

Fragilisée par une dépendance accrue à l'égard de la technologie de l'information, et en l'absence d'une stratégie commune de coopération internationale dans le cyberespace, un bon nombre de pays développés ont annoncé unilatéralement des stratégies de cyberdéfense et de cyberdissuasion, conduisant à une militarisation du cyberespace.

En ce qui concerne la politique de cyberdéfense, certains despays développés technologiquement ont ressenti la nécessité d'une protection croissante du cyberespace comme étant une composante de leur sécurité nationale. Pour cela, ils ont beaucoup développé leurs capacités informatiques pour doter leur arsenal militaire des cyberarmes qui peuvent être utilisés plus en temps de paix qu'en temps de guerre. En France par exemple, le livre blanc sur la défense et la sécurité nationale publié en 2008 «*place la sécurité des systèmes d'information au même niveau stratégique que la*

dissuasion nucléaire » ce qui « *illustre l'importance prise par ces questions pour des décideurs stratégiques et politiques* »[1]. La France a même déclaré qu'une cyberattaque de grande ampleur peut lui donner le droit à une action militaire.

Aux États-Unis, le président américain Barack Obama[2] a annoncé en 2009 « *une nouvelle guerre contre le* cyberterrorisme » et a créé au sein de la maison Blanche et sous sa direction, un poste de « responsable de la guerre contre le cyberterrorisme ». Le but étant de protéger le pays des éventuelles cyberattaques terroristes.

Pour restreindre les effets dangereux de cette politique, certaines organisations internationales ont essayé de créer des stratégies de cyberdéfense collectives pour inciter leurs membres à se coopérer en la matière. On peut citer par exemple, la stratégie de l'Union Européenne adoptée en 2013. L'OTAN qui, a considéré que la cyberdéfense est un domaine très important pour

---

(1) Alix Desforges, « *Les représentations du cyberespace : un outil géopolitique* », Hérodote, vol. 1, n° 152-153, 2014, p. 77. DOI 10.3917/her.152.0067.

(2) Depuis son arrivée au pouvoir, le président Barack Obama a accordé une attention particulière à la cybersécurité comme étant un des défis que les États-Unis doivent faire face puisqu'elle est une question de sécurité nationale.

la sécurité des pays, a également adopté une politique de cyberdéfense[1] en 2014 (et actualisé en 2017) sur la cybersécurité pour coordonner et diriger les stratégies de ses membres à cet égard.

Pour la politique de cyberdissuasion[2], elle doit être appliquée avant les cyberattaques pour éliminer tout adversaire potentiel. Elle comprend des « *mesures formatrices non militairesappliquées en temps de paix* »[3], elle peutêtre offensive ou défensive. L'idée réside dans l'aptituded'un acteur à utiliser le cyberespace pour réaliser un avantage sur les autres acteurs ce qui pouvait s'étendre sur les autres champs opérationnels[4].

---

(1) Les moyens de l'OTAN de cyberdéfense sont variés allant de la défense collective jusqu'à la gestion de crise et la sécurité coopérative. Il s'appuie à cet égard sur les règles de droit international qui s'appliquent également au cyberespace.

(2) La politique de cyberdissuasion peut être définie comme « *une stratégie par laquelle un État, désireux de défendre son intégrité, affiche son intention de convaincre tout adversaire de renoncer à une activité cybernétique destructrice en ciblant et en influençant son appareil décisionnel dans le but de susciter dans son chef la crainte de représailles dont l'ampleur dépasserait celle de l'attaque initiale* ». Emilio Iasiello, « *Is Cyber Deterrence an Illusory Course of Action?* », Journal of Strategic Security, vol. 7, n° 1, 2013, p. 37. DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5.

(3) John Klein, « *Deterring and Dissuading Cyberterrorism* », Journal of Strategic Security, vol. 8, n° 4, 2015, p. 31. DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1460.

(4) Encesens, voir; Daniel T. Kuehl, « *From cyberspace to cyberpower: Defining the problem* », dans Franklin D. Kramer, Stuart H. Starr et Larry K. Wentz, « *Cyberpower and National Security*», Ch. 2, Washington D.C, National Defense University Press: Potomac Books, 2009, pp. 24- 42.

L'essentiel est de respecter le principe de proportionnalité pour éviter une escalade des représailles.

Pourtant, plusieurs obstacles se posent à l'égard de l'application de la politique de cyberdissuasion. En premier lieu, les attaques cybernétiques sont dans la plupart des cas imprévisibles et anonymes et donc, difficile d'identifier leurs auteurs. Cette difficulté est accrue dans le cas des attaques commises, pas par des États, mais par des individus ou des groupes terroristes. Les attaquants ou les groupes terroristes sont dans beaucoup des cas soutenus ou parrainés par des États adversaires. En plus, si l'État a pu repérer l'identité des attaquants, il lui sera difficile de les poursuivre, surtout s'ils se trouvent sur un ou plusieurs territoires, puisque cela nécessite une coopération entre ces pays pour pouvoir les livrer ou les juger.D'où le caractère transfrontalier de l'attaque et des attaquants. En outre, il faut bien admettre que la question de prouver l'intervention ou même l'implication d'un État dans de telles attaques et d'engager par la suite sa responsabilité estdélicate. Par exemple, lors des attaques contre l'Estonie en 2007 (en temps de paix) ou la Géorgie en

2008[1] (en période de guerre), il était difficile de prouver l'implication et par conséquent, la responsabilité de la Russie qui a démenti toutes relations avec ces attaques et a nié toute intervention dans ces affaires. Cela, malgré les forts soupçons que la Russie y a été directement impliquée[2]. C'est pareil dans le cas du ver STUXNET ou FLAME, les américains n'ont jamais reconnu leur responsabilité de ces attaques.

Autre question relative cette fois-ci à la nature de la réaction d'unÉtat victimed'un cyberterrorisme ou se trouve dans la possibilité d'être un cible d'une attaque cyberterroriste,aurait-il le droit de recourir à la force pour se riposter ? Est-ce que cette réaction peut être considérée comme une défense légitime contre une agression armée ou bien une utilisation de la force mais au cyberespace ? Les opinions autour de cette

---

(1) La Géorgie a subi en 2008 des cyberattaques qui ont été suivi par l'invasion Russe. Ce conflit a été marqué par un recours massif aux cyberattaques de la part des russes en vue de paralyser les infrastructures stratégiques de la Géorgie. Ces attaques ont pris fin juste après la cessation du conflit. Certains l'ont considéré comme le premier cyberconflit étatique.

(2) La Russie et la Chine soutiennent leurs secteurs civils et les cybermilices qui peuvent mener des cyberattaques à la place de l'État. Ce dernier pourra nier expressément son implication dans ces cyberattaques, ce qui lui permet d'échapper de toute responsabilité internationale. Lucas Kello, *Les cyberarmes : Dilemmes et futurs possibles*, traduit par Thomas Richard, Institut français des relations internationales (IFRI), Politiques étrangères, Vol. 4, 2014, p. 149.

questionsont partagées. En règle générale, selon les principes du Droit international, le recours à la force ou l'usage de la force dans les relations internationales sont interdits selon la Charte des Nations unies[1], sauf dans le cas d'une réponse à une agression armée constituant un acte de légitime défense[2].

Des auteurs considèrent qu'une situation d'utilisation de la force dans le cyberespace peut être admise si les cyberattaques visaient un État précis de manière à lui provoquer des effets négatifs comparables à une utilisation normale de la force. Mais « *seules les formes les plus graves de l'emploi de la force peuvent être*

---

(1) L'article 2(4) de la charte des Nations Unies stipule que « *Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies* ».

(2) L'article 51 de la charte des Nations Unies prévoit « *qu'aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. Les mesures prises par des Membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité et n'affectent en rien le pouvoir et le devoir qu'a le Conseil, en vertu de la présente Charte, d'agir à tout moment de la manière qu'il juge nécessaire pour maintenir ou rétablir la paix et la sécurité internationales* ».

qualifiées d'agressions armées ».[1] La difficulté d'appliquer cette exception dans le cyberespace[2] réside dans le fait de désigner premièrement et de manière précise les auteurs de l'attaque puis prouver que l'État concerné était victime d'un cyberterrorisme (ayant l'ampleur d'une agression armée) pour pouvoir lui attribuer légitimement le droit à la légitime défense. Les États-Unis (en 2011)[3] et la France (en 2013) « *ont clairement affirmé qu'une cyberattaque de grande ampleur pourrait être considérée comme un acte de guerre et qu'ils se réserveraient le droit de répliquer par tous les*

---

(1) Barbara Louis-Sidney, « *La dimension juridique du cyberespace* », Revue internationale et stratégique, vol. 3, n° 87 , 2012, p. 77. DOI 10.3917/ris.087.0073.

(2) Si on peut considérer le cyberterrorisme comme une forme des cyberattaques, l'État victime devra prouver que « *la cyberattaque ou ses conséquences constituent un emploi illicite de la force d'une gravité, l'implication d'un État dans l'exécution ou l'organisation de l'attaque informatique, et que la cyberattaque a été commise à une fin agressive* ». Evelyne Akoto, « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ?* », Deuxième partie, Revue de Droit d'Ottawa, vol. 46, n° 1, 2015, p. 217.

(3) Selon un rapport du département de la défense américaine, le président « *se réserve le droit de répondre, par tous les moyens pour défendre sa nation, ses alliés, ses partenaires ou ses intérêts contre des actes hostiles au cyberespace*». « *The President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile acts in cyberspace. Hostile acts may include significant cyber-attacks directed against the U.S. economy, government or military. As directed by the President, response options may include using cyber and/or kinetic capabilities provided by DoD*». Rapport du Department of Defense Cyberspace Policy Report, " A Report to Congress Pursuant to the National Defense Authorization Act for fiscal Year 2011", Section 934, November 2011.

moyens »[1]. L'OTAN asimilairement considéré les cyberattaques comme type des actes de guerre nécessitant les mêmes démarches collectives y compris « la défense collective ». Il se donne le droit de riposter face à d'éventuelles attaques de ce genre en se basant sur l'article 51 de la charte des Nations Unies pour légitimer son action.

Pour surmonter les difficultés de preuve dans l'hypothèse d'une agression armée et prouver l'implication de certains États dans l'attaque cyberterroriste, certains auteurs font appel à la « *théorie de la responsabilité imputée* »[2]. Selon les règles de droit international public, la responsabilité d'un État peut être engagée si cet État manque à son devoir de vigilance qui exige que « *tout État se munisse de moyens afin de prévenir que sonterritoire ne soit utilisé de manière à léser les droits d'un autre État souverain* »[3]. Et par conséquent, la responsabilité d'un Étatsera engagée s'il connait que des cyberattaques ou des actes terroristes ont été commis à partir de son territoire contre un autre État.

---

(1) Frédérick Douzet, « *La géopolitique pour comprendre le cyberespace* », Hérodote, La Découverte, vol. 1, n° 152-153, 2e trimestre 2014, p. 15. DOI : 10.3917/her.152.0003.

(2) Evelyne Akoto, « *Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ?* », Deuxième partie, Revue de Droit d'Ottawa, vol. 46, n° 1, 2015, p. 224.

(3) *Ibid.*

IV . La recherche de la paix au cyberespace

Le cyberespace est *« un bien commun planétaire »* et *« ne relève donc pas dans son entièrèté de la compétence d'un seul État ou d'un groupe d'États »*[1]. Il est à vrai dire un véritable espace universel de partage et d'échanges de toute sorte non limité par des frontières physiques.

Mais, face aux diverses cyberattaques, et en l'absence des règles internationales qui réglementent de manière adéquate les menaces du cyberespace, et dans une communauté internationale dépourvue de toute stratégie commune de cybersécurité,on se trouve dans la nécessité d'une action universelle unifiée qui vise un cyberespace pacifique et paisible.Le fait de l'interconnectivité des affaires économiques, politiques et sociales de tous les États justifient cette nécessité de coopération. Les cyberattaques en général perturbent la stabilité interne des États et menacent ainsi la paix et la sécurité mondiales.

Il est bien évident de connaitre le rôle du droit international en ce sujet et la réaction des États face à ces nouveaux défis.

---

[1] Evelyne Akoto *« Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? »*, Revue de droit d'Ottawa, Première partie, vol. 46, no. 1, 2015, p. 6. <http://www.rdoolr.uottawa.ca/subsite/olr/>. <hal-01244603>

A - Rôle du droit international

Vu les menacescroissantesdans le cyberespace, on se demande très souvent sur le rôle du droit international, existe-t-il des règles internationales applicables aux attaques qui surviennent dans le cyberespace, et précisément, dans le cas d'un cyberterrorisme ? La réponse aux yeux de la doctrine ne semble pas être précise ou claire. Certains auteurs pensent qu'il n'existe pas à nos jours un cadre juridique international qui réglemente les activités et les menaces dans le cyberespace puisque cet espace est nouveau et n'a pas ni frontières ni limites matérielles (« Cyberspace isnowhere[1] » le cyberespace est nulle part). Il « *s'oppose à l'espace conventionnel au sens où il est affranchi de toute localisation physique ou géographique, il n'est pas un endroit, mais un point de rencontre de flux informationnels portés par des réseaux informatiques interconnectés* »[2]. En conséquence, le cyberespace, étant un espace ouvertet sans une vraie autorité régnante, est

---

(1) Davis Brown, « *A Proposal for an International Convention to Regulate the use of Information Systems in Armed Conflict* », Harvard International Law Journal, vol. 47, n° 1, hiver 2006, p. 180.

(2) Stéphane Leman-Langlois, « *Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace Commercial* », Criminologiem vol. 39, n° 1, printemps 2006, p. 65. DOI : 10.7202/013126ar.

régi par un vide juridique[1] et donc, c'est impossible « *d'appliquer des lois à internet* »[2] par exemple. En réalité, le cyberespace a permis « *un déplacement de la souveraineté, l'État en perd quelque peu au profit de l'usager et des réseaux constituants de cet espace virtuel* »[3]. De cela, le fait de l'absence d'une souveraineté nationale (qui se limite en réalité à la première couche physique relative aux infrastructures matérielles) ou d'une gouvernance universelle justifie cette approche.

Par contre, d'autres auteurs et experts affirment l'existence d'un encadrement juridique international de ces questions. Ils soulignent le fait que « *les attaques informatiques, en fonction de leur intensité, de leur finalité ou de leur auteur, sont susceptibles de déclencher l'application de différents types de corpus juridiques nationaux ou internationaux, et par conséquent, pas de*

---

(1) Cette absence de règles internationales peut être comblée par le recours aux principes généraux de droit international inspirés et formulés dans la charte des Nations unies, notamment le règlement pacifique des conflits dans le cyberespace et la préservation des intérêts et de l'intégralité de chaque État en se basant sur le concept de la souveraineté, de l'égalité et de la sécurité partagée.

(2) Pierre Trudel, « *Quel droit et quelle régulation dans le cyberespace ?* », Sociologie et sociétés, vol. 32, n° 2, 2000, p. 191. DOI : 10.7202/001806ar.

(3) *Ibid* , p. 192.

vide juridique dans le cyberespace »[1] Cet avis a été affirmé dans les rapports du groupe d'experts gouvernementaux des Nations unies chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale[2]. Ce corpus est constitué de conventions et traités internationaux, régionaux ou nationaux en matière de lutte contre le terrorisme, des résolutions de l'Assemblée générale et du conseil de sécurité en ce sujet, ainsi que certaines règles du droit international coutumier. En plus, les attaques terroristes qui arrivent dans le cyberespace peuvent certainement avoir des conséquences dans le monde physique. Pour cela, certaines règles de droit international, principalement, en ce qui concerne le droit de l'espace, de la mer, de l'air etle droit international humanitaire[3]

---

(1) Barbara Louis-Sidney, S*upra* note 78, p. 74.

(2) Ces rapports ont affirmé que le droit international, et notamment, la charte des Nations Unies, s'applique dans le cyberespace, ce qui représente une importance croissante pour le maintien de la paix et la stabilité.Rapport du groupe d'experts gouvernementaux des Nations unies chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, Doc off NU, 2013, Doc NU A/68/98 (24 juin 2013) au parag. 19. www.un. org/ga/ search/ view_doc. asp? symbol= A/68/98, www. un: org/ ga/ search/ view-doc. asp? symbol= A/68/98. Rapport du Groupe d'experts gouvernementaux chargé d'examiner le progrès de la téléinformatique dans le contexte de la sécurité internationale, Doc off NU, 2015, Doc NU A/70/174 (22 juillet 2015) au parag. 28. www. un: org/ ga/ search/ view- doc.asp?symbol= A/70/174.

(3) En général, les actes de terrorisme sont régis par les règles de DIH. La IVe Convention de Genève (1949) (article 33) et ses deux

(relatif aux conflits armés) « *ont été étendues aux activités cyber* », constituant ainsi « *le socle futur de potentielles nouvelles normes juridiques internationales ducyberespace* »[1].

Selon nous, l'idée du vide juridique au cyberespace ne peut pas être acceptée. Le cyberespace est régi par certaines règles de droit international applicable en la matière. Toutefois, il a besoin d'une règlementation particulière qui convient avec la spécificitédu milieu etla complexité des cyberattaques en raison de la déterritorialisation du cyberespace, l'anonymat des

---

Protocoles additionnels (première protocole article 51 parag. 2 et deuxième Protocole article 13 parag. 2) interdisent les « *actes de terrorisme* » et les « *actes de violence* » qui visent à répandre la terreur parmi la population civile. La question des opérations du cyberterrorisme n'a pas été expressément citée car ces situations n'existaient pas lors de la conclusion des conventions de Genève de 1949 ni ses deux protocoles. Cependant, la majorité des avis est favorable pour l'extension de l'application des règles de DIH aux attaques cybernétiques terroristes qui sont commises dans le cadre d'un conflit armé puisque le champ d'application du DIH peut englober ces développements. Selon nous, cet avis peut être justifié. L'utilisation de certaines armes est prohibée selon le DIH et les cyberattaques terroristes sont commises à travers des Cyberarmes. Ces armes peuvent être considérées, selon l'article 36 du premier protocole additionnel, comme une évolution des armes classiques (*faisant partie de l'acquisition ou l'adoption de nouvelle arme*) qui produisent les mêmes effets dévastateurs (surtout si elles sont utilisées contre des infrastructures vitaux) que les armes classiques dans le monde réel. La seule exception sur cette prohibition est que ces nouvelles armes sont utilisées contre des cibles militaires.

[1] Oriane Barat-Ginies, « *Existe-t-il un droit international du cyberespace ?* », vol. 1, n° 152-153, 2014, p. 201. DOI 10.3917/her.152.0201.

actes, la rapidité et la simplicité des techniques utilisées. Quant à question de la lutte contre le cyberterrorisme, on peut se référer aux règles spéciales qui organisent le terrorisme en général. Il est frappant de constater que malgré l'importance de cette question, aucune convention universelle n'a été conclue en ce sujet jusqu'à nos jours. On ne trouve sur la scène internationale que presque deux documents principaux qui ne traitent pas directement la question du cyberterrorisme mais organisent des questions liées au cyberespace : la convention de Budapest adoptée par l'Union Européenne et le Manuel de Tallinnrédigé par l'OTAN. Pourtant, ces deux documents ne sont pas universels et ne renferment pas ce qu'on peut le considérer comme une « stratégie mondiale ».

Pour la Convention de Budapest[1], elle se limite à aborder les questions liées à la cybercriminalité[2]. Cependant, elle n'a pas défini le cyberespace, comme étant un nouveau milieu d'attaques cybernétiques, ni traitant les autres types d'attaques, comme le

[1] La Convention de Budapest sur la cybercriminalité signée en 2001 est considérée comme le premier traité international traitant les infractions et les délits pénaux commis par l'intermédiaire des réseaux informatiques.

[2] Barbara Louis-Sidney, « *La dimension juridique du cyberespace* », Revue internationale et stratégique, vol. 3, n° 87, 2012, p. 74. DOI 10.3917/ris.087.0073.

cyberterrorisme ou la cyberguerre. Quant au Manuel de Tallinn[1], il est considéré comme la première tentative de réflexion et de codification du droit international applicable à la cyberguerre (cyberconflits) internationaux ou non internation auxconstituant ainsi le meilleur outil juridique actuel d'interprétation du droit international aux enjeux du cyberespace[2] « *seules les opérations cybernétiques atteignant un certain «degré » d'emploi de la force au regard de la charte des Nations unies (jus ad bellum) sont analysées dans le manuel* ». Cependant « *la cybercriminalité ou le cyberespionnage ne sont pas étudiés sauf dans le cas où un tel acte est en lien direct avec un conflit armé* »[3]. Considéré comme un document important, pourtant, il n'a aucune valeur juridique contraignante,les États ne sont pas obligés de le respecter ou d'appliquer ses règles, en plus, un État accusé ne peut subir aucune sanction à cet égard.

Pour les efforts des Nations Unies à ce propos, on aperçoit qu'ils sont limités, bien que la question de la lutte contre le terrorisme ait été abordée de manière plus ou moins fréquente. En 2006, l'assemblée générale a

---

(1) Le Manuel de Tallinn sur le droit international applicable à la « cyberguerre » a été rédigé par un groupe d'experts du Centre d'excellence pour la « cyberdéfense » de l'OTAN en 2013.

(2) Oriane Barat-Ginies, *Supra* note 93, p. 202.

(3) *Ibid.*

adopté à l'unanimité la « stratégie antiterroriste mondiale des Nations Unies » constituant une étape importante et une arme collective contre le terrorisme. En ce qui concerne la question du cyberterrorisme, on remarque une absence de toute stratégie internationale malgré l'affirmation expresse du secrétaire général dans son rapport intitulé « S'unir contre le terrorisme : recommandations pour une stratégie antiterroriste mondiale » que « *les terroristes se servaient de plus en plus de l'Internet pour recruter et pour diffuser des informations et de la propagande, et qu'il fallait contrer cette tendance par une action coordonnée entre les États Membres, tout en respectant les droits de l'homme et les autres obligations au regard du droit international* »[(1)]. L'ONU se réfère à l'Union Internationale des Télécommunications, pour maintenir une politique de pacification du cyberespace.

Le rôle du conseil de sécurité pourra se révéler crucial puisqu'il régit toute question qui menace la paix et la sécurité internationales en vertu du chapitre VII de la charte des Nations Unies. Or, le terrorisme dans toutes ses formes est une de ces questions menaçantes, ce

---

(1) Rapport du secrétaire général des Nations uniessur « *l'activité de l'Organisation « S'unir contre le terrorisme* », Doc off AG NU, 60e sess, Doc NU A/60/825 (2006) au parag. 58-60.

qui peut justifier une intervention du conseil de sécurité. Le conseil a adopté à maintes reprises des résolutions qui incitent les États à se coopérer et à coordonner leurs stratégies pour faire face à ce danger. Une des résolutions du Conseil de sécurité qui dénonce le recours accru des terroristes à l'internet et exige une limitation de ce recours, fut la résolution 1624 en 2005[1]. Dans le même sens, la résolution 1963 en 2010[2] a indiqué la préoccupation du conseil de l'utilisation des terroristes « *des nouvelles technologies de l'information et de la communication, en particulier Internet, pour recruter et convaincre, ainsi que pour financer, planifier et préparer leurs actes* ». Récemment, le Conseil de sécurité a adopté, en février 2017, sa première résolution[3] pionnière sur la protection des infrastructures critiques contre les

---

(1) Rés. CS 1624, Doc. off CS NU, 2005, 5261e séance, Doc. NU S/RES/1624.

[2]Rés. CS 1963, Doc. off CS NU, 2010, 6459e séance, Doc. NU S/RES/1963.

(3) Rés. CS 2341, Doc. off CS NU, 2017, 7882e séance, Doc. NU S/RES/2341. Le conseil de sécurité a demandé à ses membres d'élaborer des « *stratégies de réduction des risques* » pour faire face aux attaques terroristes contre les infrastructures critiques et de renforcer leur coopération pour lutter contre de telles attaques. Ils doivent également prendre des « *mesures de préparation* » pour intervenir efficacement en cas d'attaque contre ces infrastructures et d'affirmer la responsabilité pénale de leurs auteurs. Les États devront aussi « *participer « activement » aux efforts de prévention, de protection, d'atténuation des effets, de préparation, d'enquête, d'intervention et de relèvement en rapport avec ces attaques* ».

attaques terroristes en sollicitantla coopération de ses membres pour lutter contre les attaques terroristes contre les infrastructures critiques. Cependant, aucune action unique ni des mesures concrètes n'ont été adoptées loin que ces résolutions.

Étant un problème transnational, les organisations internationales devraient jouer un rôle primordial dans la prise en compte d'une réglementation internationale ainsi qu'un «ordre universel »[1] du cyberespace et des menaces qui le visent afin d'adopter une stratégie universelle de cybersécurité.

B - Réaction des États

La nécessité d'une réglementation du cyberespace s'avère de plus en plus pressante en raison de l'ampleur stratégique présentée dans ce milieu. Il se voit que les menaces existantes ou potentielles dans cet espace

---

[1] World Federation of Scientists, Permanent Monitoring Panel on Information Security, affirme dans un document intitulé « *Toward a Universal Order of Cyberspace: ManagingThreatsfrom Cybercrime to Cyberwar* » durant le Sommet mondial sur la société de l'information, que les activités liées au cybercrime, cyberterrorisme et cyberguerre qui peuvent constituer une violation de la paix et la sécurité internationales doivent être régit par les organes compétents des Nations Unies et selon les règles de Droit international. Ils préconisaient que les Nations Unies et la communauté scientifique internationale examinent les scénarios, critères et les sanctions juridiques internationales qui peuvent être appliquées à ce sujet. Document WSIS-03/GENEVA/CONTR/6-E, 19 nov. 2003, p. 15.

dépassent ses avantages et ses opportunités. Cependant, l'accord sur une stratégie commune dans le cyberespace semble difficile à atteindre en raison des divergences des positions des États. La crainte d'un recul important de ses pouvoirs régaliens retardecet accord.

Certains États,comme les pays de l'Europe du Nord (Suède et Pays-Bas), considèrent le cyberespace comme un espace libreindépendant qui ne doit pas subir aucune restriction.Cette opinion écarte toute réglementation du cyberespace « *sous le motif que celui-ci et ses modes de régulation traditionnels sont particulièrement inefficaces dans le cyberespace* » c'est plutôt « *une attitude qui dénote un certain radicalisme* »[1].

D'autres opinions par contre, admettent que le cyberespace est un espace comme les autres et donc il est régi par les règles du droit international. Cependant, les règles applicables au cyberespace doivent garantir la liberté d'expression. Cet avis est partagé par les États-Unis et certains pays de l'Europe comme la France.

Une troisième position, soutenue par la Russie et la chine, insiste sur la nécessité d'une *stratégie*

---

[1] Serge Kablan et Arthur Oulaï, « *L'essence des approches du droit cyberspatial et l'opportunité de la co-régulation* », Revue générale de droit, vol. 39, n° 1, 2009, p. 48. DOI:10.7202/1026981ar.

internationale contraignante[1]. Pour se protéger des attaques éventuelles du cyberespace, ces deux paysparticulièrementont opté pour une politique qui vise à restreindre les réseaux internet en se « *dirigeant même vers des Internet nationaux* » en vue de pratiquer un contrôle étatique des « *contenants (infrastructures), les contenus (données, correspondances) et rendre leurs systèmes « étanches» au reste du réseau mondial* »[2]. Ils s'efforcent à filtrer et censurer les informations ou les sites étrangers qui, selon eux, menacent la sécurité nationale. La Russie n'utilise même pas le terme « cyberespace » dans ses textes juridiques en faveur d'une notion plus large « l'espace informationnel » pour pouvoir bien le contrôler.La chine, quant à elle, considère la cybersécurité comme une préoccupation stratégique et l'intègre comme unecomposante de sa politique militaire.

De cela, on peut conclure que les divergences dans la perception de la nature du cyberespace et du degré de son indépendance retardent un consensus international sur une stratégie universelle. Le cyberespace « *devient*

---

(1) En ce sens, voir, Michel Baud, « *Cyberguerre : En quête d'une stratégie* », Focus stratégique, n° 44, Mai 2013, p. 23.

(2) Barbara Louis-Sidney, « *La dimension juridique du cyberespace* », Revue internationale et stratégique, vol. 3, n° 87, 2012, p. 80. DOI : 10.3917/ris.087.0073.

donc à la fois le vecteur et l'objet de rivalités de pouvoir entre acteurs pour son contrôle, sa domination et la régulation de ses activités »[1]. Cette difficulté se reflète également sur la question du cyberterrorisme, l'absence de toute position commune et universelle rend le fait d'arriver à un accord ou à une stratégie globale de lutte contre le cyberterrorisme une tâche difficile presque impossible. Les États se divergent même en ce qui concerne la qualification du cyberterrorisme et les positions qui doivent être prises en la matière.

Conclusio

Le cyberespace, avec toutes ses ambiguïtés, estun domaine stratégique pour la préservation de la paix et la sécurité internationales.Étant un espace opaque et non létal, le cyberespace subit depuis quelques années une prolifération des menaces qui s'avèrent jusqu'à maintenant difficilesde les configurer, en donnant l'opportunité aux différents acteurs de s'affronter « *confrontation virtuelle (à distance)* » sans une vraie intervention physique[2].

---

[1] Frédéric Douzet, Alix Desforges et Kevin Limonier, « *Géopolitique du cyberespace : « territoire», frontières et conflits* », Fronts et frontières des sciences du territoire CIST proceedings, 2014, pp. 176- 177. HAL Id : hal-01353455.

[2] Le cyberespace a permis de mener des attaques terroristes à distance sans aucune nécessité d'intervention physique sur le territoire d'un

Le cyberterrorisme, étantune de ces menaces, est une forme développée du terrorisme classique. Il n'existe pas à nos jours une définition universelle ni pour le « terrorisme » ni pour le « cyberterrorisme ». Les États n'ont pas pu parvenir à un consensus à cet égard, rendant la tâche d'adopter une convention ou même une action internationale de plus en plus difficile. Les deux phénomènes sont d'une nature similaire, mais, ils se différent dans le champ de bataille ou le théâtre des opérations, ainsi que les tactiques et les moyens utilisés.Le cyberterrorisme estmarqué par une grande asymétrie qui consiste à refuser les règles du combat imposées par l'adversaire, rendant ainsi toutes les opérations imprévisibles »et en utilisant «de forces non prévues à cet effet ...., d'armes contre lesquels les moyens de défense ne sont pas toujours adaptés ..., de méthodes qui refusent la guerre conventionnelle .... et de l'effet de surprise[1].

Pour cela, certains dirigeants et responsables politiques admettent qu'il est presque « *impossible de prévenir les actes de cyberterrorisme, qu'ils soient*

autre État qui peut être considéré comme une violation de sa souveraineté territoriale.

[1] Barthélémy Courmont et DarkoRibnikar, *Les guerres asymétriques : conflits d'hier et d'aujourd'hui, terrorisme et nouvelles menaces*, 2e éd, Paris, Dalloz / Enjeux stratégiques, 2009, p. 41.

perpétrés par des États ou par des acteurs non étatiques »[1]. Cela n'est pas que partiellement vrai[2].

Le cyberterrorisme nous semble, après cette étude, la cybermenace la moins étudiée. Les pays se préoccupent plus du cyberespionnage et de la cybercriminalité, des cybermenaces de plus en plus en expansion. Pourtant, le cyberterrorismeprécisément a besoin de plus d'attention pour pouvoir le contourner. Même s'il s'avère qu'il est un danger éventuel, la société internationale et la plupart des pays ne sont pas bien préparés pour le défendre ou au moins s'en protéger. Le fait qu'il n'est pas arrivé,jusqu'à nos jours, des situations de cyberattaques de grande ampleur (cyberterrorisme) ne veut pas dire qu'il n'arrivera jamais. Les estimations du niveau de danger sont variées. Certains pensent que le cyberterrorisme n'est qu'une hypothèse et le vraidanger derrière réside dansl'utilisation des cyberterroristes du cyberespace pour des fins de propagande, diffusion de leur idéologie,

---

(1) Jim Lewis, « *The Role of Deterrence* », (discours, Space Security Symposium, Stimson Center, 15 novembre 2012. www.stimson.org/about/news/jimlewis-of-csis-speaks-at-stimson-on-cyber-deterrence/.

(2) Colin S. Gray, *National Security Dilemmas: Challenges & Opportunities*, 1st ed., Washington D.C., Potomac Books, 2009 , p. 62.

financement de leurs activités terroristes et recrutement des militants, etc....

Étant une menace éventuelle, qu'elle soit possible ou exagérée, le danger du cyberterrorisme n'est pas tellement écarté, au contraire, il est inévitable, réel et probable. Le recours déjà des cyberterroristes au cyberespace pour des fins qui servent leurs politiques prouve qu'il est peut-être une question de temps ou de tactique pour mener des cyberattaques terroristes. Les attentats du 11 septembre n'étaient pas prévues ou même imaginables, pourtant, ils ont sévèrement frappé la première puissance mondiale (États-Unis). En plus, si les États réussissent à restreindre le terrorisme classique dans le cadre de leur stratégie de « lutte contre le terrorisme », les terroristes vont probablement se tourner vers le cyberterrorisme, qui est, pour eux un champ de bataille à faible risque et leur présente beaucoup d'avantages. Cela sans négliger la tactique intelligente poursuivie par les terroristes en ce temps qui est le recrutement des militants cultivés, qui sont, dans la plupart des cas, des citoyens des pays occidentaux et qui ont un niveau élevé de connaissance technologique et informatique. Cela peut encourager les cyberterroristes à mener des cyberattaques organisées ou, plus dur, des

cyberattaques enchainées dans un seul État ou dans plusieurs en même temps.

Étant donné que certaines organisations terroristes semblent nourrir le désir permanent d'utiliser tous les moyens possibles, y compris les cyberattaques, pour atteindre leurs objectifs, nous force à prendre ce risque au sérieux pour ne pas se dégénérer en une vraie crise. L'interdépendance croissante des États et la mondialisation fait qu'aucun État ne peut être à l'abri de cette menace transnationale. L'idée qu'on n'a pas relevé à nos jours des cas de cyberterrorisme, à proprement dire, nous donne une opportunité et plus de temps pour bien se préparer. Les responsables politiques et militaires doivent maintenir des stratégies préventives et sécuritaires pour empêcher de tels actes et minimiser les conséquences d'une éventuelle attaque. Les mesures de rétribution font partie importante de ces actions préparatoires.

En conclusion, les menaces existantes et éventuelles exigentde la communauté internationale une redéfinition de la notion de la sécurité internationale avec l'adoption d'une « cyberstratégie » capable de confronter ces nouvelles menaces tout en redressant un « Cadre juridique universel contre le cyberterrorisme » qui

152-153, 2014, pp. 201-220. DOI 10.3917/her.152.0201. Consulté le 22 avril 2018.

* BAUD Michel, « Cyberguerre : En quête d'une stratégie »,*Focus stratégique*, n° 44, Mai 2013, pp. 1-43.

* BLIN Arnaud, *L'histoire du terrorisme de l'antiquité à Al-Qaïda*, Paris, Bayard, 2006.

* BOCKEL Jean-Marie, Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense, le Sénat, Session extraordinaire, 2011-2012.

* BORIES Clémentines, « Appréhender la cyberguerre en droit international. Quelques réflexions et mises au point », *La Revue des droits de l'homme* , vol. 6, 2014, pp. 1-13. http:// journals. openedition. org/ revdh/ 984 . DOI : 10.4000/ revdh. 984. Consulté le 10 Avril 2018.

* BROWN Davis, « A Proposal for an International Convention to regulate the use of Information Systems in Armed Conflict », *Harvard International Law Journal*, vol. 47, n° , hiver 2006, pp. 179- 221.

* CLEMENT-NOGUIER Sophia, « Sécurité du fort contre asymétrie du faible », *Revue internationale et stratégique*, vol. 3, n° 51, 2003, pp. 89-96. DOI 10.3917/ris.051.0089. Consulté le 24 février 2018.

* COLLIN Barry, « The Future of CyberTerrorism: Where the Pysical and Virtual Worlds Converge »,

11th Annual International Symposium on Criminal Justice Issues, 1996.

* COLLIN Barry, «The Future of Cyberterrorism, » *Crime and Justice International*, vol. 13, n° 2, March 1997, pp. 15–18.

* CONWAY Maura, « Terrorist "use" of the Internet and Fighting Back», *Information and Security: An International Journal*, vol. 19, 2006, pp. 9-30.

* COURMONT Barthélemy, « L'émergence de nouveaux acteurs asymétriques », *Revue internationale et stratégique*, vol. 3, n° 51, 2003, pp. 81-87. DOI 10.3917/ris.051.0081. Consulté le 20 Mars 2018.

* COURMONT Barthélémy et RIBNIKAR Darko, *Les guerres asymétriques: conflits d'hier et d'aujourd'hui, terrorisme et nouvelles menaces*, 2e éd, Paris, Dalloz / Enjeux stratégiques, 2009.

* D. KRAMER Franklin, H. STARR Stuart et K. WENTZ Larry, *Cyberpower and national security*, 1st ed., Washington D.C., D.C: National Defense University Press: Potomac Books, 2009.

* DAVIS Benjamin, « Ending the Cyber Jihadi: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber governance », *Commlaw Conspectus*, vol. 15, 2006, pp. 119-186.

* DENNING Dorothy, *A view of Cyberterrorism Five Year Later*, Readings in Internet Security: Hacking, counterhacking, and Society (K. Himma ed.), Boston, Jones and Bartlett Publishers, 2006.

* DENNING Dorothy, « Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy », *Global Problem Solving Information Technology and Tools*, December 1999, https:// nautilus. org/ global- problem- solving/ activism- hacktivism- and- cyberterrorim- the- internet- as- a- tool- for- influencing- foreign- policy- 2/. A revised version appeared in *The Computer Security Journal*, vol. XVI, n° 3, summer 2000, pp. 15-35.

* DENNING Dorothy, « Cyberterrorism », témoignage devant le Comité de surveillance du terrorisme, Commission des forces armées, Chambre des représentants des États-Unis, 2000. www. stealthiss. com/ documents/ pdf/ cyberterrorism.pdf.

* DESFORGES Alix, « Cyberterrorisme : quel périmètre ? », *IRESM*, n° 11, décembre 2011, pp. 1-7.

* DESFORGES Alix, « Les représentations du cyberespace : un outil géopolitique», *Hérodote*, vol. 1, n° 152-153, 2014, pp. 67-81. DOI 10.3917/her.152.0067. Consulté le 8 Avril 2018.

* Dictionnaire de l'Académie française, supplément, an VII, 1798.

* DOUZET Frédéric, DESFORGES Alix, LIMONIER Kevin, « Géopolitique du cyberespace : « territoire », frontières et conflits », *Fronts et frontières des sciences du territoire,* CIST proceedings, 2014, pp. 173-178. HAL Id: hal-01353455. Consulté le 2 Janvier 2018.

* DOUZET Frédérick, « La géopolitique pour comprendre le cyberespace», *Hérodote*, La Découverte, vol. 1, n° 152-153, 2e trimestre 2014, pp. 3-21. DOI: 10.3917/her.152.0003. URL : https:// www. cairn. info/ revue- herodote- 2014-1-page-3 .htm. Consulté le 2 Janvier 2018.

* E. SANGER David, *Confront and Conceal : Obama's Secret Wars and Surprising Use of American Power*, New York, Crown Publishing Group, 2012.

* FILIU Jean Pierre, 2011, « *Les dynamiques du « cyberjihad* », n°47, Paris, Questions Internationales.

* FURNELL Steven et WARREN Matthew, « Computer Hacking and Cyber terrorism : the Real Threats in the New Millenium? », *Computers and Security*, vol. 18, n° 1, 1999, pp. 28-34.

* GAYRAUD Jean-François et SENAT David , « *Le terrorisme* », coll. Que Sais-Je ?, Paris, Presses Universitaires de France, 2002.

* GHERNAOUTI-HELIE Solange, « Menaces, conflits dans le cyberespace et cyberpouvoir », *Sécurité et*

stratégie, vol. 3, n° 7, 2011, pp. 61-67. DOI 10.3917/sestr.007.0061. Consulté le 22 mars 2018.

* GIBSON William, *Neuromancien*, traduction par Jean Bonnefoy, 2editions « J'ai lu », Paris, coll. SF., 1998. (Édition américainen : Neuromancer, 1984). \

* GOZZI Marie-Hélène, Paris, Le terrorisme, Ellipses, 2003.

* HOFFMAN Bruce, *Inside Terrorism*, New York, Columbia University Press, 2006.

* IASIELLO Emilio, « Is Cyber Deterrence an Illusory Course of Action? », *Journal of Strategic Security*, vol. 7, n° 1, 2014, pp. 54-67. DOI: http:// dx. doi. org/ 10.5038/ 1944-0472.7.1.5. Disponible à l'adresse : http:// scholarcommons.usf. edu/ jss/ vol7/ iss1/ 6. Consulté le 18 Avril 2018.

* JACQUEMAIN Marc, «Terrorisme, terroriste», *Quaderni, Nouveaux mots du pouvoir : fragments d'un abécédaire*, n° 63, Printemps 2007, pp. 89-91. DOI : 10.3406/ quad. 2007. 1794. http:// www. persee. fr/ doc/ quad_ 09871381_ 2007_num_63_1_1794. Consulté le 12 mars 2018.

* JENKINS Brian, *International Terrorism: A New Kind of Warfare*, California, Rand Corporation, 1974.

* KABLAN Serge et OULAI Arthur, « L'essence des approches du droit cyberspatial et l'opportunité de la co-régulation », *Revue générale de droit*, vol. 39, n° 1,

2009, pp. 5-277. DOI:10.7202/1026981ar. Consulté le 22 février 2018.

* KANT Emmanuel, *Projet de paix perpétuelle*, Paris, Collection Mille et Une Nuits, n°327, 2001, traduction de Karin Rizet.

* KELLO Lucas, « Les cyberarmes : Dilemmes et futurs possibles », *Institut français des relations internationales (IFRI)*, Politiques étrangères, vol. 4, 2014, pp. 139-150.

* KEMPF Olivier, 2014, « Le cyberterrorisme : un discours plus qu'une réalité », *Hérodote*, La Découverte, vol. 1, n° 152-153 : 82-97. DOI: 10.3917/her.152.0082. Consulté le 12 avril 2018.

* KLEIN John, « Deterring and Dissuading Cyberterrorism », Journal of Strategic Security, vol. 8, n° 4, 2015, pp. 23-38. DOI: http: // dx. doi. org/ 10. 5038/1944-0472.8.4.1460 consultable sur : http:// scholarcommons. usf. edu/ jss/ vol8/ iss4/2. Consulté le 24 mars 2018.

* L. GROSS Michael, CANETTI Daphna et R. VASHDI Dana, «Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes », *Journal of Cybersecurity*, vol. 3, n° 1, 2017, pp. 49-58. DOI: 10.1093/cybsec/tyw018 .Consulté le 12 avril 2018.

* LEMAN-LANGLOIS Stéphane, « Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace Commercial », *Criminologie*,

vol. 39, n° 1, printemps 2006, pp. 63-81. URI: http:// id.erudit. org/ iderudit/ 013126 ar, DOI: 10.7202/013126ar. Consulté le 14 février 2018.

* LEWIS Jim, « The Role of Deterrence », (discours, Space Security Symposium, Stimson Center, 15 novembre 2012, www. stimson. org/ about/ news/ jimlewis- of- csis- speaks- at- stimson- on- cyber-deterrence/. Consulté le 18 mars 2018.

* LOUIS-SIDNEY Barbara, « La dimension juridique du cyberespace », *Revue internationale et stratégique*, vol. 3, n° 87, 2012, pp. 73-82. DOI 10.3917/ris.087.0073. Consulté le 10 Mars 2018.

M. ROCHE Edward et J. BLAINE Michael, «International Convention for the Peaceful Use of Cyberspace », *Orbis: Journal of World Affairs*, vol. 58, n° 2, Spring 2014, pp. 282-296.

* MELLON Christian, *Éthique et violence des armes*, Paris, Assas Éditions, 1995.

* MENEUT Emmanuel, « La cyberguerre et la structuration des relations internationales : Le cas Nord-Coréen», *IRIS, Asia Focus*, n° 54, Décembre 2017, pp. 1-18.PFANNER Toni, « Les guerres asymétriques vues sous l'angle du droit humanitaire et de l'action humanitaire », *Revue Internationale de la Croix-Rouge*, vol. 87, 2005, pp. 259-288.

* POLLITT Mark, « Cyberterrorism: Fact or Fancy? », *Computer Fraud and Security*, n° 2, 1998, pp. 8-10.

* RID Thomas et MCBURNEY Peter, « Cyber-Weapons », *RUSI Journal*, vol. 157, n° 1, 2012, pp. 6-13. DOI: 10.1080/03071847.2012.664354. Consulté le 17 février 2018.

* ROJINSKY Cyril, « Cyberespace et nouvelles régulations technologiques », *Dalloz*, Chron., 2001, pp. 844- 852.

* S. GRAY Colin, *National Security Dilemmas: Challenges & Opportunities*, Washington D.C., Potomac Books, 2009.

* S. NYE Joseph, «Cyber power», *Belfer Center for Science and International Affairs*, Harvard Kennedy School, 2010, pp. 1-24.

* SCHMID Alex et JONGMAN Albert, *Political Terrorism: A new guide to actors, authors, concepts, data bases, theories, and literature*, London, Transaction Publishers, 2005.

* SCHJOLBERG Stein, «Terrorism in Cyberspace – Myth or reality? », article présenté au NATO Advanced Research Workshop on Cyberterrorism, Bulgaria, Sofia (October 2006), et au International Criminal Law Network (ICLN), 4th Annual Conference: Effective Counter-Terrorism and the Rule

of International Law, The Hague, The Netherlands, December 2006.

* SIMONET Loïc, « L'usage de la force dans le cyberespace et le droit international », *Annuaire français de Droit International*, vol. 58, 2012, pp. 117-143. DOI: 10. 3406/ afdi. 2012. 4673. http:// www. persee. fr/doc/ afdi_00663085_2012_num_58_1_4673. Consulté le 2 avril 2018.

* STELLA Marie, « La menace déterritorialisée et désétatisée : le cyberconflit », *Revue internationale et stratégique*, vol. 1, n° 49, 2003, pp. 165-171. DOI 10.3917/ris.049.0165. Consulté le 22 avril 2018.

* T. KUEHL Daniel, « *From cyberspace to cyberpower: Defining the problem*», dans D. KRAMER Franklin, H. STARR Stuart et K. WENTZ Larry, «Cyberpower and National Security », Washington D.C., D.C: National Defense University Press: Potomac Books, 2009, pp. 24-42.

* THOMAS Timothy, « Al Qaeda and the Internet: the Danger of "Cyberplanning"», *Parameters*, Printemps 2003, pp. 112-123.

* TRUDEL Pierre, « Quel droit et quelle régulation dans le cyberespace ? », *Sociologie et sociétés*, vol. 32, n° 2, 2000, pp. 190-210. id.erudit.org/iderudit/001806ar; DOI:10.7202/001806ar. Consulté le 22 février 2018.

* WAHNICH Sophie, « Terreur Révolutionnaire et terrorisme », *Rémanence rétinienne et troubles de la vision*, Lignes, vol. 2, n° 8, 2002, pp. 147-167. DOI 10.3917/lignes1.008.0147. Consulté le 25 février 2018.

* WALTZER Michael, *De la Guerre et du Terrorisme*, Paris, Bayard, 2004.

* WEIMANN Gabriel, « Cyberterrorism: How Real Is the Threat? », *Studies in Conflict & Terrorism*, vol. 28, 2005, pp. 129-149. DOI: 10.1080/10576100590905110. Consulté le 15 Janvier 2018.

Rapports

* ANKEN Hans, Renforcer la coopération contre le cyberterrorisme et d'autres attaques de grande ampleur sur Internet, Rapport de la commission de la culture, de la science, de l'éducation et des médias au Conseil de l'Europe, 8 juin 2015.

* Rapport de L'Office des Nations Unies contre la drogue et le crime (ONUDC), Utilisation de l'Internet à des fins terroristes, 2014.

* Rapport du secrétaire général des Nations unies, « pour une liberté plus grande : développement, sécurité et respect des droits pour tous », Doc. A/59/2005.

* Rapport du Secrétaire général sur l'activité de l'Organisation « S'unir contre le terrorisme », A/60/825, 2006,

* Rapport du groupe d'experts gouvernementaux des Nations unies chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, UN doc, A/68/98 (24 juin 2013).

* World Federation of Scientists, Permanent Monitoring Panel on Information Securiy, affirmedansun document intitulé « Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar ». Document WSIS-03/GENEVA/CONTR/6-E, 19 nov. 2003.

* Rapport du Department of Defense Cyberspace Policy Report, " A Report to Congress Pursuant to the National Defense Authorization Act for fiscal Year 2011, Section 934, November 2011.