BANQUE DES MEMOIRES

Master de Justice pénale internationale
Dirigé par Messiers les Professeurs Julian FERNANDEZ, Olivier DE FROUVILLE, Didier REBUT
2020

L'APPLICATION DU DROIT HUMANITAIRE AUX CYBERATTAQUES COMMISES DANS LES CONFLITS ARMÉS INTERNATIONAUX

Elena Volkova

Sous la direction de Monsieur le Professeur Olivier de Frouville

Remerciements

Je tiens à remercier tous ceux qui ont contribué de près ou de loin à la réalisation de ce mémoire.

J'aimerais en tout premier lieu adresser mes très sincères remerciements aux Messiers les Professeurs Julian Fernandez, Olivier de Frouville et Didier Rebut. Je mesure l'honneur qu'ils m'ont fait en me donnant la possibilité de faire mes études à l'Université Paris 2 Panthéon-Assas — un endroit idéal pour mener une réflexion approfondie. Leurs cours ont apporté de nombreuses connaissances profondes et nécessaires à la réalisation de ce mémoire.

Je tiens à remercier sincèrement Monsieur le Professeur Olivier de Frouville, mon directeur de mémoire, pour m'avoir fait l'honneur de diriger mon mémoire, pour son profond soutien tout au long de ce travail de recherche et ses conseils toujours avisés en me laissant une grande liberté dans l'appréhension de mon travail.

Mes remerciements s'adressent en outre à mon premier professeur de droit Robin Caballero pour son aide et ses conseils précieux pendant cette année qui m'ont apporté à pousser toujours plus loin tout en préservant un esprit critique.

Enfin, j'exprime ma gratitude à ma famille, et notamment à ma mère et à mon arrière-grand-mère qui m'ont soutenu tout au long de la réalisation de ce mémoire et qui ont toujours cru en moi.

Résumé

La transformation numérique que nous connaissons aujourd'hui a conduit à l'émergence de nouvelles menaces. Les cyberattaques, dont le nombre a considérablement augmenté au cours des dernières années, constituent une des menaces les plus graves : capables de s'infiltrer dans les systèmes de défense et de paralyser les systèmes informatiques civils, les cyberopérations sont devenues une arme efficace dans les conflits armés internationaux.

Des experts techniques, spécialistes du droit international et chefs de la sécurité, préoccupés par le fait que le droit humanitaire ne prévoie pas explicitement dans ses dispositions la régulation des attaques informatiques, sont tombées d'accord sur la transposition des normes du droit humanitaire coutumier dans le cyberespace. Les règles fondamentales concernant le comportement des combattants, la protection des civils, l'exercice du droit à la légitime défense et le principe de responsabilisation ont ainsi été adaptées au cybercontexte.

Néanmoins, la mise en œuvre des normes du droit humanitaire est toujours difficile dans le monde cybernétique. Cet état de choses s'explique à la fois par le fait que les capacités techniques sont inégales pour les pays développés et les pays en développement, et par la tentative des parties au conflit de se soustraire à leur responsabilité en utilisant des outils les rendant anonymes.

Par conséquent, la communauté internationale doit agir sur le plan technique pour obtenir des preuves solides établissant un lien entre la cyberattaque et son auteur, ainsi que négocier sur le plan politique afin de canaliser les disputes liées à l'application du droit et sensibiliser les sociétés sur les dangers des cyberopérations.

Principales abréviations

al.	alinéa(s)
art.	article
CAI	conflit armé international
CANI	conflit armé non-international
CICR	Comité international de la Croix-Rouge
CIJ	Cour internationale de Justice
CPJI	Cour permanente de Justice internationale
CNRS	Centre national de la recherche scientifique
CPI	Cour pénale internationale
DIH	Droit international humanitaire
FISNUA	Force intérimaire de sécurité des Nations Unies pour Abyei
FORPRONU	Force de protection des Nations Unies
Ibid	*Ibidem*
IMTFE	International Military Tribunal for the Far East
GCSC	Global Commission on the Stability of Cyberspace
GGE	Groupe d'experts gouvernementaux
MINUAD	Mission conjointe des Nations Unies et de l'Union africaine au Darfour
MINUSIL	Mission des Nations Unies en Sierra Leone
MINUSS	Mission des Nations Unies au Soudan du Sud
MONUC	Mission de l'Organisation des Nations Unies en République démocratique du Congo
No.	Numéro
ONG	Organisation non gouvernementale
ONU	Organisation des Nations Unies
OTAN	Organisation du Traité de l'Atlantique Nord
p. (pp.)	page(s)
PA I	Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977
par. (paras)	paragraphe(s)
CS (CSNU)	Conseil de sécurité des Nations unies

SCADA	Supervisory Control And Data Acquisition (Système de contrôle et d'acquisition de données en temps réel)
SDN	Société des Nations
TIC	Technologies de l'information et de la communication
TMIEO	Tribunal militaire international pour l'Extrême-Orient
TPIR	Tribunal pénal international pour le Rwanda
TPIY	Tribunal pénal international pour l'ex-Yougoslavie
TSSL	Tribunal spécial pour la Sierra Léone
UE	Union européenne
UNICEF	Fonds des Nations Unies pour l'enfance
UNICRI	Institut interrégional de recherche des Nations Unies sur la criminalité et la justice
UNIDIR	Institut des Nations Unies pour la recherche sur le désarmement
Vol.	Volume

Sommaire

Introduction

« *Plus un jour ne se passe sans que l'on ne découvre une nouvelle campagne malveillante dans le cyberespace* »[1] a déclaré en novembre 2018 le ministre des Affaires étrangères Jean-Yves Le Drian lors de l'ouverture de Forum pour la gouvernance d'Internet dont le but est d'affronter les problèmes dans le domaine de la sécurité cybernétique.

Les avancées enregistrées sur le plan technologique ont abouti à la création de nouveaux moyens de guerre, les cyberattaques, qui dépassent les questions de la simple cybercriminalité et qui peuvent être traitées comme des « actes hostiles » malgré leur nature non cinétique[2]. À l'heure actuelle, le cyberespace lui-même peut être considéré comme un cinquième domaine d'intervention dans les affaires intérieures et extérieures d'un État après l'air, la terre, la mer et l'espace. Nonobstant sa nature virtuelle, « *il est également présent à l'intérieur de ces champs traditionnels, dès lors qu'une cyberattaque peut produire des effets non seulement dans le cyberespace, mais également sur les théâtres physiques* »[3]. Ce potentiel a été également reflété dans la nouvelle doctrine militaire de lutte informatique offensive de France de 2019 dans laquelle il a été reconnu que « *les armées doivent désormais, systématiquement, regarder le combat cybernétique comme un mode d'action à part entière dont les effets se combinent aux autres dans une manœuvre globale* »[4].

Un exemple récent démontre que l'emploi de cyberarmes lors des conflits armés devient une réalité. Le 5 mai 2019, pour la première fois dans l'histoire du conflit israélo-palestinien, le Hamas a tenté de « *perturber la qualité de vie des Israéliens* »[5] via une cyberattaque. Israël a été le premier à répondre par une attaque physique pour protéger ses citoyens. Les parties au conflit n'avaient jamais eu recours aux cyberattaques contre les civils. Jamais un État n'avait

[1] *Le Point*, « La France tente de relancer les négociations internationales sur le cyberspace », le 12 novembre 2018, URL : https://www.lepoint.fr/economie/la-france-tente-de-relancer-les-negociations-internationales-sur-le-cyberespace-12-11-2018-2270549_28.php (visité le 07/11/2019).

[2] ALLAND (Denis), CHETAIL (Vincent), DE FROUVILLE (Olivier), *Unité et diversité du droit international : écrits en l'honneur du professeur Pierre-Marie Dupuy*, Leiden, Boston, Martinus Nijhoff Publishers, 2014, p. 282.

[3] Assemblée Nationale, Commission de la Défense Nationale et des Forces Armées, Rapport d'information, le 4 juillet 2018, p. 10, URL : http://www.assemblee-nationale.fr/15/pdf/rap-info/i1141.pdf (visité le 28/11/2019).

[4] Éléments publics de doctrine militaire de lutte informatique offensive, p. 4, URL : https://www.defense.gouv.fr/content/download/551555/9394645/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf (visité le 25/11/2019).

[5] *Le Monde*, « Israël dit avoir déjoué une cyberattaque du Hamas à Gaza, avant de frapper le site d'origine », le 6 mai 2019, URL : https://www.lemonde.fr/pixels/article/2019/05/06/israel-dit-avoir-replique-a-une-attaque-informatique-par-une-frappe-aerienne-une-premiere_5459063_4408996.html (visité le 10/11/2019).

revendiqué ainsi l'emploi de la force militaire traditionnelle pour punir une cyberattaque en temps réel. L'histoire montre que le recours à la force physique afin d'empêcher une attaque dans le cyberdomaine a déjà eu lieu en 2015 : les États-Unis ont attaqué en 2015 un membre de l'État islamique, Junaid Hussain, qui a été le chef du « Cyber Caliphate ». Cependant, l'élimination de Hussein ne constituait toutefois pas une réponse immédiate à la cyberattaque, il a fallu plusieurs mois aux États-Unis pour se préparer à cette opération.

Ces observations nous laissent penser que les cyberattaques peuvent constituer la bonne « *évolution continue du droit des conflits armés et des crimes de guerre* »[6]. Les cyberopérations ont la capacité de causer les mêmes dégâts que les attaques conventionnelles : saboter le matériel militaire[7], altérer ou supprimer des informations stratégiques étatiques[8], répandre un virus dans les hôpitaux afin de provoquer la mort des personnes blessées et malades[9], priver des populations civiles d'électricité[10], provoquer le rejet des substances toxiques par des usines

[6] DE FROUVILLE (Olivier), MARTELLY (Olivia), « La juridictionnalisation du droit des conflits armés : Les tribunaux internationaux mixtes », Permanence et mutations du droit des conflits armés, Colloque, Université Lyon 3, 2-3 octobre 2008, p. 4, URL : http://www.frouville.org/Publications_files/Art-Lyon-mainDocFINAL-1.pdf (visité le 05/03/2020).

[7] « *In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace* » : The United States Department of Defense, Quadrennial Defense Review Report, p. 37, 2010, URL : https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf (visité le 13/05/2020).

[8] Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 6.

[9] Des chercheurs israéliens ont mis au point un logiciel malveillant qui permettait aux attaquants d'ajouter des tumeurs malignes réalistes dans les résultats de l'examen à la tomographie ou à l'IRM ainsi que d'effacer de véritables tumeurs cancéreuses dans les scans, ce qui conduirait à un diagnostic erroné et éventuellement à un échec du traitement des patients : *The Washington Post*, « Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists », le 3 avril 2019, URL : https://www.washingtonpost.com/gdpr-consent/?destination=%2ftechnology%2f2019%2f04%2f03%2fhospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists%2f%3futm_term%3d.de95da701f32&utm_term=.de95da701f32 (visité le 02/12/2019); Le CICR s'est également déclaré préoccupé par le fait que les cyberattaques peuvent nuire au fonctionnement d'équipement médical, tel que les stimulateurs cardiaques et les pompes à insuline, qui permettent de surveiller à distance la santé de chaque patient ainsi que le fonctionnement d'équipement médical lui-même : ICRC, Expert Meeting 14–16 november 2018 – Geneva, The potential human cost of cyber operations, mai 2019, p. 8, URL : https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf (visité le 02/12/2019) ; Pendant la pandémie de COVID-19, de nombreux hôpitaux en République Tchèque, en France, en Espagne, en Thaïlande et aux États-Unis ont été touché par des cyberattaques. Ces attaques ont forcé le personnel médical à reporter des interventions chirurgicales urgentes, à abandonner de nouveaux arrivants patients en état critique. De plus, l'hôpital à cause des cyberopérations certains établissements de soins ont retardé le traitement des tests de COVID-19 de plusieurs jours : MACAK (Kubo), RODENHÄUSER (Tilman), GISEL (Laurent), «Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections?», le 2 avril 2020, URL : https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/ (visité le 15/05/2020).

[10] La cyberattaque contre le réseau électrique ukrainien a provoqué une coupure d'électricité à Ivano-Frankivsk (Ukraine) le 23 décembre 2015. Selon des estimations provenant de diverses sources, entre 200.000 et 1,5 million des civils ont fait l'objet de ce virus : Voir, par exemple, Ukraine : *Le Figaro*, « Une cyberattaque coupe l'électricité », le 5 janvier 2016, URL : https://www.lefigaro.fr/flash-actu/2016/01/05/97001-20160105FILWWW00381-ukraine-une-cyberattaque-coupe-l-electricite.php (visité le 02/12/2019).

chimiques[11], c'est-à-dire, qu'elles sont capables d'apporter un avantage militaire au cours du conflit armé.

Nonobstant ce progrès dans le domaine des armements, les questions réglementaires des cyberopérations restent en suspens. La première difficulté à laquelle nous faisons face aujourd'hui est qu'il n'y a pas de définition commune de cyberattaque. En tout premier lieu, il faut noter que les cyberattaques qui font l'objet de notre étude sont celles qui atteignent le seuil de gravité nécessaire au sens de l'article 49 du Protocole Additionnel I et qui ont, par conséquent, pour objectif de donner un avantage sur l'adversaire. Elles se distinguent de cyberattaques qui visent à exploiter des réseaux pour recueillir illicitement des informations à des fins lucratives (par exemple, la cyberescroquerie). De plus, le Comité international de la Croix-Rouge (ci-après CICR) rappelle que des cyber-pirates sont « *considérés comme des civils et restent donc protégés par le Droit international humanitaire (ci-après le DIH) contre toute attaque directe* » même dans une situation de conflit armé, contrairement aux combattants qui utilisent les cyberames en tant que moyens de guerre[12]. Dans ce cas l'activité illicite des cyber-pirates serait régie par d'autres branches du droit.

En parlant de la définition de cyberattaque, il faut noter qu'elle est inextricablement liée à la notion de cyberespace dans la mesure où les États définissent les cyberattaques. En France le Ministère des Armées de France entend par « cyberattaque » un « *acte malveillant de piratage informatique dans le cyberspace* »[13]. D'après la Stratégie en matière de cybersécurité pour l'Allemagne, la cyberattaque, c'est « *IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security* »[14]. La définition dans la Stratégie en matière de cybersécurité de l'Autriche est identique — « *"cyber attack" refers to an attack through IT in cyber space, which is directed against one or several IT system(s)* »[15]. Alors que certains autres États ne mentionnent pas le cyberespace : « *"cyber attack" refers to deliberate*

[11] *The New York Times*, « A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try », le 15 mars 2018, URL : https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html (visité le 02/12/2019).

[12] Comité international de la Croix-Rouge, « Quelles limites le droit de la guerre impose-t-il aux cyberattaques ? », le 28 juin 2013, URL : https://www.icrc.org/fr/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm (visité le 24/01/2019).

[13] La cyberdéfense : enjeu majeur pour le ministère, le 17 octobre 2018, URL : https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation (visité le 28/11/2019).

[14] Federal Ministry of the Interior, Cyber Security Strategy for Germany, février 2011, p. 14, URL : https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (visité le 28/11/2019).

[15] Austrian Cyber Security Strategy, 2013, p. 20, URL : https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf (visité le 28/11/2019).

acts that seriously compromise national security, stability or prosperity by manipulating, denying access to, degrading or destroying computers or networks or the information resident on them »[16]. Une telle divergence des vues ne permet pas d'établir un cadre dans lequel une cyberopération doit se dérouler.

De plus, même la notion de cyberespace n'est pas comprise de la manière identique par la communauté internationale. Certains mettent sur un pied d'égalité « cyberspace » et « Internet »[17], d'autres estiment qu'Internet n'est que l'un des éléments du cyberespace[18]. La première approche restreint considérablement le champ des cyberattaques pouvant être objet de notre étude, et exclut celles qui ont été commises sans l'usage d'Internet. Par exemple, la première cyberattaque, lancée en 1982, qui a introduit un cheval de Troie dans le système de contrôle et d'acquisition de données en temps réel (ci-après le SCADA) du gazoduc transsibérien a abouti à l'explosion d'un gazoduc sans recourir à Internet. Similairement, le ver Stuxnet a infecté le SCADA utilisé pour le contrôle des centrifugeuses iraniennes d'enrichissement d'uranium en 2010.

Il convient à cet égard de recourir à la définition proposée par le CICR qui entend par « cyberattaque », ou « cyberopération »[19] les actions cybernétiques contre un réseau informatique lancées dans des infrastructures de technologies de l'information, y compris Internet, à des fins hostiles « *contre un ennemi et destinées à obtenir, altérer, détruire,*

---

[16] Australian Government, Australia's Cyber security strategy, 2016, p. 15, URL : https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf (visité le 28/11/2019).

[17] « *Cyberspace – [t]he electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 3 billion people are linked together to exchange ideas, services, and friendship* » : National Cyber Security Strategy, Canada's Vision for Security and Prosperity in the Digital Age, URL : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx (visité le 28/11/2019).

[18] « *Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks* » : Cyber Security Strategy of the United Kingdom : safety, security and resilience in cyber space, juin 2009, p. 7, URL : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (visité le 28/11/2019) ; « *Le cyberespace est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunication, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs de services en ligne* » : La cyberdéfense : enjeu majeur pour le ministère, le 17 octobre 2018, URL : https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation (visité le 28/11/2019) ; « *Le Cyberespace est l'environnement global né de l'interconnexion des systèmes d'information et de communication. Le cyberespace est plus large que le monde informatique et contient également les réseaux informatiques, systèmes informatiques, médias et données numériques, qu'ils soient physiques ou virtuels* » : Belgian National Cyber Security Strategy, le 23 novembre 2012, p. 13, URL : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en (visité le 28/11/2019) .

[19] Le CICR met sur un pied d'égalité les termes « opération » et « attaque ».

perturber ou transférer des données stockées sur un ordinateur, traitées par un ordinateur ou transmises au moyen d'un ordinateur »[20] lors d'un conflit armé.

Cependant, toute cyberattaque ne tombe pas sous le régime du droit international humanitaire. Pour le clarifier, il faut examiner les trois cyberattaques habituellement citées : celle contre l'Estonie en 2007, celle contre la Géorgie en 2008 et contre Iran en 2010[21]. Dans le premier cas, les actions de déplacement de Soldat de Bronze, monument rendant hommage aux soldats soviétiques morts aux combats durant la Seconde Guerre mondiale, mais perçu comme un symbole de l'occupation soviétique, ont provoqué un tollé en Estonie en avril 2007. Au cours des semaines qui ont suivi la nuit des émeutes, l'infrastructure numérique de l'Estonie a subi une série des « *cyberattaques visant des sites Internet des administrations publiques, des banques et des journaux nationaux* »[22]. Les conséquences de ces actions ont été minimes et, malgré la probabilité d'un scénario du péril de la vie des civils à cause des problèmes avec les lignes téléphoniques de services d'urgence, ces attaques n'ont pas été considérées comme un recours à la force[23] ou une agression armée[24]. Bien que les autorités estoniennes ont évoqué la « cyberguerre », la communauté internationale a souligné qu'il n'y avait aucun dommage physique ou de souffrance mesurable suffisante pour la qualifier comme « cyberguerre ».

Une autre cyberattaque s'est produite dans le contexte de la guerre entre la Géorgie et la Russie en août 2008 dans les régions séparatistes d'Abkhazie et d'Ossétie du Sud. Parallèlement au déploiement de ses troupes en Ossétie du Sud, la Russie a lancé des cyberattaques de type DdoS (*Distributed Denial of Service attack* – attaque par déni de service distribuée, « *technique qui utilise plusieurs dispositifs informatiques (ordinateurs ou smartphones, par exemple), tels que les bots d'un "botnet", pour provoquer un "déni de service"* [*"non-disponibilité des*

---

[20] CICR, « Guerre informatique », le 1er septembre 2011, URL : https://www.icrc.org/fr/doc/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.htm (visité le 24/01/2020).

[21] CHAN-TUNG (Ludovic), « Le droit international à l'épreuve de la cyberguerre - le cas de Stuxnet », Université Grenoble, janvier 2018, p.2, URL : https://www.researchgate.net/publication/323855978_Le_droit_international_a_l'epreuve_de_la_cyberguerre_-_le_cas_de_Stuxnet (visité le 22/01/2020).

[22] BARAT-GINIES (Oriane), FERRO (Coline), « Le cyberespace : un nouveau champ de conflictualité », *Revue géostratégique*, No. 38, le 17 avril 2016 URL : http://www.academiedegeopolitiquedeparis.com/le-cyberespace-un-nouveau-champ-de-conflictualite/ (visité le 23/09/2019).

[23] GERVAIS (Michael), « Cyber Attacks and the Laws of War », *Berkeley Journal of International Law*, 2012, p. 540, URL : https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1422&context=bjil (visité le 22/01/2020).

[24] BARAT-GINIES (Oriane), « Existe-t-il un droit international du cyberespace ? », *Hérodote*, janvier 2014, p. 210. URL : https://www.cairn.info/revue-herodote-2014-1-page-201.htm (visité le 23/09/2019).

ressources du système informatique pour leurs utilisateurs"[25]] *à une ou plusieurs cibles* »[26]), qui avaient pour but d'isoler la Géorgie[27]. En effet, l'accès aux actualités internationales et aux sites gouvernementaux de Géorgie s'en est retrouvé bloqué[28]. Cette cyberattaque est demeurée semblable à celle opérée en Estonie, et ne constitue pas une cyberguerre ou un recours à la force, dans la mesure où le degré pour qualifier la situation de guerre n'a pas été atteint. Cependant, contrairement à la cyberattaque en Estonie, celle en Géorgie a été lancée dans le cadre du conflit armé internationale, elle a pour but de faciliter les opérations physiques et c'est pourquoi elle tombe *de facto* « *sous le régime du droit des conflits armés* » d'après certains auteurs[29].

En ce qui concerne le cas de Stuxnet, il s'agissait d'un « *ver informatique conçu pour cibler les logiciels et les équipements, comprenant les systèmes SCADA (Supervisory Control and Data Acquisition) développés par Siemens Corporation* »[30]. Ce dernier est apparu en 2010 en vue d'infecter les « *ordinateurs gérant la rotation des centrifugeuses enrichissant l'uranium à Natanz* »[31] et, par conséquent, suspendre le programme nucléaire d'Iran. Pour ce faire, le Stuxnet visait à effectuer deux tâches, à savoir : modifier la vitesse de rotation des centrifugeuses pour les détruire ; et envoyer des signaux indiquant que les centrifugeuses fonctionnaient normalement. Ainsi, les opérateurs n'étaient pas avertis du problème et ne pouvaient empêcher les centrifugeuses de s'autodétruire[32]. D'après Mathew Burrows, conseiller du National Intelligence Council américain, le ver Stuxnet « *a pu, quoique pour une courte période, suspendre le programme nucléaire iranien. Il a détruit près de 1 000 centrifugeuses pour enrichir le combustible d'uranium. Selon des experts, les Iraniens, en détectant un virus et en éliminant 1 000 appareils infectés, ont été en mesure de prévenir davantage de dommages* »[33]. Cependant les opinions des experts sont divisées sur la question du statut de cette cyberattaque à savoir si elle avait atteint le degré de gravité d'une attaque armée. D'une

[25] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, p. 564.

[26] *Ibid*, p. 565.

[27] CHAN-TUNG (Ludovic), op. cit., p. 2.

[28] GERVAIS (Michael), op. cit., p. 568.

[29] BARAT-GINIES (Oriane), « Existe-t-il un droit international du cyberespace ? », op. cit., p. 206.

[30] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., p. 567.

[31] CHAN-TUNG (Ludovic), op. cit., p. 3.

[32] RICHMOND (Jeremy), « Evolving Battlefields : Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict ? », *Fordham International Law Journal*, Vol. 35, Issue 3, 20122012, p. 844, URL : https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2433&context=ilj (visité le 14/09/2019).

[33] BURROWS (Mathew), *The Future, Declassified : Megatrends That Will Undo the World Unless We Take Action*, Mann, Ivanov and Ferber Publisher, Moscow, 2015, p. 193.

part, le degré des dommages causés ne permet pas de considérer cette cyberattaque comme une agression armée[34]. D'autre part, certains experts ont considéré que le ver pouvait être couvert par le droit des conflits armés parce que « *Stuxnet a été un objectif militaire* » *et « ses conséquences ne se sont pas limitées au domaine virtuel, mais ont pénétré celui de la réalité puisque du matériel militaire – des centrifugeuses – a été détruit* »[35].

Partant, la cyberattaque doit être qualifiée d'attaque armée si elle s'exerce dans le cadre d'un conflit armé et a pour objectif de donner un avantage sur leurs adversaires[36] ou si elle a pour objectif des cibles militaires, c'est-à-dire, elles tombent sous le coup des dispositions de droit international humanitaire « *lorsqu'elles sont utilisées comme moyens et méthodes de guerre dans le contexte d'un conflit armé, tel que défini par le DIH* »[37]. Le Groupe international d'experts a confirmé cette approche dans le Manuel de Tallinn, où les aspects les plus cruciaux du droit international ont été transposés aux activités dans le cyberespace. Ce groupe a convenu que « *tout recours à la force blessant ou tuant des personnes, ou endommageant ou détruisant des biens satisferait aux exigences en matière de portée et d'effets. Ils ont également convenu que les actes de collecte de cyber-renseignement ainsi que les cyberopérations impliquant une brève ou périodique interruption de services cybernétiques non essentiels, ne constituent pas des attaques armées* »[38].

L'augmentation du niveau de menace posée par l'utilisation des cyberarmes s'accompagne de la complexité de l'attribution de la responsabilité. D'une part, ce problème est provoqué, par l'absence de compétences techniques nécessaires pour identifier le responsable par des instances juridiques. Dans le cadre des cyberopérations l'anonymat est la règle plutôt que l'exception. Il est dès lors impossible, dans la plupart des cas, de suivre la trace de leurs auteurs.

D'autre part, l'absence d'une réponse internationale homogène concernant les modalités d'application des normes du droit reste la pierre d'achoppement dans ce domaine : en effet, ni les Conventions de Genève ni le Statut de Rome ne mentionnent explicitement les

[34] Cette position a été appuyée par les experts de Manuel de Tallinn et le Conseil de Sécurité des Nations Unies.
[35] CHAN-TUNG (Ludovic), op. cit., p. 3.
[36] LIN (Herbert), «Cyber conflict and international humanitarian law », *International Review of Red Cross,* Vol. 94, No. 886, 2012, p. 515, URL : https://e-brief.icrc.org/wp-content/uploads/2016/09/29.-Cyber-conflict-and-international-humanitarian-law.pdf (visité le 26/10/2019).
[37] CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », Rapport, XXXIIème Conférence internationale de la Croix-Rouge et du Croissant-Rouge, 8-10 décembre 2015, Genève, Suisse, p.47, URL: https://www.icrc.org/fr/download/file/15110/32ic-report-on-ihl-and-challenges-of-armed-conflicts-fre.pdf (visité le 02/12/2019).
[38] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 71, par. 8, p. 341.

cyberopérations. Bien que la communauté mondiale reconnaisse que le droit international est applicable aux cyberattaques, y compris l'ONU[39] et le CICR[40], l'absence des documents spécialisés comme ceux qui déjà existent dans le domaine de cybercriminalité[41] entrave l'application des normes du droit international humanitaire. L'importance de ce problème a également été soulignée en février 2018 par le Secrétaire général des Nations Unies Antonio Guterres qui a exhorté les acteurs mondiaux à la Conférence de Munich sur la sécurité à réfléchir sur le fondement juridique de la régulation des conflits menés avec des cyberattaques[42]. La problématique de ce mémoire porte donc sur la question centrale suivante:

Dans quelle mesure le droit international humanitaire contemporain est-il applicable aux cyberattaques ?

Le présent mémoire a pour but d'examiner des caractéristiques et spécificités des conflits armés internationaux dans lesquelles les parties recourent aux cyberattaques comme aux moyens de guerre et montrer à quel point le droit humanitaire est capable de donner une réponse adéquate à des défis d'aujourd'hui. Par conséquent, nous nous concentrerons en premier lieu sur les règles qui peuvent être appliquées (Partie 1), afin de traiter des points essentiels liés au contrôle de la mise en œuvre ces règles afin d'assurer le respect du DIH sur le champ de bataille (Partie 2).

[39] Assemblée générale, Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, par. 24, le 22 juillet 2015, URL : https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&Lang=F (visité le 30/11/2019).

[40] Le CICR a indiqué que, quelles que soient la nature et la nouveauté de la méthode et du moyen utilisé dans les guerres, y compris dans le cyberspace, il faut respecter les principes généraux et les règles du DIH : CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », op. cit., p.48.

[41] Voir, par exemple, Convention de Budapest sur la cybercriminalité du 23 novembre 2001.

[42] GUTERRES (António), « La multiplication des conflits a aggravé l'insécurité mondiale », le 16 février 2018, URL : https://news.un.org/fr/story/2018/02/1005952 (visité le 29/09/2019).

PARTIE I — LES RÈGLES DU DIH APPLICABLES AUX CYBERATTAQUES

L'histoire de l'humanité c'est aussi l'histoire des conflits. Le code Lieber constitue la première tentative de codification du droit de la guerre. Adopté en 1863, pendant la guerre civile des États-Unis, par le juriste Francis Lieber, le code Lieber a essayé de réglementer la conduite des troupes en temps de guerre et est devenu le « *précurseur* » de la Convention de Genève de 1864. C'est cette dernière qui a joué un rôle central dans l'élaboration de normes en les imposant à la communauté internationale grâce aux efforts d'Henri Dunant. Avec l'évolution des armes, les lois de la guerre n'ont cessé de progresser, en créant une nouvelle branche du droit, le droit international humanitaire. Également appelé « droit des conflits armés », il réglemente la conduite des hostilités pour limiter les effets des conflits armés et protéger les personnes qui ne participent pas aux hostilités.

Aujourd'hui, le droit international humanitaire comprend les quatre Conventions de Genève de 1949 et les deux Protocoles Additionnels de 1977. En plus de ces documents établissant les règles pour les conflits armés internationaux et non internationaux, le DIH est complété par les règles d'origines coutumières. En effet, certaines des normes établies pour les conflits armés, par exemple, lors de la Conférence de La Haye de 1907, sont devenues coutumières après avoir passé l'épreuve du temps. Elles sont obligatoires pour les États et les belligérants, même si ces derniers n'ont pas adopté ces règles. C'est le cas des Conventions de Genève, mais aussi d'autres traités entrent également dans cette catégorie de coutume internationale.

L'apparition d'un nouveau champ bataille dans le domaine numérique et l'augmentation des cyberattaques a fait réfléchir les milieux universitaires et les praticiens du droit à la façon dont ces normes juridiques, dont la plupart a été élaboré à une époque où les cyberattaques étaient inconcevables, peuvent couvrir ces actes hostiles.

À première vue, le recours aux cyberattaques dans les conflits armés internationaux n'est pas expressément interdit par les lois de la guerre, sous réserve du respect des principes fondamentaux qui sont au cœur de l'ensemble des dispositions relatives à la conduite des hostilités, même si elles se produisent dans le cyberespace. Cependant, avant que nous examinions l'applicabilité de ces principes (Chapitre 2), il faut tout d'abord comprendre les caractéristiques particulières d'un conflit armé international dans lequel des parties au conflit recourent aux cyberarmes (Chapitre 1).

Chapitre 1 – La cyberattaque dans différents contextes d'un conflit armé international

Le combattant d'aujourd'hui possède un grand arsenal d'armes « classiques » et d'armes nouvelles, telles que les cyberattaques. Cependant, le droit international humanitaire, comme il ressort de sa définition, ne s'applique qu'au nombre limité de situations où les belligérants utilisent ces armes : les situations de conflits armés. L'histoire et l'expérience des dernières années montrent que le conflit armé international qui nous intéresse ici se déroule de plus en plus avec des cyberarmes. À cet égard, il est donc important de déterminer la façon dont les spécificités des conflits accompagnés des cyberattaques influent sur l'application du droit des conflits armés (Section 1) et si elles peuvent entraîner un CAI en devenant un acte déclencheur (Section 2).

Section 1 – La caractéristique d'un conflit armé international mené avec des cyberattaques

Le droit international humanitaire distingue deux types de conflits armés internationaux : le conflit armé non-international entre les forces militaires d'un État, et un ou plusieurs groupes armés non-étatiques, ou entre tels groupes, et le conflit armé international dans lequel deux ou plusieurs États s'opposent les uns aux autres. Dans notre étude, nous nous focaliserons sur le deuxième type de conflit parce que les cyberattaques les plus dommageables aujourd'hui ont été lancées pendant les conflits entre les États.

La position des experts du Manuel de Tallinn en ce qui concerne l'applicabilité du DIH aux cyberattaques dans les conflits armés peut sembler assz claire[43] :

> **RÈGLE 80 — Applicabilité du droit des conflits armés**
>
> Les cyberopérations exécutées dans le contexte d'un conflit armé sont soumises au droit des conflits armés.

Cependant tous les conflits ne constituent pas un conflit armé international au sens du droit humanitaire, surtout si les parties au conflit recourent aux cyberattaques, comme nous le verrons. En effet, le Professeur Olivier de Frouville souligne qu'il existe trois situations qui peuvent être classées dans la catégorie du CAI : la guerre déclarée entre des États, la lutte contre l'apartheid et la

[43] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 80, p. 375.

décolonisation et, finalement, l'occupation[44]. La Convention de Genève pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne de 1949 (ci-après la Convention de Genève I) donne une précision à ce sujet en soulignant que les règles du droit humanitaire s'appliquent « *en cas de guerre déclarée ou de tout autre conflit armé surgissant entre deux ou plusieurs des Hautes Parties contractantes* »[45]. La déclaration d'une guerre représente l'évidence la plus prudente, la plus simple et la plus rare de l'existence d'un conflit parce que les parties au conflit ont de plus en plus tendance à nier l'état de guerre. C'est pour cette raison que les membres de la Conférence internationale de la Croix-Rouge de 1938 ont reconnu à l'unanimité que « *la Convention de Genève devait s'appliquer à tous les cas d'hostilités, qu'ils soient ou non précédés d'une déclaration de guerre* »[46].

La deuxième situation nous renvoie aux guerres de libération nationale « *contre la domination coloniale et l'occupation étrangère et contre les régimes racistes dans l'exercice du droit des peuples à disposer d'eux-mêmes* »[47] dont le caractère international n'a été reconnu que dans le Protocole additionnel I en 1977.

Finalement, l'état d'occupation dans lequel le territoire « *se trouve placé de fait sous l'autorité de l'armée ennemie* »[48] conduit également à l'application du droit international humanitaire dans le contexte d'un conflit armé international. Bien qu'il n'y ait pas de notion juridique de l'occupation du cyberspace, les cyberarmes peuvent être utilisées pour maintenir le régime créé par la puissance occupante et, à l'inverse, le gouvernement d'occupation peut lancer des cyberopérations qui seront capables de perturber ou de dégrader les systèmes informatiques utilisés par une puissance occupante pour maintenir son autorité[49].

Toutefois, au-delà de la présence de deux États ou plus, le conflit armé international se distingue de celui non-international par l'absence de seuil de violence nécessaire pour l'application du DIH. Les Commentaires sur les Conventions de Genève de 1949 confirment que « *tout désaccord*

---

[44] DE FROUVILLE (Olivier), *Droit international pénal : sources, incriminations, responsabilité*, Pedone, 2012, p. 204.

[45] CG (I), art. 2.

[46] Conférence préliminaire des Sociétés Nationales de la Croix-Rouge pour l'étude des Conventions et de divers problèmes ayant trait à la Croix-Rouge, Genève, 26 juillet — 3 août 1946 : procès-verbaux, Volume II, Séance de la Commission I, Révision de la Convention de Genève et des dispositions connexes, samedi 27 juillet – jeudi 1er août 1946, allocution de Jean Pictet, p. 4, cité dans GRIGNON (Julia), *L'applicabilité temporelle du droit international humanitaire*, Schulthess, Genève, 2014, p. 37.

[47] PA (I), art. 1, par. 4.

[48] Règlement de La Haye de 1907, art. 42.

[49] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., par.3, pp. 543-544.

survenant entre les deux États et entraînant l'action des forces armées est un conflit armé au sens de l'article 2, même si l'une des parties nie l'existence d'un état de guerre. Peu importe la durée du conflit ou le nombre de victimes »[50]. Pour la première fois cette définition a été confirmée dans l'arrêt *Tadic* rendu en 1995 par le Tribunal pénal international pour l'ex-Yougoslavie (ci-après TPIY) :

> « *[N]ous estimons qu'un conflit armé existe chaque fois qu'il y a recours à la force armée entre États (…). Le droit international humanitaire s'applique dès l'ouverture de ces conflits armés et s'étend au-delà de la cessation des hostilités jusqu'à la conclusion générale de la paix* »[51].

La France, compte tenu de la position de la jurisprudence et des Conventions de Genève, élargit le champ d'application de cette règle et englobe le cyberespace : « *des cyberopérations constitutives d'hostilités entre deux ou plusieurs États peuvent caractériser l'existence d'un conflit armé international* »[52]. Enfin, le raisonnement des experts du Manuel de Tallinn va dans le même sens : « *Un conflit armé international existe chaque fois qu'il y a des hostilités, qui peuvent inclure ou se limiter à des cyberopérations, entre deux ou plusieurs États* »[53].

Nous voyons que tout conflit armé international nécessite deux conditions cumulatives : l'existence d'élément international représenté au moins par les deux États-parties à un conflit et l'existence des hostilités entre ces États.

En ce qui concerne le premier élément, il est indispensable de souligner que la participation d'un État n'a pas besoin d'être directe. Dans l'affaire *Tadić* le TPIY a reconnu le conflit armé international peut exister si « *les troupes d'un autre État interviennent dans le conflit ou encore, si certains participants au conflit armé interne agissent au nom de cet autre État* »[54].

Cette précision devient cruciale dans le cybercontexte où les cyberterroristes, les hacktivistes, les cyberpatriotes et les groupes de hackers contrôlés par un État peuvent coexister sur un même territoire et être auteurs d'une cyberattaque. En effet, le pourcentage approximatif actuel de l'activité de ces acteurs obtenu par l'analyse des 490 cyberattaques est la suivante:

---

[50] PICTET (Jean), Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, ICRC, Geneva, 1952, p. 32.

[51] TPIY, *Le Procureur c. Duško Tadić*, Chambre d'Appel, Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, le 2 octobre 1995, par. 70.

[52] Délégation à l'information et à la communication de la défense, Droit international appliqué aux opérations dans le cyberespace, p. 12, URL : https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf (visité le 10/01/2020).

[53] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 82, par. 8, p. 379.

[54] TPIY, *Le Procureur c. Duško Tadić*, Chambre d'Appel, Arrêt, le 15 juillet 1999, par. 84.

49 % des attaques sponsorisées par des États, 26 % ont été commis par hacktivistes, 5 % par terroristes et 20 % par d'autres groupes[55]. La situation s'aggrave parce que « *la rapidité et l'anonymat des cyberattaques rendent difficile la distinction entre les actions* [de ces acteurs] »[56] et en fait « *au tout début d'une attaque, il peut être impossible de préciser si le pirate informatique est parrainé par un État, s'il est autonome ou s'il est membre d'un groupe malveillant ou criminel* »[57].

Considérons, tout d'abord, la distinction entre ces groupes. Les organisations terroristes telles qu'Al-Qaïda et Daech peuvent être représentées également par des cyberterroristes parce qu'elles n'hésitent pas à recourir aux cybertechnologies afin d'atteindre leurs objectifs, à savoir « *lancer des campagnes de recrutement, de radicalisation et de promotion basées sur l'apologie de crimes et d'actes terroristes* »[58] à travers les outils d'Internet ou même lancer des cyberttaques comme en atteste l'activité du Cyber-Califat. Nous pouvons citer à titre d'exemple l'attentat dans l'église de Saint-Etienne-du-Rouvray commis par Adel Kermiche qui tenait un journal propagandiste pour 200 personnes sur Telegram avant l'attaque[59]. La question est de savoir si le DIH peut être applicable aux cyberattaques commises par des terroristes ? Dans le rapport de 2015 le CICR a clarifié cet aspect. En tout premier lieu, le Comité souligne que les régimes normatifs régissant les conflits armés et le terrorisme « *demeurent fondamentalement différents* »[60], bien que le droit humanitaire interdise « *expressément la plupart des actes qualifiés de "terroristes"* »[61], parce que certaines situations terroristes « *peuvent être qualifiées de conflit armé international, d'autres de conflit armé non international, tandis que de nombreux actes de violence n'entrent dans aucune catégorie de conflit armé faute de satisfaire*

[55] Verint, Thales, *The Cyberthreat Handbook*, octobre 2019, p.6, URL : https://thalesgroup-myfeed.com/THECYBERTHREATHANDBOOK (visité le 24/03/2020).

[56] White House, The national strategy to secure cyberspace, février 2003, p. 9, URL : https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf (visité le 18/03/2020).

[57] GENDRON (Angela), RUDNER (Martin), « Évaluation des cybermenaces pesant contre les infrastructures du Canada », Rapport préparé pour le service canadien du renseignement de sécurité, mars 2012, p. 26, URL : https://www.canada.ca/content/dam/csis-scrs/documents/publications/CyberTrheats_AO_Booklet_FRA.pdf (visité le 18/03/2020).

[58] LABORDE (Françoise), « Intensifier la lutte contre le cyberterrorisme sur les réseaux sociaux », 15e législature, 2017, URL : https://www.senat.fr/questions/base/2017/qSEQ170800939.html (visité le 18/03/2020) ; Voir aussi HECKER (Marc), TENENBAUM (Élie), « Quel avenir pour le djihadisme ? Al-Qaïda et. Daech après le califat », *Focus stratégique*, No. 87, Ifri, janvier 2019, pp. 74-75, URL : https://www.ifri.org/sites/default/files/atoms/files/fs87_hecker_tenenbaum.pdf (visité le 18/03/2020).

[59] *The Huffington Post*, «Pourquoi l'appli Telegram, utilisée par Adel Kermiche pour annoncer son attentat, échappe toujours à la surveillance», le 28 juillet 2016, URL : https://www.huffingtonpost.fr/2016/07/28/telegram-messagerie-adel-kermiche-eglise-attentat-saint-etienne-du-rouvray_n_11239130.html (visité le 24/03/2020).

[60] CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », 2015, op. cit., p. 22.

[61] *Ibid.*

au critère du lien »[62]. Deuxièmement, en ce qui concerne les groupes terroristes concrets, le CICR indique clairement dans son rapport que les actes d'Al-Qaida ou de l'État islamique ne représentent pas un conflit armé d'ampleur mondiale en cours [63] : ni Al-Qaida ni l'État islamique avec leurs groupes associés dans d'autres régions du monde ne sont partie unique au sens du DIH[64] et, en outre, le DIH ne s'applique pas au-delà du territoire des parties au conflit et « *les critères de l'intensité et du degré d'organisation constitutive d'un conflit armé non international au sens du DIH devraient être remplis sur le territoire de chaque État tiers pour déclencher l'applicabilité du DIH* »[65] ce qui n'est pas le cas de plupart pays touchés par des actes d'Al-Qaida ou de l'État islamique. Un autre exemple : le conflit entre la Syrie et l'État islamique dans lequel le DIH s'applique, mais seulement dans le cadre des CANI [66] ce qui n'entre pas dans le cadre de la présente étude. Ainsi, le conflit mené avec des cyberattaques serait qualifié de conflit international seulement si les groupes terroristes étaient contrôlés par un État, ce qui sera examiné plus loin.

Le terme « hacktivistes » entend un groupe des personnes qui « *ciblent des infrastructures essentielles* [ce qui] *pourrait présenter une menace indéniable pour la sécurité nationale*»[67] dans le but de favoriser des changements politiques ou sociaux et qui « *n'utilisent aucune structure hiérarchique et qui fonctionnent de façon itérative* »[68]. Un de ces mouvements est *Anonymous*, qui a participé au conflit entre les Philippines et la Malaisie. En février 2013 les tensions entre les deux États sur le statut du Sabah [69] ont reçu une nouvelle impulsion avec l'apparition des forces armées en Malaisie. Mais, quelques semaines plus tard, le conflit s'est poursuivi dans le cyberespace. Les hacktivistes d'Anonymous ont hacké les sites gouvernementaux des deux États et ont appelé au cessez-le-feu en assumant un rôle de conciliateur : « *Well, its time for us to PEACE and stop attacking each other. To end up this*

[62] CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », 2015, op. cit., p. 24.
[63] *Ibid.*
[64] *Ibid.*
[65] *Ibid.*
[66] SASSOLI (Marco), «Le droit international humanitaire mis à mal en Syrie», *Plaidoyer*, No. 2, 2017, p. 4, URL : https://archive-ouverte.unige.ch/unige:93489 (visité le 02/04/2020).
[67] GENDRON (Angela), RUDNER (Martin), « Évaluation des cybermenaces pesant contre les infrastructures du Canada », op. cit., p. 36.
[68] *Ibid*, p. 26.
[69] Les racines du conflit se trouvent dans l'accord entre le sultanat de Sulu et les représentants de la British North Borneo Company qui a donné le droit à ce dernier de céder ou louer le Nord-Bornéo (territoire de Sabah). En 1963 le Sabah a fait partie du territoire de la Fédération de Malaisie en exerçant son droit à l'autodétermination. Pourtant, les Philippines qui se considèrent comme successeur du Sultanat de Sulu affirment toujours leurs revendications territoriales sur Sabah et invoquent que le territoire n'a été que loué à la British North Borneo Company, mais la souveraineté du Sultanat sur le territoire n'ayant jamais été cédé.

way, this is our last defacement and from now on none of us will step or touch ur (sic) country site and none of you are able to touch our country site »[70]. Un autre exemple, le groupe d'hacktivistes brésiliens Pryzraky Group qui a commis des cyberattaques contre plusieurs États : en janvier 2019 contre l'agence gouvernementale NASA des États-Unis, en février-mars 2019 contre les sites gouvernementaux de Soudan (la Chambre de commerce soudanaise, le Ministère du Pétrole et du Gaz, le Ministère de l'Intérieur et le Bureau de la présidence) afin de renverser le régime d'Omar el-Bechir, en mars 2019 contre le gouvernement du Nicaragua pour soutenir des mouvements de protestation dans ce pays[71]. Cependant aucune de ces attaques n'a provoqué un conflit international parce que les groupes d'hacktivistes ne sont pas sous le contrôle étatique, même le groupe brésilien Pryzraky Group.

La motivation des cyberpatriotes est tout à fait différente. En tant que personnes physiques, ils se considèrent comme des soldats irréguliers qui mènent une guerre contre un « ennemi » afin de sauver l'honneur national contre une menace perçue en formant une sorte de cyber-milice volontaire et agissant là où l'État ne veut pas ou ne peut pas agir[72] « *soit par manque d'expertise technique ou par manque de volonté politique* »[73]. Le conflit israélo-palestinien est un bon exemple d'activités d'hackers patriotes. Dès le début de la deuxième Intifada (2000-2005), marquée par le soulèvement des Palestiniens à la suite d'une visite d'Ariel Sharon au Mont du Temple et du meurtre de trois soldats israéliens, des hackers israéliens et palestiniens ont lancé une série d'attaques DoS et DDoS dont les cibles principales étaient des sites gouvernementaux et militaires des deux parties[74]. Il est indispensable de noter que les actions des cyberpatriotes possédant les compétences requises peuvent devenir l'acte déclencheur d'un conflit et entraîner un véritable conflit armé dans le monde physique avec des effets néfastes réels, en particulier, dans des situations déjà instables. Mais il est également possible que ces groupes soient un voile qui recouvre les vrais protagonistes du conflit, les États, en offrant à ces pays la possibilité de nier la responsabilité dans le futur.

[70] *The Hacker News*, «Philippines-Malaysia Cyber war over Sabah land dispute», le 4 mars 2013, URL : https://thehackernews.com/2013/03/philippines-malaysia-cyber-war-over.html (visité le 03/04/2020).

[71] Verint, Thales, *The Cyberthreat Handbook*, op. cit., p.141.

[72] DAHAN (Michael), «Hacking for the homeland: Patriotic hackers versus hacktivists», in: HART (Doug), ICIW 2013 8th International Conference on Information Warfare and Security, Denver, Colorado, USA, 2013, p. 51.

[73] *Ibid*, p. 56.

[74] *Ibid*, p. 54.

L'État est l'acteur non seulement le plus actif dans le cyberespace (les attaques commises par des structures étatiques représentent entre 42 %[75] et 49 %[76] du nombre total des cyberattaques), mais également le plus puissant : « *Les intrusions des États-nations sont parmi les plus difficiles à contrecarrer, car elles disposent de ressources considérables, d'une connaissance des exploits potentiels du jour zéro et de la patience pour planifier et exécuter des opérations* »[77]. Une autre caractéristique qui distingue les hackers étatiques des cyberpatriotes est qu'ils sont sous le contrôlé d'un État qui, à son tour, peut leur donner des instructions, alors que les patriotes commettent des cyberattaques de leur propre initiative.

L'analyse des cyberattaques étatiques montre qu'il existe deux types de hackers contrôlés par les forces gouvernementales. D'une part, nous pouvons voir le secteur privé ou les personnes qui ont été embauchés par un État : nous pouvons citer à titre d'exemple le plan de 2009 proposé par Obama qui prévoyait la création des partenariats public-privé pour faciliter le partage d'informations sur les cyberincidents et coordonner les efforts pour « *détecter, prévenir et répondre aux incidents de cybersécurité importants* »[78]. Les documents, y compris la cyberstratégie des États-Unis, actualisés en permanence et les initiatives législatives visant à créer et établir un cadre de coopération et de coordination entre le secteur privé et public[79], montrent un intérêt constant pour les États-Unis en ce qui concerne la collaboration avec des structures privées.[80]. D'autre part, il y a des hackers qui font partie de l'armée nationale comme en témoigne l'exemple des Unités 61398 et 61486 de l'Armée populaire de libération de la Chine qui comprend des centaines de hackers[81] qui sont considérés, en particulier, comme responsables des cyberattaques contre des industries américaines de l'énergie nucléaire, des métaux et des industries solaires[82]. La France, à son tour, également dispose d'une équipe de

[75] Verint, Thales, *The Cyberthreat Handbook*, op. cit., p.6.

[76] Radware, « A Higher Percentage of Companies Say They've Been Targeted By Nation-State Hackers, Radware Survey Finds », le 14 janvier 2020, URL : https://www.radware.com/newsevents/pressreleases/2020/global-application-network-security-report (visité le 06/04/2020).

[77] Radware, Global Application & Network Security Report 2019-2020, 2020, p.11, URL : https://www.radware.com/ert-report-2020/ (visité le 06/04/2020).

[78] White House, Cyber space policy review : Assuring a Trusted and Resilient Information and Communications Infrastructure, p. 23, URL : https://fas.org/irp/eprint/cyber-review.pdf (visité le 04/04/2020).

[79] Voir, par exemple, Cybersecurity Enhancement Act of 2014 (S.1353) proposé par sénateurs Rockefeller et Thune, URL : https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf (visité le 06/04/2020).

[80] LOBEL (Hannah), «Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict», *Texas International Law Journal*, Vol. 47, Issue 3, p. 634, URL : https://heinonline.org/HOL/LandingPage?handle=hein.journals/tilj47&div=28&id=&page= (visité le 04/04/2020).

[81] STEYL (Matthew), Cybersecurity and Rising China: Analysis of Policy Proposals, Curriculum in Global Studies, University of North Carolina at Chapel Hill, 2014, p. 2, URL : https://cdr.lib.unc.edu/concern/honors_theses/vt150p11z (visité le 04/04/2020).

[82] U.S. District Court, Western District of Pennsylvannia, *United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui*, Grand Jury, Indictment, May 1 2014, p. 6.

« combattants cyber » qui ne cesse d'augmenter. En effet, la loi de programmation militaire 2019-2025 prévoit un recrutement de 1500 de personnes supplémentaires visant à porter à 4000 le nombre de personnels en total sein du Ministère des Armées d'ici à 2025 et une augmentation significative des moyens alloués à la cyberdéfense[83].

Cependant, dans la pratique les choses ne sont pas aussi simples. L'exemple de la cyberattaque contre l'Estonie en 2007 que nous avons déjà traité illustre la complexité d'établir une liaison avec le gouvernement russe. D'une part, l'Estonie, en la personne d'Urmas Paet, ministre estonien des Affaires étrangères à l'époque, a accusé la Russie d'implication directe dans les cyberattaques de 2007[84] : « *IP addresses have helped to identify that the cyber terrorists' attacks against the Internet pages of Estonian government agencies and the Office of the President have originated from specific computers and persons in Russian government agencies, including the administration of the President of the Russian Federation* »[85]. D'autre part, le mouvement politique Nachis a plaidé coupable de cette cyberattaque et a reconnu que « *c'était un acte de désobéissance civile, absolument légal* »[86] qui s'est inséré parfaitement dans leur lutte contre le déplacement d'un soldat de bronze[87]. Ces conclusions permettent de dire que la responsabilité incombe au groupe et pas à l'État. Cependant, un autre aspect tout aussi important de cette histoire est le fait que le mouvement a été créé par l'administration du Président de la Fédération de Russie afin d'appuyer les autorités russes[88]. De plus, pour quelle raisonles hackers patriotes ont-ils lancé des cyberattaques en utilisant les adresses IP gouvernementales et en piégeant le gouvernement russe si les hackers ne s'inquiétaient pas vraiment de leur responsabilité? Dans le paragraphe qui suit, nous examinerons les critères et

[83] Loi no. 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, par. 3.1.3.4, URL : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037192797&categorieLien=id (visité le 12/05/2020).

[84] WĘGLIŃSKI (Konrad), «Cyberwarfare and responsibility of states», *Torun International Studies*, No. 1 (9), février 2017, p. 80, URL : https://www.researchgate.net/publication/316838873_CYBERWARFARE_AND_RESPONSIBILITY_OF_STATES (visité le 01/04/2020).

[85] Declaration of the Minister of Foreign Affairs of the Republic of Estonia, le 1er mai, URL : https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia (visité le 07/04/2020).

[86] *Reuters*, «Kremlin loyalist says launched Estonia cyber-attack», le 11 mars 2019, https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313 (visité le 28/03/2020).

[87] LASNIER (Virginie), « Le mouvement de jeunes "nachi" ou une progéniture de la démocratie dirigée russe (2005-2009) », mémoire, Université du Québec à Montréal, octobre 2009, p.99, URL : https://archipel.uqam.ca/2460/1/M11085.pdf (visité le 03/04/2020).

[88] *Lenta*, « "Идущие вместе" наступили на грабли », 24 février 2005, URL : https://lenta.ru/articles/2005/02/23/young/ (visité le 03/04/2020) ; Voir aussi LASNIER (Virginie), «Le mouvement de jeunes « nachi » ou une progéniture de la démocratie dirigée russe (2005-2009)», op. cit., p. 44.

les conditions requises pour établir la liaison entre les groupes non-étatiques et l'État pour déterminer le rôle de chacun dans un conflit armé international.

Confirmée par la Cour pénale internationale (ci-après CPI) dans l'affaire *Ntaganda*[89], la jurisprudence fixe les conditions de contrôle par un État des troupes agissant en son nom. Ces conditions figurent dans le « *overall control* » test et prévoient qu'un État étranger « *joue un rôle dans l'organisation, la coordination ou la planification des actions militaires du groupe militaire, en plus de le financer, l'entraîner, l'équiper ou lui apporter son soutien opérationnel* »[90]. Ainsi, si un État exerce ce « *contrôle global* » sur un groupe organisé de hackers qui lance une cyberattaque contre un autre État, un conflit armé doit être qualifié d'« *international* ».

Un autre élément nécessaire pour que le conflit soit considéré comme « *armé* » — l'existence des hostilités. Les Commentaires de Conventions de Genève les définissent comme « *les actes qui, par leur nature et leur but, sont destinés à frapper concrètement le personnel et le matériel des forces armées* »[91]. Ainsi, le recrutement, la formation des hackers et les autres facteurs qui affectent l'efficacité d'une cyberattaque ne sont pas considérés comme hostilités parce qu'ils ne frappent pas directement l'adversaire. Cette conclusion reflète la position de la Cour internationale de Justice dans l'affaire *Nicaragua c. États-Unis* de 1986[92]. De plus, dans cet esprit il est nécessaire de souligner que le cyberespionnage ne fait pas partie d'hostilités au sens du DIH. On entend par les activités d'espionnage tout acte commis clandestinement ou sous de faux prétextes qui utilise les cybercapacités pour se rassembler, ou tenter de recueillir des informations[93]. Tout comme espionnage « classique », le cyberespionnage est licite au sens du droit international et droit international humanitaire[94]. D'après les experts du Manuel de Tallinn, la seule chose qui pourrait violer les DIH, c'est le moyen utilisé pour le cyberespionnage qui rendrait le cyberespionnage illégal. Par exemple, l'opération de cyberespionnage serait illicite si l'espion piraterait l'infrastructure cybernétique d'un

[89] CPI, *Le Procureur c. Bosco Ntaganda*, Chambre de première instance VI, Jugement, le 8 juillet, par. 726.
[90] *Ibid*, par. 727.
[91] CICR, Les Commentaires sur Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux de 1977, 1987, l'article 51, par. 1942.
[92] « *Selon la Cour, si le fait d'armer et d'entraîner les contras peut assurément être considéré comme impliquant l'emploi de la force contre le Nicaragua, il n'en va pas forcément de même pour toutes les formes d'assistance du Gouvernement des États-Unis. La Cour considère, en particulier, que le simple envoi de fonds aux contras, s'il constitue a coup sûr un acte d'intervention dans les affaires intérieures du Nicaragua, comme il sera expliqué plus loin, ne représente pas en lui-même un emploi de la force*» : CIJ, *Nicaragua c. États-Unis*, Arrêt, 27 juin 1986, par. 228.
[93] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 89, par. 4, p. 410.
[94] *Ibid*, par. 5, p. 410.

autre État afin d'extraire des données d'une manière qui entraînerait une perte de fonctionnalité de cette infrastructure.

Un excellent exemple de l'existence des hostilités dans le domaine numérique — la situation dans laquelle un État utilise des cyberattaques en combinaison avec des armes conventionnelles ou pour soutenir les dernières. À titre d'illustration, nous pouvons citer le conflit entre la Russie et la Georgie de 2008 (Annexe 1[95]). Ce conflit est devenu le premier à avoir lieu dans les quatre domaines : l'air, la terre, la mer et le cyberespace. Le 7 août 2008 des troupes russes sont entrées en Ossétie du Sud et plus tard, le même jour, les sites georgiens ont été attaqués. Au cours de la guerre, les cyber-combattants se sont concentrés principalement sur les sites d'information et les sites du gouvernement georgien, les services des institutions financières, des entreprises, des établissements d'enseignement, des médias occidentaux. Les Russes ont utilisé des botnets pour mener principalement des attaques DDoS parallèlement à des opérations destruction de pages Web et au spamming massif sur les e-mails publics afin de les obstruer. Les sites du gouvernement, ainsi que les banques et les téléphones portables ne fonctionnaient pas plusieurs jours[96]. Afin de récupérer les sites du Président, du Ministère des affaires étrangères, du Parlement et du Ministère de la Défense, le gouvernement a dû déplacer ses pages d'information sur des serveurs américains et polonais[97].

La situation était la même pour le conflit entre l'Inde et le Pakistan. Une nouvelle étape de la confrontation indo-pakistanaise a eu pour résultat des cyberattaques pakistanaises contre près de 100 sites Web et systèmes critiques du gouvernement indien en mars 2019 suite à une attaque contre les forces militaires indiennes au Cachemire. L'Inde, à son tour, a indiqué qu'elle avait également pris des cybermesures offensives pour contrer ces attaques[98].

Comme nous le voyons, le recours à des cyberarmes dans un contexte d'utilisation des armes classiques donne à penser que cette situation constituerait un conflit armé international. Cependant,

---

[95] DEIBERT (Ronald), ROHOZINSKI (Rafal), CRETE-NISHIHATA (Masashi), « Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war », *Security Dialogue*, Vol 43 (I), février 2012, p. 15, URL : https://www.researchgate.net/publication/258186818_Cyclones_in_Cyberspace_Information_Shaping_and_Denial_in_the_2008_Russia-Georgia_War (visité le 17/01/2020).

[96] KOZLOWSKI (Andrzej), «Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan», International Scientific Forum, 12-14 December 2013, Tirana, Albania Proceedings, Vol. 3, p. 238, URL : https://www.researchgate.net/profile/Nnedinma_Umeokafor/publication/260107032_International_Scientific_Forum_ISF_2013vol3/links/02e7e52f964505c201000000.pdf#page=246 (visité le 17/01/2020).

[97] *Mediapart*, « Une cyberguerre dans le conflit russo-géorgien ? », le 29 août 2008, URL : https://blogs.mediapart.fr/edition/les-invites-de-mediapart/article/290808/une-cyberguerre-dans-le-conflit-russo-georgien (visité le 19/01/2020).

[98] Center for Strategic and International Studies, Significant Cyber Incidents, décembre 2019, URL : https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (visité le 23/01/2020).

la question si la cyberattaque peut elle-même « ouvrir » des hostilités sans le soutien des armes conventionnelles est un sujet d'une vive préoccupation. Mais avant de passer à l'examen de cette question dans les paragraphes qui suivent, nous nous permettons d'attirer l'attention sur la position de la France en réponse à la résolution 73/27 relative aux « Progrès de l'informatique et des télécommunications et sécurité internationale » et à la résolution 73/266 relative à « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale » :

> « *L'hypothèse d'un conflit armé constitué exclusivement d'activités numériques ne peut être exclue par principe, mais repose sur la capacité des cyberopérations à atteindre le seuil de violence requis pour qualifier l'existence d'un conflit armé international ou non-international* »[99].

Il convient donc d'analyser de manière plus approfondie ce seuil de violence et les effets que la cyberattaque doit entraîner pour devenir l'acte déclencheur d'un conflit armé, c'est ce que nous ferons dans la Section suivante.

Section 2 – La cyberattaque comme acte déclencheur d'un conflit armé international

En 2018, la société Mondelez International a déposé une plainte contre son assureur Zurich Insurance pour refus d'indemnisation pour les préjudices causés par l'attaque du ransomware NotPetya. D'après les informations communiquées par Mondelez, NotPetya a provoqué le dysfonctionnement d'environ 1700 serveurs de la société et 24000 de ses ordinateurs portables pour une perte chiffrée à 100 millions de dollars. La police d'assurance de Zurich Insurance, à son tour, prévoyait l'indemnisation pour « *physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction* »[100]. Un an avant le dépôt de la plainte, le logiciel de rançon NotPetya a frappé des entreprises dans le monde entier, y compris des compagnies nationales d'électricité, et des institutions publiques et est devenu la cyberattaque « *la plus coûteuse* »[101] de l'histoire d'Internet en causant 10 milliards de dollars de dégâts. Mais ce qui présente un intérêt particulier pour notre étude, c'est la

[99] Réponse de la France à la résolution 73/27 relative aux « Progrès de l'informatique et des télécommunications et sécurité internationale » et à la résolution 73/266 relative à « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale », 2019, par. 3, a), p. 9, URL : https://www.un.org/disarmament/wp-content/uploads/2019/09/France-2019.pdf (visité le 12/05/2020).

[100] Circuit Court of Illinois, *Mondelez International v. Zurich American Insurance Company*, le 10 octobre 2018, par.7.

[101] Kaspersky, «Top 5 most notorious cyberattacks», novembre 2018, URL : https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/ (visité le 09/04/2020).

caractéristique de cette cyberattaque. Les gouvernements britanniques[102] et américains[103] ont déclaré que l'attaque avait été lancée par des hackers russes contre l'Ukraine. Par conséquent, Zurich Insurance a décidé de traiter NotPetya comme « *hostile or warlike action* »[104] invoquant une réserve prévue par le contrat d'assurance pour les actes de ce type parrainés par un État, par une puissance souveraine, par les forces armées, navales ou aériennes ou par les personnes agissant en leur nom à la fois en temps de paix et en temps de guerre[105]. La question se pose toutefois de savoir dans quelles circonstances la cyberattaque peut constituer l'acte déclencheur d'un conflit armé international.

Nous nous permettons de citer à nouveau la position du TPIY dans *l'arrêt Tadić,* dans lequel le Tribunal a défini le début d'un conflit armé international comme le « *recours à la force armée* »[106], ce qui a été par la suite confirmé dans *l'arrêt Kunarac et autres*[107]. Le mot « *armé* » est un élément déterminant puisque c'est l'utilisation des armes qui nous laisse penser que des hostilités se produisent et que le conflit armé existe bien, parce que le conflit armé international « *résulte, par définition, de l'emploi par un État de la force armée contre un autre État* »[108]. De nombreux auteurs partagent cette approche instrumentaliste[109] en soulignant que le caractère armé d'un acte déclencheur est une condition *sine qua non* d'un conflit armé[110] permettant de le distinguer d'autres actes hostiles tels que la rupture des relations diplomatiques et la pression psychologique sur un État[111], l'imposition de sanctions économiques ou simplement la menace de la force[112] bien que la dernière soit susceptible de provoquer des actions de la part du Conseil de Sécurité en vertu du Chapitre VII de la Charte des

---

[102] Gouvernement du Royaume-Uni, «Foreign Office Minister condemns Russia for NotPetya attacks», le 15 février 2018, URL : https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (visité le 12/04/2020).

[103] Statement from the Press Secretary, le 15 février 2018, URL : https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ (visité le 12/04/2020).

[104] Circuit Court of Illinois, *Mondelez International v. Zurich American Insurance Company*, op. cit., par. 13.

[105] *Ibid*.

[106] TPIY, *Le Procureur c. Duško Tadić*, Chambre d'Appel, Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, le 2 octobre 1995, par. 70.

[107] TPIY, *Le Procureur c. Dragoljub Kunarac, Radomir Kovač et Zoran Vuković*, Chambre d'Appel, Arrêt, le 12 juin 2002, par. 56.

[108] DAVID (Eric), *Principes de droit des conflits armés*, Bruylant, Bruxelles, 2012, p. 166.

[109] «*The instrument-based approach focuses on the means used to commit an act, ie weapons, and has been traditionally employed to distinguish armed force from economic and political coercion* » in: ROSCINI Marco «Cyber operations as a use of force», Research Paper No. 16-05, University of Westminster School of Law, p. 6, URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2631078 (visité le 11/05/2020).

[110] «*However, actions involving the threat but not the use of force before an armed conflict has begun will not necessarily constitute acts of war, in that they will not in themselves give rise to a condition of armed conflict*» : GREENWOOD (Christopher), «Scope of Application of Humanitarian Law», p. 57 in: FLECK (Dieter), The Handbook of International Humanitarian Law, Oxford, 2008.

[111] «*Breaking off diplomatic relations with a State, or withdrawing recognition from it, does not suffice. An economic boycott or a psychological pressure is not enough*» : DINSTEIN (Yoram), *War, Aggression and Self-Defence*, Cambridge : Cambridge University Press, 2011, p.10.

[112] «*Mere threats of military force or other activities that do not reach the threshold of armed force, in particular economic sanctions, are not considered armed conflict*» : WERLE (Gerhard), *Principles of international criminal law*, TMC Asser Press, Haye, 2005, p. 288.

Nations Unies. En d'autres termes, nous pouvons noter que, d'après l'opinion partagée par la plupart d'auteurs, le CAI existe lorsqu'une partie au conflit « *prend des mesures qui blessent, tuent, endommagent ou détruisent* »[113]. Dans le même temps, il convient de souligner que peu importe quelles sont les armes utilisées dans un conflit – cinétiques ou non cinétiques – qui provoquent ces effets[114]. Par conséquent,

> « *l'acte déclencheur est ainsi en général commis par des armes explosives, biologiques ou chimiques, ou au moyen de techniques qui entraînent les mêmes conséquences* »[115].

En se demandant quelles cyberattaques peuvent déclencher un CAI, Nils Meltzer ajoute également celles « *parrainées par l'État* [qui] *donneraient lieu à un conflit armé international si elles sont conçues pour nuire à un autre État, non seulement en causant directement la mort, des blessures ou des destructions, mais également en affectant directement ses opérations militaires ou sa capacité militaire* »[116].

D'un autre côté, le droit international humanitaire admet que le conflit armé international peut exister même en l'absence de tout affrontement, ce qui a été réservé, par exemple, pour la situation d'occupation : « *La Convention* [de Genève I] *s'appliquera également dans tous les cas d'occupation de tout ou partie du territoire d'une Haute Partie contractante, même si cette occupation ne rencontre aucune résistance militaire* »[117].

La clarification sur le fait de savoir laquelle des deux approches est applicable aux cyberattaques pour comprendre quand elle peut constitue un acte déclencheur n'a été exprimée qu'en 2016 dans les Commentaires sur la Convention de Genève I qui soulignaient que « *lorsque des cyberopérations ont des effets similaires aux opérations cinétiques classiques, elles constituent un conflit armé international* »[118]. Les conclusions dans la thèse soutenue par Djemila Carron l'année précédente vont

---

[113] SCHMITT (Michael), «Wired warfare: Computer network attack and jus in bello», CICR, 2002, p. 373, URL : https://www.icrc.org/en/doc/assets/files/other/365_400_schmitt.pdf (visité le 10/05/2020).

[114] «*Still, what counts is not the specific type of ordnance, but the end product of its delivery to a selected objective*» : DINSTEIN (Yoram), «Computer Network Attacks and Self-Defense», p. 103 in: SCHMITT (Michael), O'DONNELL (Brian), Computer network attack and international law, Symposium on Computer Network Attack and International Law, *International Law Studies*, Vol. 76, Naval War College, URL : https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1397&context=ils (visité le 10/05/2020).

[115] CARRON (Djemila), *L'acte déclencheur d'un conflit armé international*, Schulthess, Genève, 2016, p. 437, URL : https://archive-ouverte.unige.ch/unige:95601/ATTACHMENT01 (visité le 11/04/2020).

[116] MELZER Nils, «Cyber operations and jus in bello», p.5 in: UNIDIR, «Confronting cyberconflict», Disarmament Forum, 2011, URL : https://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf (visité le 11/05/2020).

[117] CG (I), article 2, al. 2.

[118] CICR, Les Commentaires sur la Convention de Genève pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne de 1949, article 2, 2016, par. 255.

dans le même sens et admettent également qu'une cyberattaque est capable de déclencher un conflit armé international « *si elle résulte en vies humaines, blessures, dommages ou destructions à des personnes ou à des biens. En ce sens, les cyber opérations ne se distinguent pas d'autres types de comportements* »[119]. Ainsi, nous pouvons légitimement penser qu'au niveau temporel le droit humanitaire sera appliqué aux cyberattaques « *dès que les hostilités ont éclaté en fait, même si aucune déclaration de guerre n'est intervenue, et quelle que soit la forme que revêt l'intervention armée* »[120] et « *s'étend au-delà de la cessation des hostilités jusqu'à la conclusion générale de la paix* »[121].

Cette conception matérialiste a été reprise dans le Manuel de Tallinn bien que les experts proposent les autres critères qui permettent de préciser si les cyberopérations sont considérées comme un recours à la force, tout en soulignant que cette liste n'est ni exhaustive ni formelle:

a) « La gravité (les conséquences doivent inclure les dommages physiques aux personnes ou à la propriété, tandis que les inconvénients ou les irritations ne constituent pas un recours à la force) ;

b) L'instantanéité (une cyberopération produisant des résultats immédiats sera sûrement plus reconnue comme un recours à la force que des cyberactions dont les effets se traduisent après des semaines ou des mois) ;

c) Le caractère direct (une cyberopération dont la cause et l'effet sont clairement liés est plus susceptible d'être qualifiée de recours à la force) ;

d) Le caractère invasif (plus les cyberopérations empiètent sur l'État visé ou sur ses cybersystèmes plus elles sont susceptibles d'être qualifiées de recours à la force). Le nom de domaine joue un rôle crucial dans ce sens : les cyberopérations qui ciblent spécifiquement le nom de domaine d'un État particulier ou d'un organe d'État particulier peuvent, pour cette raison, être considérées comme plus intrusives que celles qui ciblent des extensions de noms de domaine non spécifiques à un État, telles que ".com**"** ;

[119] CARRON (Djemila), «L'acte déclencheur d'un conflit armé international», op. cit., p.437.

[120] Conférence préliminaire des Sociétés Nationales de la Croix-Rouge pour l'étude des Conventions et de divers problèmes ayant trait à la Croix-Rouge, op. cit. note 117, p. 4., cité dans GRIGNON (Julia), *L'applicabilité temporelle du droit international humanitaire*, Schulthess, Genève, 2014, p. 38.

[121] TPIY, *Le Procureur c. Duško Tadić*, Chambre d'Appel, Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, le 2 octobre 1995, par. 70.

e) La mesurabilité des effets (une cyberopération qui peut être évaluée en termes très spécifiques (par exemple, quantité de données corrompues, pourcentage de serveurs désactivés, nombre de fichiers confidentiels exfiltrés) est plus susceptible d'être qualifiée de recours à la force) ;

f) Le caractère militaire (un lien entre la cyberopération en question et les opérations militaires accroît les risques de caractérisation de recours à la force) ;

g) La participation d'un État (plus un lien est clair et étroit entre un État et des cyberopérations, plus il est probable que d'autres États la qualifieront de recours à la force par cet État) ;

h) La légalité présomptive (les actes non interdits sont autorisés, c'est-à-dire, en l'absence d'un traité juridique qui l'interdit ou d'une interdiction du droit coutumier, un acte est présumé légal). À titre d'illustration, le droit international ne prohibe pas la propagande, les opérations psychologiques, l'espionnage, par conséquent, les actes relevant de ces catégories et d'autres sont supposés être légaux et ils sont moins susceptibles d'être considérés par les États comme des recours à la force »[122].

Il faut souligner que l'idée que la cyberattaque doit avoir un certain degré de gravité a été soutenue non seulement au niveau international, mais se reflète aussi dans les doctrines nationales. En particulier, le Ministère des Armées de France a défini clairement sa position dans un rapport spécial et a déclaré que « *si l'hypothèse d'un conflit armé constitué exclusivement d'activités numériques ne peut être exclue par principe, elle repose toutefois sur la capacité des cyberopérations autonomes à atteindre le seuil de violence requis pour une telle qualification* »[123].

Plus précisément, l'Académie de droit international humanitaire et de droits humains à Genève a examiné cette problématique dans le contexte du conflit américano-iranien. Les tensions entre ces deux États se poursuivent depuis plus d'un demi-siècle, cependant nous pouvons constater une nouvelle détérioration des relations en 2019. Le 20 juin 2019, le corps des Gardiens de la révolution islamique, organisation paramilitaire de la République islamique d'Iran, a utilisé un missile sol-air pour abattre un MQ-4 Triton, drone américain destiné à la surveillance en mer. Dans quelques jours, les médias ont annoncé que les services de renseignement iraniens, y compris les systèmes informatiques qui contrôlaient les lancements

[122] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 69, par. 9, pp. 334-335.

[123] Délégation à l'information et à la communication de la défense, Droit international appliqué aux opérations dans le cyberespace, op.cit., p. 12.

de missiles iraniens, ont été victimes l'objet des cyberattaques commises par les États-Unis[124]. Bien que cette situation soulève bien des questions[125], les experts de l'Académie de droit international humanitaire et de droits humains à Genève considèrent que « *même lorsque les cyberactivités sont le seul moyen par lequel des actions hostiles sont prises par les États, elles pourraient déclencher l'application des règles du DIH* »[126].

Pourtant, l'approche matérialiste a ses limites. En s'appuyant sur la définition matérialiste d'un acte déclencheur, les cyberattaques qui ne produisent pas des effets similaires aux opérations cinétiques restent non réglées dans les Commentaires contemporains des Conventions de Genève et la question de savoir si elles peuvent déclencher un conflit armé reste toujours ouverte dans le DIH[127]. Néanmoins, certains auteurs proposent la solution à ce problème. En particulier, Marco Roscini, qui offre une approche fondée sur des objectifs, d'après laquelle « *cyber operations reach the threshold of the use of armed force when they are conducted against national critical infrastructure (NCI), whatever their effects on such infrastructure or the nature of the operation might be* »[128]. Ces conclusions concordent avec le Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications qui inclut parmi les attaques les plus graves « *celles qui sont dirigées contre une infrastructure essentielle d'un État et contre les systèmes d'information correspondants* »[129]. Enfin, nous devons également garder en mémoire que les cyberattaques non couvertes par les lois de la guerre peuvent relever du domaine d'application de la

[124] *The New York Times*, « U.S. Carried Out Cyberattacks on Iran », le 22 juin 2019, URL : https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html (visité le 19/12/2019).

[125] En particulier, les experts de l'Académie de droit international humanitaire et de droits humains à Genève s'interrogent si les cyberattaques contre l'Iran sont considérées comme la réponse à l'attaque contre un drone américain ou elles ont été planifiées à l'avance, c'est-à-dire, s'il y a un lien direct entre deux attaques parce que la majorité des experts du Manuel de Tallinn est parvenue à un consensus que ce lien est nécessaire pour l'application du DIH : Voir HRNJAZ (Miloš), The War Report « The United States of America and the Islamic Republic of Iran: An international armed conflict of low intensity », Académie de droit international humanitaire et de droits humains à Genève, décembre 2019, p. 6, URL : https://www.geneva-academy.ch/joomlatools-files/docman-files/The%20United%20States%20Of%20America%20And%20Islamic%20Republic%20Of%20Iran%20An%20International%20Armed%20Conflict%20Of%20Low%20Intensity.pdf (visité le 17/12/2019).

[126] *Ibid.*

[127] CICR, Les Commentaires sur la Convention de Genève pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne de 1949, l'article 2, 2018, par. 256 ; Voir aussi CICR, «Les cyberopérations en période de conflit armé : 7 questions juridiques et politiques essentielles», le 3 avril 2020, URL : https://www.icrc.org/fr/document/les-cyberoperations-en-periode-de-conflit-arme-7-questions-juridiques-et-politiques (visité le 09/05/2020).

[128] ROSCINI (Marco), «Cyber Operations as a Use of Force», Research Paper No. 16-05, University of Westminster School of Law, le 31 mars 2014, p.7, URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2631078 (visité le 10/05/2020).

[129] Assemblée générale, Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, op. cit., par. 5.

clause Martens[130] étant donné que son applicabilité est garantie par le Statut qui dispose que « *la coutume internationale comme preuve d'une pratique générale acceptée comme étant le droit* »[131] ainsi que de principes fondamentaux du DIH ce qui sera examiné plus précisément dans le Chapitre 2.

Chapitre 2 — Les principes fondamentaux du droit humanitaire appliqués aux cyberattaques

> « *It is precisely because this law* [droit international humanitaire] *is so intimately bound to humanity that it assumes its true proportions, for it is upon this category of law, and no other, that the life and liberty of countless human beings depend if war casts its sinister shadow across the world* »[132].

L'histoire des conflits est inextricablement liée au développement d'armes, alors que les normes du droit humanitaire n'ont pas toujours été suffisantes et ont parfois été prises trop tard. Le progrès scientifique de la seconde moitié du XIXe siècle au début XXe siècle a provoqué la hausse spectaculaire de l'armement et a mis au service de la guerre de nouvelles inventions militaires : les armes chimiques, les avions militaires, les chars, les mines navales, les torpilles… En espérant de maîtriser ce processus, les experts du droit international humanitaire ont pu d'élaborer les principes fondamentaux qui pourraient être appliqués à tout type d'armes indépendamment des avancées en matière de DIH.

Bien que la quantité de ces principes varient d'une source à l'autre, certains d'entre eux demeurent inchangés. Le CICR, en particulier, souligne l'existence de trois principes fondamentaux (Section 1) et quatre principes supplémentaires qui découlent des précédentes (Section 2), faisant valoir qu'ils sont applicables aux nouvelles technologies.

Section 1 – L'application des principes de distinction, de proportionnalité et de précaution aux cyberattaques

Les principes de distinction, de proportionnalité et de précaution sont la clef de voûte du droit international humanitaire. Toute partie au conflit a l'obligation de les respecter dans la planification

[130] CICR, «Le droit international humanitaire et les cyberopérations pendant les conflits armés», novembre 2019, p. 6, URL : https://www.icrc.org/fr/document/le-droit-international-humanitaire-et-les-cyberoperations-pendant-les-conflits-armes (visité le 12/05/2020).

[131] Statut la Cour Internationale de Justice, art. 38, par. 1 b).

[132] PICTET (Jean), *Development and principles of international humanitarian law*: course given in July 1982 at the University of Strasbourg as part of the courses organized by the International Institute of Human Rights, Springer, 1985, p. 1.

et la conduite de l'attaque. L'applicabilité de ces principes au cyberdomaine a été reconnue par le CICR pour la première fois tout récemment — en 2011 et a reconfirmée dans son rapport de 2015 dans lequel il a déclaré que *« l'usage de cybercapacités en situation de conflit armé doit respecter l'ensemble des principes et des règles du DIH, comme pour toute autre arme et tout autre moyen ou méthode de guerre, nouveau ou ancien »*[133].

D'un point de vue pratique, l'application de ce principe pose néanmoins un grave problème pour le droit dans le cybercontexte. Reprenons les trois principes fondamentaux un par un.

La première règle exige que

> « *ceux qui préparent ou lancent une attaque fassent tout ce qui est pratiquement possible pour vérifier que les objectifs attaqués ne sont ni des personnes civiles ni des biens de caractère civil, afin d'épargner les civils dans toute la mesure* »[134].

Elle fait partie du droit international humanitaire coutumier[135] et a été codifiée dans le Protocole additionnel I aux Conventions de Genève de 1949 dans les articles 48, 51 et 52 dont le but principal est de protéger la population civile et les biens de caractère civil. Ces mêmes dispositions soulignent que *« [l]es attaques doivent être strictement limitées aux objectifs militaires »*.

En vertu du principe de distinction, toute attaque intentionnelle dirigée contre la population civile constitue un crime de guerre lorsqu'elle est commise dans un conflit armé international[136]. Les attaques sans discrimination sont également reconnues comme telles, si elles peuvent causer incidemment des dommages aux personnes civiles qui seraient excessifs par rapport à l'avantage militaire attendu[137]. En février 2020, pendant la deuxième session d'Open-Ended Working Group de l'ONU le CICR a réaffirmé son attachement à ce principe, en rappelant aux participants que ces dispositions s'appliquent au cyberespace[138].

---

[133] Le CICR a indiqué que, quelles que soient la nature et la nouveauté de la méthode et du moyen utilisé dans les guerres leur l'usage, y compris dans le cyberspace, il faut respecter des principes généraux et des règles du DIH : CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », op. cit., p.48.

[134] TPIY, *Le Procureur c. Stanislav Galić*, Chambre de Première Instance I, Jugement et opinion, le 5 décembre 2003, par. 58.

[135] HENCKAERTS (Jean-Marie), DOSWALD-BECK (Louise), *Droit international humanitaire coutumier, Volume I : règles*, CICR, 2006, Règles 1, 7, URL : https://www.icrc.org/fr/doc/assets/files/other/icrc_001_pcustom.pdf (visité le 07/02/2020).

[136] « *Le fait de diriger intentionnellement des attaques contre la population civile en tant que telle ou contre des civils qui ne participent pas directement part aux hostilités* » : Statut de Rome, art.8, par. 2, al. b) i).

[137] PA I, art. 51, par. 5 al. b).

[138] ICRC, Principles of IHL (distinction, proportionality) have direct bearing on cyber operations, Statement to the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security; Second substantive session; Agenda item «International law», le 12 février 2020,

En se fondant sur l'article 48 du Protocole I et sur l'article 8 par. 2 al. b) i) et ii) du Statut de Rome, le Manuel de Tallinn élargit également le champ d'application du principe de distinction au cyberespace[139] :

> **RÈGLE 93 — Distinction**
>
> Le principe de distinction s'applique aux cyberattaques.

L'importance de ce principe a été reflétée dans la nouvelle doctrine militaire de lutte informatique offensive de France de 2019 qui oblige les forces militaires françaises à respecter la distinction lors de la planification et le lancement de toute cyberattaque. Compte tenu de la nature spécifique des cyberopérations, le commandement est tenu de « *réunir les renseignements nécessaires à l'identification de l'objectif et de choisir le moyen le plus adapté pour mettre en œuvre le principe de distinction* »[140].

Cependant il ne suffit pas de faire une distinction entre les civils et les combattants, il est interdit également d'attaquer la population civile et les biens civils[141]. Une formulation que nous avons trouvée particulièrement intéressante sur ce sujet est celle exprimée dans l'avis consultatif rendu par la CIJ sur la licéité de l'utilisation des armes nucléaires et qui pourrait servir d'orientation aux États pendant leur mise au point de nouveaux types d'armes, y compris les cyberarmes :

> « *les États ne doivent jamais prendre pour cible des civils, ni en conséquence utiliser des armes qui sont dans l'incapacité de distinguer entre cibles civiles et cibles militaires* »[142].

La première question qui se pose est de savoir comment faire respecter cette règle dans les conditions où les militaires et les civils partagent le même cyberespace et où tout est interconnecté[143]. En particulier, le CICR avance comme argument le fait que 90 % du cyberespace est de la nature civile[144] et qu'il existe un lien très fort entre des réseaux informatiques militaires et des infrastructures

---

https://www.icrc.org/en/document/principles-international-humanitarian-law-distinction-proportionality-have-direct-bearing (visité le 02/05/2020).

[139] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 93, p. 420.

[140] Délégation à l'information et à la communication de la défense, Droit international appliqué aux opérations dans le cyberespace, op. cit., p. 14.

[141] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 94, p. 422.

[142] CIJ, Licéité de la menace ou de l'emploi d'armes nucléaires, Avis consultatif, le 8 juillet 1996, par. 78.

[143] ICRC, «Cyberwarfare and international humanitarian law: the ICRC's position», p. 3, URL : https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf (visité le 07/02/2020).

[144] ICRC, Expert Meeting 14–16 november 2018 – Geneva, op. cit, p. 33.

commerciales[145]. La situation dans les pays, dont les systèmes techniques sont plus perfectionnés, comme aux États-Unis, est bien pire : ancien directeur du National Intelligence Michael McConnell a estimé que « *98% of U.S. government communications, including classified communications, travel over civilian-owned-and-operated networks and systems* »[146]. Ainsi, la cyberattaque contre une cyberinfrastructure militaire est susceptible de se répandre dans les systèmes informatiques civils.

La deuxième question qui se pose est de savoir comment nous pouvons lancer une cyberattaque contre les forces militaires dans le cybercontexte? Les conflits armés internationaux « classiques » prévoient le port d'uniforme militaire[147] ainsi que le port des armes ouvertement par le combattant[148]. Ces règles permettent non seulement de faire une distinction entre les combattants et la population civile en vue de garantir la protection renforcée pour la dernière, mais également pour l'identification des parties au conflit — cela permet de rattacher les combattants à un État déterminé. Toutefois, le caractère anonyme des cyberattaques pose un problème du rattachement d'une activité cybernétique à une partie au conflit. La situation s'aggrave par le fait que les individus ne sont généralement pas physiquement visibles lorsqu'ils lancent des cyberattaques. De plus, dans le cadre des cyberopérations l'anonymat est la règle plutôt que l'exception.

Cette situation remet en question le respect de l'autre disposition du droit humanitaire, d'après laquelle toute personne est présumée civile en cas de doute[149]. Est-ce que l'ordinateur qui programme une cyberattaque doit automatiquement être considéré comme objectif militaire et son propriétaire comme combattant? Qu'est-ce qu'il faut faire dans la situation où un malfaiteur recourt au botnet[150]? Le Manuel de Tallinn ne donne pas les réponses à ces questions, cependant il exprime plus clairement sur la notion des « attaques indiscriminées ». Dans la situation où il est techniquement possible de *diriger* une cyberattaque contre une cible légitime, mais l'auteur de cette attaque ne parvient pas à le faire, il va violer le droit international

[145] CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », Rapport, XXXI[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge, 28 novembre – 1[er] décembre 2011, Genève, Suisse, p.42, URL: https://www.icrc.org/fr/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-fr.pdf (visité le 09/02/2020).

[146] JENSEN (Eric Talbot), 'Cyber Warfare and Precautions Against the Effects of Attacks', *Texas Law Review*, Vol. 88, 2010, par. 1534, URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661218 (visité le 13/02/2020).

[147] PA I, article 44, par.7.

[148] *Ibid*, article 44, par.3.

[149] PA I, article 50, par. 1. ; Voir aussi SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., p. 424.

[150] Nous entendons par « botnet » un réseau d'ordinateurs compromis, appelés « bots », contrôlés à distance par un intrus et utilisés pour mener des cyberopérations coordonnées — DDos attaques — comme il a été défini par les experts internationaux : SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., p. 563. Dans ce cas tout appareil technique peut devenir un appareil « zombie » et participer à des cyberattaques alors que son vrai utilisateur n'en est pas du tout conscient.

humanitaire[151], à savoir l'article 51, par. 4 du Protocole Additionnel I. À titre d'illustration, les experts du Manuel expliquent que le téléchargement d'un malware sur au serveur Web auquel des utilisateurs militaires autant que des civils ont l'accès, sera considéré comme une cyberattaque indiscriminée[152]. À cet égard, il n'est pas superflu de rappeler que les auteurs de Stuxnet ont pris en compte le principe de distinction lors de l'élaboration de la cyberattaque. Le ver a probablement été implanté dans le réseau local de la centrale électrique de Natanz via une clé USB infectée[153]. Ce système a été isolé des autres réseaux et elle n'avait pas d'accès à Internet, c'est pourquoi l'infrastructure civile n'avait pas été touchée.

La position du CICR présenté dans le rapport de 2011 est beaucoup plus stricte que celle des experts du Manuel de Tallinn. D'après elle, même si un virus a été introduit dans un réseau militaire, mais il pourrait se répandre dans des systèmes civils ou aller au-delà des frontières d'un État, et compromettre le fonctionnement de ces systèmes, tels actes « *seraient considérés comme frappant sans discrimination, puisqu'ils ne pourraient pas être dirigés contre un objectif militaire spécifique* »[154] au regard du DIH. Cependant, l'activité malveillante dans le cyberespace s'accompagne toujours de risques, ne serait-ce que parce un outil de la lutte informatique « *peut être volé, copié ou imité par des adversaires ou des acteurs tiers* »[155]. Cet état de choses ne permettrait de recourir aux cyberattaques lors d'un conflit armé, c'est pourquoi il est nécessaire de se limiter à la prise de *toutes les mesures possibles* (dans l'esprit des Conventions de Genève) pour éviter la propagation d'un malware à partir des objets civils.

Néanmoins, il faut noter que certaines attaques contre les civils peuvent être licites. Le droit international humanitaire prévoit cette exception pour les « *campagnes idéologiques, politiques ou religieuses* »[156]. Des experts internationaux élargissent le champ d'application de cette règle au cybercontexte[157]. Tel est le cas des cyberattaques commises dans un but de propagande comme la distribution de tracts envoyés par email. La situation suivante peut illustrer ce type d'attaques psychologiques : en l'espèce, les États-Unis d'Amérique avaient

[151] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., p. 467.

[152] *Ibid*, par. 2, p. 468.

[153] Center for Security Studies, 'Hotspot Analysis: Stuxnet', Cyber Defense Project, Zürich, octobre 2017, p. 4, URL : https://www.researchgate.net/publication/323199431_Stuxnet (visité le 09/02/2020).

[154] CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », 2011, op. cit., p.44.

[155] Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 9.

[156] CICR, Les Commentaires sur Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux de 1977, 1987, l'article 48, par. 1875.

[157] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., par. 5, p. 421.

lancé une cyberattaque contre le réseau militaire sécurisé de l'Iraq. Avant le début du conflit entre les États-Unis et l'Iraq, des milliers de soldats iraquiens ont reçu des messages appelant à abandonner leurs chars pour rester indemnes[158]. Or, la transmission de messages électroniques à la population ennemie appelant à la capitulation est estimée conforme au droit des conflits armés.

Ayant un des principes clefs du droit humanitaire, le principe de distinction sert de base à deux autres — la proportionnalité et la précaution. L'existence de ces principes confirme une triste réalité que les victimes sont inévitables pendant la guerre et les parties doivent prendre toutes les mesures possibles pour les éviter ou les minimiser autant que possible.

Le principe de proportionnalité joue un rôle important pour la protection de la population civile : si une attaque peut causer des dommages collatéraux excessifs aux civils par rapport à l'avantage militaire concret et direct attendu, celle-ci doit être annulée ou interrompue[159]. Dans le cybercontexte, les attaques disproportionnées sont également interdites en vertu de Manuel de Tallinn sur la base des articles 51, par. 5 al. b), et 57, par. 2 al. a) iii), du Protocole additionnel I :

> **RÈGLE 113 — Proportionnalité**
>
> Une cyberattaque qui pourrait d'entraîner des pertes de vies humaines, des blessures corporelles ou des dommages matériels, ou une combinaison des deux, qui seraient excessifs par rapport à l'avantage militaire concret et direct attendu est interdite.

Comme nous voyons, dans la situation où le dommage est excessif par rapport à l'avantage militaire concret et direct attendu de l'opération, la cyberattaque serait interdite[160]. Dans ce cas le recours à des programmes malveillants qui se propagent sans la possibilité de les contrôler et qui risquent de nuire aux infrastructures civiles constituerait une violation des règles du droit international. Cet aspect trouve son affirmation dans la règle suivante du Manuel de Tallinn:

> **RÈGLE 112 — Objectifs militaires clairement séparés et distincts**
>
> Une cyberattaque qui traite comme une cible unique un certain nombre d'objectifs cybermilitaires clairement distincts dans une cyberinfrastructure principalement utilisée à des fins civiles est interdite si cela nuirait à des personnes ou objets protégés.

---

[158] CLARKE (Richard Alan), KNAKE (Robert), *Cyber War: The Next Threat to National Security and What to Do About It*, Harper Collins Publishers, 2010, pp. 9-10.

[159] PA I, article 51, par. 5, al. b)., article 57 par. 2, al. iii). ; Voir aussi ICRC, « Cyberwarfare and international humanitarian law: the ICRC's position », op. cit., p. 3.

[160] Statut de Rome, article 8 par. 2, al. b) iv).

Par exemple, en vertu de cette disposition, toute attaque qui arrête le système de refroidissement des centres de serveurs qui contiennent des serveurs militaires et, notamment, des serveurs civils, viole cette règle s'il est techniquement possible d'utiliser un moyen informatique pour simplement fermer les sous-systèmes qui sont chargés du refroidissement des serveurs militaires[161].

Les mesures de distinction entre les objets civils et militaires dans le cybercontexte sont actuellement à l'examen. Nous nous permettons de citer, à titre d'exemple, une des initiatives présentées lors de la réunion d'experts organisée par le CICR en 2018. Il a été proposé de développer « *a digital watermark to identify certain actors (for instance, civil defence organizations and their assets) or infrastructure (hospitals and critical infrastructure) in cyber space in order to prevent them from being attacked* »[162]. Toutefois, il a été noté que la réalisation de ce projet exigerait la création d'un organe spécial chargé à marquer des biens qui bénéficiaient d'une protection spécifique par analogie avec l'usage de l'emblème de la Croix-Rouge et à créer un registre internationalement reconnu des objets numériques qui étaient protégés. Sur le plan technique, les experts proposent, entre autres, utiliser des adresses IP ou une signature numérique[163]. Dans ce cas les opérateurs des cyberattaques pourraient programmer des logiciels malveillants en fonction des données présentées dans ce registre pour épargner des objets et des infrastructures marqués. Cependant, cette initiative devrait faire face à des dangers supplémentaires. En particulier, l'existence de tel registre est susceptible de faciliter des attaques pour les hackers qui ont créé un virus initialement dans le but de détruire des objets protégés[164].

À cet égard, nous voudrions noter que les États-Unis ont déjà commencé à mettre en œuvre une initiative similaire dans la pratique. Par analogie avec les zones démilitarisées, ils comptent créer des « *digital safe havens* » pour les données qui bénéficient d'une protection spéciale. En particulier, ce projet vise à séparer un réseau du département de la Santé et des Services sociaux du réseau du Pentagone pour qu'ils ne soient pas sur les mêmes serveurs[165].

Nous nous permettons de rappeler que le principe de proportionnalité ne concerne que les cyberattaques qui ont été commises contre l'objectif légitime et qui ont causé incidemment des

[161] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., par. 2, p. 470.

[162] ICRC, Expert Meeting 14–16 november 2018 – Geneva, The potential human cost of cyber operations, op. cit., pp. 40-41.

[163] *Ibid*.

[164] *Ibid*.

[165] SEGAL (Adam), «Cyberspace Governance: The Next Step» (Policy innovation memorandum no. 2), Council on foreign relations, International Institutions and Global Governance Program, le 14 novembre 2011, p.3, URL : https://cdn.cfr.org/sites/default/files/pdf/2011/03/Policy_Innovation_Memo2_Segal.pdf (visité le 29/03/2020).

dommages aux biens de caractère civil et des pertes en vies humaines et des blessures aux civils, mais aussi des dommages aux biens de caractère civil[166]. En particulier, des cyberattaques dirigées contre le Global Positioning System (ci-après le GPS) peuvent aboutir aux dommages collatéraux dans le domaine d'aviation civile ou de transports maritimes. L'expérience des États confirme la possibilité de ce scénario : le gouvernement de Suisse a annoncé que des « *cyberattaques visant le système de navigation par satellite GPS se sont multipliées* » et a constaté avec regret que « *dans les applications civiles, tous les récepteurs de signaux GPS sont vulnérables et ne disposent d'aucune protection face à de telles manipulations* »[167].

En outre, s'agissant de la proportionnalité, il est indispensable de définir la notion des dommages « *excessifs* » par rapport à l'avantage militaire concret et direct attendu qui fait la cyberattaque illicite. L'article 57, par. 2 al. a) iii) du Protocole Additionnel I dispose que « *par les mots "concret et direct", on a voulu marquer qu'il s'agissait d'un intérêt substantiel et relativement proche, en éliminant les avantages qui ne seraient pas perceptibles ou qui ne se manifesteraient qu'à longue échéance* »[168]. Puisque chaque opération militaire est unique, la corrélation entre l'avantage militaire et des dommages excessifs doit être évaluée au cas par cas. Cette position est partagée par les commentateurs du Protocole additionnel I qui définissent des dommages excessifs comme ceux qui affectent « *gravement* »[169] les civils, tout en reconnaissant que cette disposition « *laisse (…) un champ assez vaste à l'appréciation* »[170]. À cet égard, il faut mettre en avant que les conséquences des cyberopérations telles que l'irritation, le stress ou la peur ne sont pas considérées comme des dommages civils collatéraux[171].

Le mot même d' « *avantage attendu* » prévoit une analyse que les parties au conflit sont tenues de faire avant le lancement d'une attaque. Nous voyons dans la doctrine militaire française que cette exigence concerne l'analyse des risques liés à l'emploi d'une cyberarme et inclut l'évaluation préalable de « *l'immédiateté de l'action, la dualité des cibles et*

---

[166] GEISS (Robin), LAHMANN (Henning), «Cyber warfare: applying the principle of distinction in an interconnected space», *Israel Law Review*, Vol. 45 (3), 2012, p. 397, URL : https://eprints.gla.ac.uk/78067/1/78067.pdf (visité le 12/02/2020).

[167] Département fédéral de la défense, de la protection de la population et des sports, Le portail du Gouvernement Suisse, « Protection de récepteurs GPS contre des cyberattaques », le 23 février 2018, URL : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-69896.html (visité le 09/02/2020).

[168] CICR, Les Commentaires sur Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux de 1977, 1987, l'article 57, par. 2209.

[169] *Ibid*, par. 2216.

[170] CICR, Les Commentaires sur Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux de 1977, 1987, l'article 57, par. 2210.

[171] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 113, par. 5, p. 472.

l'hyperconnectivité des réseaux [qui] exigent un processus de ciblage numérique spécifique encadrant l'ensemble des phases de la cyberopération, ceci afin de les soumettre aux principes de distinction, de précaution et de proportionnalité, notamment en vue de minimiser les dommages et les pertes civiles potentiels »[172].

Enfin, il nous reste d'examiner l'application du dernier principe fondamental dans le cyberespace qui peut être exprimé par le « *devoir de conduire les opérations en épargnant les personnes civiles et les biens de caractère civil* »[173]. En tant que règle du droit international coutumier[174], le principe de précaution impose aux parties au conflit de « *prendre toutes les précautions pratiquement possibles pour protéger contre les effets des attaques la population civile et les biens de caractère civil soumis à leur autorité* »[175]. Par conséquent, cette disposition peut également imposer des restrictions quant au moment et au lieu de l'attaque. Les mesures de précaution doivent être appliquées aussi bien en conjonction avec le principe de proportionnalité qu'indépendamment de celui-ci. Autrement dit, si les pertes parmi les civils ne seront pas excessives par rapport à l'avantage militaire concret et direct attendu de l'opération, la partie au conflit qui lance une attaque est obligée quand même de prendre toutes les mesures de précautions possibles pour minimiser les dommages, les blessures et les morts.

Le Manuel de Tallinn impose ce principe aux parties au conflit dans le cybercontexte, en se fondant sur l'article 57 par. 1 du Protocole additionnel I :

> **RÈGLE 114 — Soins constants**
>
> Pendant les hostilités impliquant des cyberopérations, il faut veiller en permanence à épargner la population civile, les personnes civiles et les biens de caractère civil.

Bien que le droit des conflits armés ne définisse pas les termes « *soins constants* », les experts ont noté que dans le cybercontexte des cyberopérations, il s'agissait du devoir des commandants et

[172] Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 13.
[173] CICR, Les Commentaires sur Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux de 1977, 1987, l'article 57, par. 2215.
[174] HENCKAERTS (Jean-Marie), DOSWALD-BECK (Louise), *Droit international humanitaire coutumier, Volume I : règles*, op. cit., Règle 22.
[175] Voir aussi ICRC, Expert Meeting 14–16 november 2018 – Geneva, The potential human cost of cyber operations, op. cit., p. 8.

de toutes les autres personnes impliquées dans ces opérations d'être constamment sensibles aux effets de leurs activités sur la population civile pour éviter tout effet inutile[176].

Les précautions peuvent être réparties en trois types : les précautions avant une attaque, pendant une attaque et contre les effets des attaques. Les mesures qui doivent être prises avant une attaque sont liées à la vérification des cibles pour ne pas viser les citoyens[177]. Selon les règles du DIH, les groupes de personnes qui ne sont pas membres des forces armées ou qui ne participent pas à une levée en masse sont reconnus comme des personnes civiles, au bénéfice du doute. Le principe de précaution avant une attaque prescrit également une évaluation concernant un dommage éventuel et l'arrêt de l'attaque si ce dommage sera excessif[178]. Si les circonstances le permettent, les parties doivent également avertir de façon efficace les civils avant une éventuelle attaque[179] et, même dans les situations où il existe le choix entre plusieurs cibles avec un avantage militaire équivalent, les combattants doivent privilégier la cible qui présente le moins de danger pour la population civile[180], tant dans le monde physique que dans le cyberespace[181]. En revanche, cette règle ne s'applique pas aux cyberopérations quand les biens de caractère civil se retrouvent endommagés ou détruits sans que la population civile ne soit pas exposée à un risque[182]. Ce point est particulièrement important, dans la mesure où les cyberattaques endommagent souvent l'infrastructure cybernétique civile sans causer de préjudice à la population. De plus, les règles du DIH prévoient que si la cyberattaque a l'élément de surprise, son auteur n'est pas obligé à donner un avertissement pour que l'ennemi ne puisse améliorer la protection contre cette attaque et n'aie pas de la possibilité de localiser et de neutraliser l'outil par lequel l'une autre partie au conflit lance une cyberattaque[183].

Le deuxième type de précautions qui doivent être prises pendant une attaque prévoit que dans les situations où la cible civile a été prise par erreur pour un objectif militaire ou si elle a cessé d'être un objectif militaire (dans le cas où des civils ont décidé de ne plus participer aux hostilités), l'attaque doit être annulée[184].

---

[176] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 114, par. 4, p. 477.

[177] *Ibid*, Règle 115, p. 478.

[178] PA I, article 57, par. 2, al. a) iii).

[179] *Ibid*, article 57, par. 2, al. c).

[180] *Ibid*, article 57, par.3.

[181] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 118, p. 481.

[182] *Ibid*, par. 3 p. 485.

[183] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 118, par. 8, p. 486.

[184] PA I, article 57, par.2, al. b) ; Voir aussi SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 119, p. 483.

Gardant à l'esprit que chaque partie à un conflit armé a l'obligation de prendre des mesures de précaution non seulement contre toute attaque, mais dans le but de défendre leurs propres civils contre les effets des attaques[185], les experts ont proposé quelques initiatives qui pourraient être utilisées pour protéger les hôpitaux[186]. Citons, par exemple, le recours aux précautions passives, comme la séparation des infrastructures informatiques militaires et civiles ; la séparation des systèmes informatiques dont l'infrastructure essentielle dépend d'Internet ; les actions qui visent à procéder à des copies de sauvegarde des données civiles importantes ; les mesures préalables pour assurer la réparation rapide des systèmes informatiques importants ; l'enregistrement numérique d'importants objets culturels ou spirituels pour faciliter leur reconstruction en cas de destruction ; l'utilisation de logiciels antivirus pour protéger les systèmes civils susceptibles d'être endommagés ou détruits lors d'une attaque contre une cyberinfrastructure militaire[187].

Les autres mesures tout aussi significatives proposées par des experts dans le Manuel de Tallinn se focalisent sur deux aspects : la mise à jour des logiciels opportune et la réalisation des essais de sécurité. Comme nous l'avons indiqué, l'utilisation des équipements obsolètes dans les services civils et militaires augmente le risque que la cyberattaque compromettrait le fonctionnement de ces systèmes. C'est pourquoi les experts recommandent non seulement de procéder régulièrement à la mise à jour des systèmes améliorant leur sécurité, mais également d'interdire complètement l'utilisation de systèmes et de logiciels obsolètes[188]. Mais une longue durée de vie des équipements médicaux est un autre défi, car parfois ils peuvent ne plus recevoir de support ou de mises à jour après leur création, contrairement à des autres systèmes civils et militaires. À ce propos, les spécialistes incitent à une plus grande transparence des produits qui pourrait modifier un code source en cas de détections des vulnérabilités et développer les mises à jour pour des produits qui n'étaient plus pris en charge par leurs fournisseurs d'origine[189].

Enfin, une autre initiative vise, quant à elle, à réaliser des essais de sécurité, c'est-à-dire, à recourir à un faux procès de pénétration pour évaluer l'état de préparation des services civils en matière de cybersécurité pour les protéger contre les cyberattaques dans le futur. C'est d'autant plus remarquable que certains gouvernements disposent des laboratoires spéciaux visant à tester et

[185] PA I, article 58.
[186] PA I, article 58.
[187] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Rule 100, par. 3, p. 488.
[188] ICRC, Expert Meeting 14–16 november 2018 – Geneva, The potential human cost of cyber operations, op. cit., p. 76.
[189] ICRC, Expert Meeting 14–16 november 2018 – Geneva, The potential human cost of cyber operations, op. cit., p. 20.

anticiper les effets d'opérations potentiellement dangereuses menées par des criminels ou adversaires[190]. Nous pouvons citer à cet égard l'exemple de *Metasploit* qui représente « *un framework libre d'exploitation de vulnérabilités facilitant la préexploitation (recherche de bugs, écriture d'exploits ou de shellcodes), l'exploitation (envoi de l'exploit) et la post-exploitation (exécution de code arbitraire, accès à des fichiers, injection de serveur VNC)* »[191]. La communauté internationale, à son tour, a déjà montré son intérêt à cette forme des exercices. Par exemple, les États du G7 ont mené dans plusieurs pays simultanément la simulation de cyberattaque transfrontalière dans le secteur financier en été 2019 lors d'une conférence sur la cybersécurité à la Banque de France[192].

Toutefois, en examinant les mesures de précautions il est indispensable de garder toujours à l'esprit les difficultés liées à l'application de ce principe dans la pratique. En particulier, les experts participants à la réunion du CICR en 2018 sur les pertes humaines éventuelles dues aux cyberopérations ont noté que parfois les attaquants eux-mêmes pouvaient avoir une compréhension limitée des conséquences potentielles de leurs actions, car ils pouvaient avoir des informations incomplètes sur la configuration du réseau et les interconnexions[193]. Cela signifie que les conséquences complètes peuvent en fait ne pas toujours être évaluées avec précision avant l'attaque. D'autre part, cet état de choses nécessite un haut niveau de compétence parmi ceux qui lancent des cyberattaques. À cet égard, nous ne pouvons manquer d'invoquer l'expérience du ministère des Armées de la France qui prévoient l'appui des « *experts opérationnels de la cyberdéfense militaire, placés sous la responsabilité du commandant de la cyberdéfense (COMCYBER), disposant des connaissances techniques nécessaires, d'une capacité à exploiter les informations disponibles (exploitation des renseignements collectés, capacité d'identification stricte des cibles, de corrélation entre l'arme et les effets recherchés, etc.), et qui bénéficient de formations dédiées à la complexité de la cyberarme* »[194] lors des cyberopérations dans le respect du principe de précaution.

---

[190] Le gouvernement des États-Unis recourt à Metasploit pour combler ses lacunes sécuritaires : *Forbes*, « Critical Windows Warning Gets Real As Wormable Exploit Weaponized », le 7 septembre 2019, URL : https://www.washingtontimes.com/news/2018/oct/10/government-hackers-using-publicly-available-tools-/ (visité le 13/02/2020).

[191] BACHMANN (Julien), OBERLI (Nicolas), « Le framework Metasploit », *MISC*, No. 52, novembre 2010, URL : https://connect.ed-diamond.com/MISC/MISC-052/Le-framework-metasploit (visité le 13/02/2020).

[192] *Le Figaro*, « Le G7 va mener une simulation de cyberattaque dans la finance », le 10 mai 2019, URL : https://www.lefigaro.fr/flash-eco/le-g7-va-mener-une-simulation-de-cyberattaque-dans-la-finance-20190510 (visité le 23/05/2020).

[193] ICRC, Expert Meeting 14–16 november 2018 – Geneva, The potential human cost of cyber operations, op. cit., p. 32.

[194] Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 16.

Finalement, le commentaire du CICR sur les mesures de précaution indique également qu'il est « *clair que les précautions ne doivent pas faire la vie de la population civile difficile, voire impossible* »[195]. Cependant, l'incapacité d'une partie à prendre des précautions passives n'empêche pas l'autre partie de mener une cyberattaque[196].

Les principes de distinction, de proportionnalité et de précaution que nous venons d'examiner constituent le fondement du droit international humanitaire qui permet de limiter les effets des conflits armés internationaux déclenchés et menés par le bias des cyberattaques. Mais en plus, ces trois « piliers » du DIH servent de base à des autres principes qui peuvent également résoudre le problème de réglementation des cyberarmes.

Section 2 – Les principes supplémentaires du DIH appliqués aux cyberattaques

Les trois piliers du DIH – les principes de distinction, de précaution et de proportionnalité – restent solides aujourd'hui. Néanmoins, certaines organisations internationales humanitaires reconnaissent l'existence d'autres principes qui sont étroitement liés à ceux que nous avions examinés dans le paragraphe précédent. Compte tenu du fait que la quantité de ces principes varient d'une source à l'autre, nous nous concentrons ici seulement sur cinq d'entre eux reconnus par le CICR : l'humanité, l'équilibre entre la nécessité militaire et le principe d'humanité, l'interdiction des maux superflus et des souffrances inutiles, l'égalité des belligérants et non-réciprocité[197].

Après avoir examiné les dispositions de la Convention (IV) de Genève et du Protocole I additionnel, nous pouvons constater que le DIH place l'idée que tout personne a le droit d'être traité, en toutes circonstances, avec humanité en tête de ses priorités. De plus, selon Jean Pictet, le droit humanitaire dans son ensemble s'inspire de ce premier principe[198] – le traitement avec l'humanité – qui trouve son expression dans la disposition suivante[199] :

---

[195] CICR, Les Commentaires sur Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux de 1977, 1987, l'article 58, par. 2245.

[196] HENCKAERTS (Jean-Marie), DOSWALD-BECK (Louise), *Droit international humanitaire coutumier, Volume I : règles*, op. cit., Règle 22, p. 96.

[197] MELZER (Nils), *Droit international humanitaire : introduction détaillée*, CICR, Genève, 2018, pp. 21-24, URL : https://shop.icrc.org/international-humanitarian-law-a-comprehensive-introduction-2752.html (visité le 15/02/2020) ;

[198] «*Humanitarian law receives its impulse from moral science all of which can be summed up in one sentence, "do to others what you would have done to yourself". This crystallizes the wisdom of nations and is the secret of happiness, or at least, of the best order of society*» : PICTET (Jean), «The principles of international humanitarian law», *International Review of the Red Cross*, Vol. 6, Issue 66, septembre 1966, p. 462, URL : https://www.loc.gov/law/mlr/pdf/RC_Sep-1966.pdf (visité le 17/05/2020).

[199] Convention de Genève IV.

Article 27 Traitement I. Généralités

1. Les personnes protégées ont droit, en toutes circonstances, au respect de leur personne, de leur honneur, de leurs droits familiaux, de leurs convictions et pratiques religieuses, de leurs habitudes et de leurs coutumes. Elles seront traitées, en tout temps, avec humanité et protégées notamment contre tout acte de violence ou d'intimidation, contre les insultes et la curiosité publique.

Le principe du « *traitement avec humanité* » revient de manière récurrente non seulement dans les quatre Conventions de Genève, mais également dans le *corpus juris* de la protection de l'individu dans lequel il relie des branches juridiques telles que le droit international humanitaire et le droit international des droits de l'Homme[200]. En particulier, cela a été démontré dans l'affaire Mucić et autres dans laquelle le TPIY a déclaré ce qui suit :

> « *Tant les droits de l'homme que le droit humanitaire ont pour principal objet le respect des valeurs humaines et la dignité de la personne humaine. Ces deux corpus juridiques procèdent d'un souci de la dignité humaine, qui est à la base d'une série de règles humanitaires fondamentales* »[201].

Ce principe revêt une telle importance que la Cour internationale de justice ne pas fait de différence entre les « *considérations d'humanité* » et les « *principes généraux du droit humanitaire* » dans une célèbre affaire *Nicaragua c. États-Unis* de 1986[202].

Le respect du principe de l'humanité revêt un caractère général et absolu « *en toutes circonstances* » et « *en tout temps* »[203] et nous pouvons légitimement penser que la situation de cyberguerre n'exclut pas l'application de ce principe ce qui s'affirme par la clause de Martens qui fait partie du droit humanitaire depuis sa première apparition dans le préambule de la Convention II de La Haye de 1899 concernant les lois et coutumes de la guerre sur terre :

> « *En attendant qu'un code plus complet des lois de la guerre puisse être édicté, les Hautes Parties Contractantes jugent opportun de constater que, dans les cas non compris dans les*

---

[200] ALLAND (Denis), CHETAIL (Vincent), DE FROUVILLE (Olivier), *Unité et diversité du droit international* : écrits en l'honneur du professeur Pierre-Marie Dupuy, op. cit., pp. 161-162.

[201] TPIY, *Le Procureur c. Zejnil Delalić, Zdravko Mucić, Hazim Delić et Esad Landžo*, Chambre d'Appel, Arrêt, le 20 février 2001, par. 149.

[202] *Les « considérations d'humanité » seraient ainsi des principes généraux, une base éthique ou morale, qui s'appliquent en toutes circonstances, en temps de paix comme en temps de conflit armé* » : ABI-SAAB (Rosemary), « Les "Principes généraux" du droit humanitaire selon la Cour internationale de justice », *Revue Internationale de la Croix-Rouge*, 1987, pp. 384-385, URL : https://international-review.icrc.org/sites/default/files/S0035336100091449a.pdf (visité le 15/05/2020).

[203] CICR, Les principes fondamentaux de la Croix-Rouge et du Croissant-Rouge, p. 2, URL : https://www.icrc.org/fre/assets/files/other/icrc_001_0513_principes_fondamentaux_cr_cr.pdf (visité le 16/05/2020).

> *dispositions réglementaires adoptées par Elles, les populations et les belligérants restent sous la sauvegarde et sous l'empire des principes du droit des gens, tels qu'ils résultent des usages établis entre nations civilisées, des lois de l'humanité et des exigences de la conscience publique* »[204].

Cette clause apparaît également à l'article 1 par. 2 du Premier Protocole additionnel sous une forme un peu modifiée.

Toute nécessité militaire de lancer une cyberattaque liée étroitement au principe d'humanité. La quête de cet équilibre représente le deuxième principe fondamental. II est exprimé dans le Préambule de la Déclaration de Saint-Pétersbourg interdisant les projectiles explosifs de 1868 et dispose que « *le seul but légitime que les États doivent se proposer, durant la guerre, est l'affaiblissement des forces militaires de l'ennemi* ». C'est-à-dire l'état de guerre ne donne pas aux parties aucune carte blanche pour mener les hostilités sans aucune contrainte[205].

D'autres principes du droit international découlent logiquement du principe d'humanité, notamment le principe d'interdiction des maux superflus et des souffrances inutiles formulée pour la première fois dans la Déclaration de Saint-Pétersbourg mentionnée ci-dessus. Cette déclaration prévoit l'interdiction de l'emploi des armes qui « *aggraveraient inutilement les souffrances des hommes mis hors de combat, ou rendraient leur mort inévitable* »[206].

En se fondant sur l'article 35 (2) du Protocole I et l'article 23 (e) de la Convention de la Haye, le Manuel de Tallinn dispose :

> **RÈGLE 104 — Maux superflus ou souffrances inutiles**
>
> Il est interdit d'employer des moyens ou méthodes de cyberguerre de nature à causer des maux superflus ou souffrances inutiles.

Les termes « *maux superflus* » et « *souffrances inutiles* » désignent une situation dans laquelle une arme ou un usage particulier d'une arme aggrave les souffrances sans offrir aucun avantage militaire supplémentaire à un attaquant. Au sens étroit, le principe d'interdiction des maux superflus

---

[204] Convention (II) concernant les lois et coutumes de la guerre sur terre et son Annexe: Règlement concernant les lois et coutumes de la guerre sur terre, la Haye, 29 juillet 1899, Préambule.

[205] PA I, article 35, par. 1 ; Règlement de La Haye, article 22 ; Voir aussi SASSOLI (Marco), BOUVIER (Antoine) et QUINTIN (Anne), *How Does Law Protect in War ?*, Chapitre 5, CICR, 2014, URL : https://www.icrc.org/en/doc/assets/files/publications/icrc-0739-part-i.pdf (visité le 16/05/2020).

[206] Déclaration à l'emploi, en temps de guerre, des explosifs sous Projectiles 400 Grammes Poids, 11 décembre 1868.

et des souffrances inutiles limite le choix des méthodes et moyens qui peuvent être utilisés pendant la guerre y compris les poisons et armes empoisonnées ; les armes chimiques et biologiques ; les balles qui s'épanouissent ou explosent dans le corps humain (balles dumdum) ; les armes qui ont pour effet principal de blesser par des éclats qui ne sont pas localisables par rayons X ; les projectiles explosifs et inflammables ; les mines, pièges et dispositifs similaires ; les armes incendiaires et les armes avant tout destinées à brûler des biens ou des personnes ; les armes à laser aveuglantes ; les restes explosifs de guerre ; les mines antipersonnel ; les armes à sous-munitions[207]. Cependant, le droit coutumier reconnaît que les armes interdites ne se limitent pas à cette liste. Il ne faut pas oublier qu'il existe des armes qui sont « *acceptables* », mais dont l'utilisation peut être abusive et provoquer des maux superflus et des souffrances inutiles.

De plus, l'article 36 du Protocole additionnel I sur les armes nouvelles impose aux États de « *déterminer si l'emploi en serait interdit, dans certaines circonstances ou en toutes circonstances, par les dispositions du présent Protocole ou par toute autre règle du droit international applicable à cette Haute Partie contractante* ». L'utilisation abusive de cyberarmes appartient à cette catégorie comme dispose le Manuel de Tallinn :

> **RÈGLE 116 — Choix des moyens ou des méthodes**
>
> Ceux qui planifient ou prennent une décision de lancer une cyberattaque doivent prendre toutes les précautions le plus que possible en ce qui concerne le choix des moyens ou méthodes de guerre employés dans le cadre d'une telle attaque, afin d'éviter et, en tout état de cause, de minimiser les blessures accidentelles des civils, pertes de vies civiles et les dommages ou la destruction d'objets civils.

Le problème majeur lié à ce sujet est la capacité de malware de se propager sans contrôle humain. Le cas le plus fréquemment mentionné à ce sujet est la propagation du ver *Slammer* qui a été le plus rapide dans l'histoire et qui a surchargeait les réseaux et désactivait les serveurs de bases de données[208]. La majorité des experts soulignent que l'utilisation de ce type d'armes constituerait un exemple de violation du DIH[209]. Cette position est partagée par le gouvernement français :

---

[207] HENCKAERTS (Jean-Marie), DOSWALD-BECK (Louise), *Droit international humanitaire coutumier, Volume I : règles*, op. cit., Règle 70, pp. 323-324.

[208] MOORE (David), PAXSON (Vern), SAVAGE (Stefan), SHANNON (Colleen), STANIFORD (Stuart), WEAVER (Nicholas), «Inside the slammer worm», *IEEE Security & Privacy Magazine*, No. 1(4), 2003, p. 33, URL : https://www.researchgate.net/publication/3437498_Inside_the_Slammer_worm (visité le 13/02/2020).

[209] CICR, « Pas de vide juridique dans le cyberspace », le 16 août 2011, URL : https://www.icrc.org/fr/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (visité le 15/02/2020) ; Voir aussi Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 16.

> « *Le recours à des programmes malveillants qui se reproduisent volontairement et se propagent sans contrôle ou réversibilité possible, et donc susceptibles de provoquer des dommages significatifs sur des systèmes ou des infrastructures civiles critiques, est contraire au DIH* »[210].

La question est néanmoins de déterminer la façon dont les auteurs peuvent limiter les conséquences des cyberattaques compte tenu du fait que « *l'incertitude quant aux effets d'une opération* [est] *une caractéristique inhérente aux cyberopérations* »[211] ? De plus, comme les cyberoutils sont principalement constitués de codes, il y a toujours un risque d'erreurs.

Une des méthodes déjà examinées visant à limiter des effets imprévus et involontaires — ne télécharger le malware que dans le système militaire fermé. Parmi les autres mesures nécessaires pour prévenir la production des effets en cascade figurent un contrôle passif, ou autonome, un contrôle actif et un contrôle hybride[212]. Le premier se manifeste dans le fait que la cyberarme elle-même « *observe* » un environnement numérique et agit en fonction de ces observations. Ces mesures peuvent inclure l'activation d'auto-destruction d'un virus sur les clés USB infectées après un certain nombre de jours, ou l'activation du malware sous certaines conditions[213] ce qui était prévu par les auteurs du Stuxnet : « *Stuxnet was designed to cause subtle failures in industrial equipment. Before installing itself, Stuxnet ensures a certain system configuration is present. It first checks the operating system and version, choosing to only target specific Windows systems* »[214]. Lorsque ces circonstances particulières n'existaient pas, le virus restait inerte. Un contrôle actif prévoit que le malware transmet des données par un serveur à un développeur qui, à son tour, décide quelles sont les actions à prendre soit par la transmission des instructions ou des commandes à un malware, soit par des mises à jour de code[215]. Enfin, un contrôle hybride est une combinaison des deux premiers : le malware vérifie si

[210] Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 16.

[211] ICRC, Expert Meeting 14–16 november 2018 – Geneva, The potential human cost of cyber operations, op. cit., p. 38.

[212] RAYMOND (David), CONTI (Gregory), CROSS (Tom), FANELLI Robert, «A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons», 5th International Conference on Cyber Conflict, 2013, p.10, URL : https://ccdcoe.org/uploads/2018/10/8_d1r2s6_raymond.pdf (visité le 15/05/2020).

[213] Par exemple, un malware peut viser certains types de protocoles de transport. Tous les protocoles servent à transmettre des données sur une connexion réseau. Les réseaux civils utilisent le Transport Control Protocol (TCP) et User Datagram Protocol (UDP), tandis que le système SCADA et le système de contrôle des infrastructures (ICS) utilisent ses propres protocoles de transport. Ainsi, un développeur peut programmer qu'un logiciel malveillant propagerait seulement par des protocoles de transport spécifiques.

[214] RAYMOND (David), CONTI (Gregory), CROSS (Tom), FANELLI Robert, «A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons», op.cit., p.8.

[215] *Ibid*, p. 10.

un système répond à certains critères pour s'activer et décide s'il doit contacter un développeur pour recevoir des instructions ou pas[216].

Le dernier principe du droit international humanitaire est le principe d'égalité des belligérants et de non-réciprocité. Il touche la nécessité du respect des dispositions du DIH par toutes les parties au conflit armé indépendamment des motifs qui les animent, de la nature ou de l'origine du conflit[217]. En ce sens ni l'intensité ni les autres facteurs du conflit armé ne peuvent être pris en considération pour justifier des manquements au droit des conflits armés[218], même si une autre partie ne respecte pas les règles de guerre (non-réciprocité des obligations humanitaires)[219].

Pour conclure la première partie de ce travail, nous nous permettons de citer la position exprimée par l'Australie dans son *non paper* avec les études de cas d'application du droit international aux cyberattaques qui est la quintessence des positions de la plupart des États :

> « *[I]f a cyber operation rises to the same threshold as that of a kinetic "attack" (or act of violence) under IHL, the rules governing such attacks during armed conflict will apply to those kinds of cyber operations. Applicable IHL rules will also apply to cyber operations in an armed conflict that do not constitute or rise to the level of an "attack", including the principle of military necessity and the general protections afforded to the civilian population and individual civilians with respect to military operations* »[220]

Comme il ressort de notre analyse, le consensus auquel sont parvenus les différents États, organisations internationales et ONG permet de constater que le droit international humanitaire sera appliqué aux cyberattaques qui sont capables d'engendrer des dommages, des blessures et des morts comme aux actes déclencheurs et aux cyberattaques qui n'ont pas atteint le degré de gravité nécessaire, mais qui accompagnent des conflits armés internationaux existants. Néanmoins, ces normes juridiques resteront lettre morte sans leur application dans la pratique.

---

[216] RAYMOND (David), CONTI (Gregory), CROSS (Tom), FANELLI Robert, «A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons», op.cit., p. 10.

[217] Conventions de Genève I-IV, article 1 commun.

[218] PA I, préambule, al. 5.

[219] Conventions de Genève I-IV, article 1 commun.

[220] Australia's OEWG Non Paper: Case studies on the application of international law in cyberspace, p. 10, URL : https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf (visité le 12/05/2020).

PARTIE 2 — MISE EN ŒUVRE DES RÈGLES DU DIH DANS LE CYBERCONTEXTE

Le conflit armé au sein duquel tous les participants respecteraient les normes du droit et suivraient la loi à la lettre reste aujourd'hui un idéal à atteindre. En effet, il serait utopique de penser que l'existence du corpus de droit international applicable aux conflits armés internationaux et de juridictions chargées de sanctionner les violations de cette branche du droit suffit à garantir pleinement le respect du droit humanitaire. Au contraire, la jurisprudence dont le champ continue à s'élargir nous montre que ce n'est pas le cas et les cyberattaques ne font pas exception.

Comme elles sont susceptibles de violer la souveraineté d'un autre État et déclencher un conflit, cela soulève inévitablement un nombre important d'interrogations sur les réactions possibles de la part de l'État attaqué et de la communauté internationale. Les cyberattaques contre l'Estonie en 2007, contre la Géorgie en 2008, contre l'Iran en 2010 ont démontré que l'enquête qui permettrait identifier les suspects avec certitude prend beaucoup de temps. En même temps, les conséquences d'une cyberattaque peuvent se manifester avec des années de retard ce qui a démontré le cas de Stuxnet. Dans les deux situations, la communauté internationale est confrontée à de nombreux défis.

Nous parlons, tout d'abord, du problème de l'applicabilité du test Caroline qui donne à un État le droit de répondre à une attaque et, en particulier, de l'exigence de l'imminence d'une menace prévue par le test, qui prend un caractère complètement différent dans le cyberespace où il n'y a littéralement qu'un clic à faire pour attaquer. Dans le même temps, la révélation des traces des cyberattaques, ainsi que son auteur après une longue période met en cause le droit de légitime défense en soi. Finalement, la communauté internationale affronte la tâche de punir les responsables des cyberattaques pour empêcher la militarisation d'un cyberespace et garantir le respect du droit international humanitaire.

À cet égard, nous consacrerons une partie substantielle de notre étude à comprendre plus précisément l'exercice du droit de légitime défense (Chapitre 3) et à la responsabilisation des auteurs des cyberattaques (Chapitre 4).

Chapitre 3 — La réaction aux cyberattaques

Le système international moderne régissant l'usage de la force en droit international tire sa force juridique de la Charte des Nations Unies, pour laquelle le maintien de la paix et de la sécurité internationales est le principal objectif. Dans la poursuite de ce but, la Charte interdit aux Etats, « *dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force* »[221]. Cependant, l'interdiction du recours à la force n'est pas absolue. Dans certaines conditions (frôlant le droit fondamental de tout État à la survie[222]) fixées par le droit international, la force peut être utilisée contre un autre État si c'est ce que prévoit la légitime défense (Section 1) ou un tel acte est autorisé par le Conseil de sécurité de l'ONU dans le cadre d'un mécanisme de sécurité collective (Section 2).

Conscient du fait que la cyberattaque est susceptible d'avoir les mêmes effets que celle cinétique et, par conséquent, de déclencher un conflit armé international, nous allons examiner dans les sections suivantes, dans quelle mesure des exceptions au principe de non-recours à la force sont applicables au cyberespace.

Section 1 – Le droit d'un État de légitime défense contre les cyberopérations

Le droit à la légitime défense est considéré comme un élément inhérent à un État qui trouve son origine dans le droit des gens :

> « *§49 (…) Toute nation, comme tout homme, a donc le droit de ne point souffrir qu'un autre donne atteinte à sa conservation, à sa perfection et à celle de son État, c'est-à-dire de se garantir de toute lésion : et ce droit est parfait, puisqu'il est donné pour satisfaire à une obligation naturelle et indispensable* ».
>
> « *§50. Le plus sûr est de prévenir le mal, quand on le peut. Une nation est en droit de résister au mal qu'on veut lui faire, d'opposer la force, et tout moyen honnête, à celle qui agit actuellement contre elle, et même d'aller au-devant des machinations, en*

[221] Charte des Nations Unies, 1945, article 2, par. 4.

[222] « *La Cour ne saurait au demeurant perdre de vue le droit fondamental qu'a tout État à la survie, et donc le droit qu'il a de recourir à la légitime défense, conformément à l'article 51 de la Charte, lorsque cette survies est en cause*» : CIJ, Licéité de la menace ou de l'emploi d'armes nucléaires, Avis consultatif, le 8 juillet 1996, par. 96.

observant toutefois de ne point attaquer sur des soupçons vagues et incertains, pour ne pas s'exposer à devenir elle-même un agresseur injuste »[223].

En exerçant sa souveraineté pleine et entière sur son territoire, les États sont chargés, dans le même temps, de prouver l'existence d'une attaque qui justifierait son propre recours à la force comme légitime défense ce que la CIJ a confirmé dans l'affaire *République islamique d'Iran c. États-Unis d'Amérique* en 2003[224] et ce que nous examinerons ci-après plus en détail.

Étant le seul moyen légitime de recourir à la force armée, le droit à la défense a permis d'établir les garanties de maintien de la paix prévues par les Traités de Westphalie de 1648 et l'équilibre dans les relations internationales. Cependant le concept d'une légitime défense tel que nous le connaissons aujourd'hui est apparu après l'affaire dite *Caroline*. En 1837 les rebelles du Haut-Canada se sont insurgés contre les forces britanniques. Une assistance appréciable a été reçue d'un sympathisant américain qui assurait le ravitaillement des canadiens par le biais du navire « Caroline ». En espérant mettre fin à cette aide, les forces armées britanniques ont attaqué le navire en invoquant que « *necessity of self-defense was instant, overwhelming, leaving no choice of means, and no moment of deliberation (…), and that the British force, even supposing the necessity of the moment authorized them to enter the territories of the United States at all, did nothing unreasonable or excessive; since the act, justified by the necessity of self-defense, must be limited by that necessity, and kept clearly within it* »[225]. Ces anciens critères de nécessité et la proportionnalité de la défense ainsi que la présence ou l'imminence de la menace qui ne laisse ni le choix des moyens ni le temps de délibérer constituent la base juridique sur laquelle les États agissent aujourd'hui[226].

Au niveau international, la reconnaissance du droit à la défense sur le plan législatif déduit des Accords de Locarno qui prévoyaient que le seul usage légitime de la force par les États-parties c'est la nécessité de se défendre[227] ce qui a été consacré par l'article 51 de la charte des Nations unies qui reconnaît qu'« *[a]ucune 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* » et par la décision du Tribunal

[223] DE VATTEL (Emeric), *Le Droit des gens ou Principes de la loi naturelle appliqués à la conduite et aux affaires des nations et des souverains* [1757], Livre II, Tome II, Chap. IV, Paris, Chez Janet et Cotelle, 1820, pp. 277-278.

[224] CIJ, *République islamique d'Iran c. États-Unis d'Amérique*, Jugement, le 6 novembre 2003, paras. 64 et 72.

[225] Cité dans AUST (Anthony), Handbook of International Law, Cambridge University Press, 2010, p. 209.

[226] CASSESE (Antonio), *International Law*, 2ème édition, Oxford, Oxford University Press, 2005, p. 355.

[227] Accords de Locarno, 1925, article 2, URL : https://dl.wdl.org/11586/service/11586.pdf (visité le 03/06/2020).

militaire de Tokyo[228]. En outre, en se fondant sur « *le texte même de l'article 51 mentionnant le "droit naturel" (en anglais "the inherent right") de légitime défense* » [229] la CIJ a reconnu dans l'affaire *Nicaragua* le caractère coutumier de ce droit. Enfin, les dispositions du Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite vont dans le même sens en vertu desquelles le recours à la légitime défense exclut l'illicéité des actions de l'État[230].

Cependant, une analyse plus approfondie de l'article 51 montre sa certaine ambiguïté en ce qui concerne le recours à la légitime défense préemptive, ce qui provoque de vives discussions à cause des différentes interprétations de ces dispositions. Sur le fond, il est indispensable de répondre à la question suivante : le droit international oblige-t-il nous à attendre que des vies soient perdues ou des biens soient endommagés avant que nous puissions entreprendre des actes de légitime défense? Certains experts qui insistent sur une lecture littérale affirment que l'État n'a le droit de légitime défense que si l'attaque a eu lieu[231]. Mais contrairement à cela, il existe un grand nombre des États qui adoptent une vision contraire à la vision restrictive et disent que dans certaines circonstances la force peut se produire quelque temps avant le lieu d'une attaque armée[232]. Kofi Annan, ancien secrétaire général des Nations unies, a déclaré également dans son rapport qu'il partageait ce point de vue : « *Imminent threats are fully covered by Article 51, which safeguards the inherent right of sovereign States to defend themselves against armed attack* »[233]. Bien qu'aucun consensus n'ait encore été réalisé entre les deux écoles, elles s'accordent sur le fait que la légitime défense préventive autorise le recours

---

[228] «*Any law, international or municipal, which prohibits recourse to force is necessary limited by the right of self-defence*» : TMIEO, In re Hirota et autres, 1948, paras. 356, 364, cité dans DINSTEIN (Yoram), *War, Aggression and Self-Defence*, op. cit., p. 181.

[229] CIJ, *Nicaragua c. États-Unis*, Arrêt, 27 juin 1986, par. 176.

[230] Nations Unies, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, 2001, article 21, URL : http://legal.un.org/ilc/texts/instruments/french/commentaries/9_6_2001.pdf (visité le 19/06/2020).

[231] « *[T]his right [of self-defense under Article 51] does not exist against any form of aggression which does not constitute «armed attack». (…) [T]his term means something that has taken place. Art. 51 prohibits «preventive war». The «threat of aggression» does not justify self-defense under Article 51. (…) The «imminent» armed attack does not suffice under Article 51* » : KUNZ (Josef), «Individual and Collective Defense in Article 51 of the Charter of the United Nations», *American journal of International Law*, Vol. 41, p. 872, 1947, cité dans ROBERTSON (Horace), «Self-Defense against Computer Network Attack under International Law», Symposium on Computer Network Attack and International Law, *International Law Studies*, Vol. 76, Naval War College, p. 123, URL : https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1396&context=ils (visité le 12/06/2020).

[232] «*But a State may resort to force in self-defence, even before its territory is penetrated by another State*» : DINSTEIN (Yoram), *War, Aggression and Self-Defence*, op. cit.,p. 189.

[233] Report of the Secretary-General, «In larger freedom: towards development, security and human rights for all», le 21 mars 2005, par. 124, URL : https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=4abcac0e2 (visité le 03/06/2019) ; Voir aussi «*However, a threatened State, according to long established international law, can take military action as long as the threatened attack is imminent, no other means would deflect it and the action is proportionate*» : The Secretary-General's High-level Panel Report on Threats, Challenges and Change, «A more secure world: our shared responsibility», le 2 décembre 2004, par. 188, URL : https://www.un.org/ruleoflaw/files/gaA.59.565_En.pdf (visité le 03/06/2020).

à la force dans un contexte où une riposte est nécessaire et proportionnelle, ce que la CIJ a confirmé dans sa jurisprudence. Par exemple, dans l'affaire des Plates-formes pétrolières, la Cour a estimé que « *[l]es États-Unis doivent également démontrer que leurs actions étaient nécessaires et proportionnées à l'agression armée subie par eux » pour que ses actes puissent justifier l'attaque contre des plateformes pétrolières iraniennes et être interprétés comme légitime défense* »[234]. Aussi, traitant de la question de savoir si l'action militaire menée par l'Ouganda en RDC entre août 1998 et juillet 1999 pouvait être considérée comme un acte de légitime défense, la Cour a déclaré que en prenant compte le fait que « *les conditions préalables à l'exercice du droit de légitime défense n'étant pas réunies dans les circonstances de l'espèce, la Cour n'a pas à se demander si un tel droit de légitime défense a été ou non exercé dans des circonstances caractérisées par la nécessité et s'il l'a été d'une manière proportionnée* »[235] ce qui montre que ces deux éléments sont nécessaires pour justifier le droit à la légitime défense.

Considérons maintenant l'applicabilité du droit à la légitime défense et les principes de la légitime défense préventive par rapport aux cyberattaques. Dans un premier lieu, il est indispensable de noter que le droit d'employer la force en faveur de la légitime défense s'étend non seulement aux attaques armées cinétiques. Cette disposition trouve son affirmation dans le fait que les attaques chimiques, biologiques et radiologiques ont la capacité d'atteindre un tel degré de gravité, de sorte qu'on peut les considérer comme des attaques armées qui déclenchent le droit de légitime défense malgré leur nature non cinétique. En effet, dans son avis consultatif sur la *Licéité de la menace ou de l'emploi d'armes nucléaires*, la CIJ a précisé que les dispositions liées à l'exercice du droit de légitime défense « *s'appliquent à n'importe quel emploi de la force, indépendamment des armes employées* »[236]. La plupart des juristes reconnaissent le recours à ce droit naturel dans le cyberespace aussi[237] :

> **RÈGLE 71 — Légitime défense contre une attaque armée**
>
> L'État qui est la cible d'une cyberopération qui atteint le niveau d'une attaque armée peut exercer son droit inhérent à la légitime défense. La question de savoir si une cyberopération constitue une attaque armée dépend de son ampleur et de ses effets.

[234] CIJ, *République islamique d'Iran c. États-Unis d'Amérique*, Jugement, 6 novembre 2003, par. 51.
[235] CIJ, *République démocratique du Congo c. Ouganda*, Affaire des Activités armées sur le territoire du Congo, Jugement, le 19 décembre 2005, par. 147.
[236] CIJ, Avis consultatif, Licéité de la menace ou de l'emploi d'armes nucléaires, le 8 juillet 1996, par. 39, URL : https://www.icj-cij.org/files/case-related/95/095-19960708-ADV-01-00-FR.pdf (visité le 22/01/2020).
[237] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 71, p. 339.

Par défaut, nous utiliserons dans la présente étude la définition d'une cyberattaque qui atteint le niveau d'une attaque armée telle qu'elle a été décrite dans le chapitre précédent, c'est-à-dire, celle qui est susceptible de provoquer les blessures, les morts, les dommages et la perte de fonctionnalité de l'infrastructure[238] et contre laquelle l'État peut agir en recourant au droit de légitime défense. De plus, en vertu de « *pin prick theory or accumulation of effects* », l'État a la possibilité de se défendre même si plusieurs cyberattaques liées entre elles sont d'un degré inférieur, mais dans sa totalité atteignent le degré de gravite.

Le droit de légitime défense dans le cyberespace est reconnu non seulement par des experts du Manuel de Tallinn, mais également par la majorité des États. En particulier, l'Australie insiste sur le fait que l'État a le droit d'agir lorsque l'État-attaquant a montré son intention délibérée à lancer une attaque armée et lorsque l'État-victime perdrait sa dernière chance de se défendre efficacement à moins qu'elle n'agisse[239]. La France, à son tour, justifie l'invocation de la légitime défense contre les cyberopérations dont les conséquences ont atteint le seuil de gravité nécessaire[240], tout comme les États-Unis qui reconnaissent le recours à ce droit inhérent lorsque cela est justifié («*when warranted*»)[241]. Finalement, nous nous permettons

[238] Il faut constater qu'il n'y a pas de consensus sur l'application du droit à la légitime défense en fonction de la gravité d'une attaque. Par exemple, le juge Simma dans son opinion individuelle a admis le recours à la force contre les actes d'un degré inférieur : « *[I]l existe aussi des actes militaires hostiles d'un degré inférieur, qui n'atteignent pas le seuil de l'«agression armée» au sens de l'article 51 de la Charte des Nations Unies. Contre les actes hostiles de ce genre, un État peut bien entendu se défendre, mais uniquement par des mesures dont la portée et la nature sont plus restreintes (la principale différence résidant dans le fait que la possibilité de légitime défense collective n'existe pas dans ce cas, voir Nicaragua), et qui doivent aussi être très rigoureusement nécessaires et proportionnées, et suivre immédiatement l'acte qui les a motivées* » : CIJ, Affaire des plates-formes pétrolières *République islamique d'Iran c. États-Unis d'Amérique*, le 6 novembre 2003, Opinion individuelle de M. Simma, par. 13. Néanmoins, la majorité des États insistent sur le recours à la légitime défense seulement si l'attaque a atteint le seuil nécessaire de gravité.

[239] Senator the Hon George Brandis QC Attorney-General of Australia, «The right of self-defence against imminent armed attack in international law», Lecture delivered at the T C Beirne School of Law The University of Queensland, le 11 avril 2017, p.8, URL : https://law.uq.edu.au/files/25365/2017%2004%2011%20-%20Attorney-General%20-%20Speech%20-%20The%20Right%20of%20Self-Defence%20Against%20Imminent%20Armed%20Attack%20in%20International%20Law%20-%20for%20publication.pdf (visité le 10/06/2020).

[240] « *Une attaque informatique majeure visant la France, eu égard aux graves dommages qu'elle causerait, pourrait constituer une « agression armée », au sens de l'article 51 de la Charte des Nations unies, et justifier l'invocation de la légitime défense* » : SGDSN, *Revue stratégique de cyberdéfense*, le 12 février 2018, p. 82, URL : http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf (visité le 03/06/2020) ; Voir aussi Réponse de la France à la résolution 73/27 relative aux « Progrès de l'informatique et des télécommunications et sécurité internationale » et à la résolution 73/266 relative à « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale », op. cit., par. 3, a), p. 9.

[241] « *When warranted, the United States will respond to hostile acts in cyber-space as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners* » : White House, International Strategy For Cyberspace, Prosperity, Security, and Openness in a Networked World, mai 2011, p. 14, URL : https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (visité le 12/06/2020).

de citer la position de l'Estonie qui a été la victime d'une célèbre cyberattaque en 2007 et qui a souligné que « *States have the right to react to malicious cyber operations, including using diplomatic measures, countermeasures, and, if necessary, their inherent right of self-defence* »[242].

Cette justification d'une attaque en réponse nous amène à reconnaître comme justes les conclusions faites par le chercheur Walter Sharp par rapport à l'application des critères établis dans l'affaire Caroline au cyberespace :

> « *Recall that anticipatory self-defense is permissible when "the necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation". There seems to be no better circumstance for anticipatory self-defense to apply than when technology allows an unlawful use of force, and potentially an armed attack, to occur literally at the speed of light. The right to respond in anticipatory self-defense does not apply to the penetration of all government computer systems during peacetime, but it should apply presumptively to those sensitive systems that are critical to a state's vital national interests. As previously discussed, any use of force in anticipatory self-defense must be necessary and proportional under international law* »[243].

Le premier critère qu'il faut examiner, c'est la nécessité d'une réponse. Il détermine si la force est le seul moyen pour répondre à une attaque ou si des alternatives pacifiques suffiront. De plus, les États ont l'obligation de « *régler leurs différends par des moyens pacifiques, mais ils gardent une totale liberté dans le choix et l'appréciation de ces moyens* »[244]. Si un État peut contrer une attaque armée réelle ou imminente par des mesures n'impliquant pas la force armée, il n'a aucune justification pour l'utiliser. S'agissant du cyberespace, si les mesures de protection comme le *firewall* sont suffisantes pour contrer la cyberattaque, d'autres mesures, qu'elles soient cyber ou cinétiques, au niveau du recours à la force seront interdites[245]. Cependant, pour

---

[242] Republic of Estonia, Information System Authority, Cyber Security in Estonia 2020, p.4, URL : https://www.ria.ee/sites/default/files/cyber_aastaraamat_eng_web_2020.pdf (visité le 21/07/2020).

[243] SHARP (Walter Gary), *Cyberspace and the use of force*, Aegis Research Corporation, 1999, p. 129, URL : http://www.thomas-hastings.org/CyberSpace%20and%20the%20Use%20of%20Force%20-%20Sharp1999.pdf (visité le 10/06/2020).

[244] DECAUX (Emmanuel), DE FROUVILLE (Olivier), *Droit international public*, 11 édition, Dalloz, 2018, p. 397.

[245] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Règle 72, par. 3, p. 349 ; Voir aussi BARADARAN (Nazanin), HABIBI (Homayoun), «Cyber Warfare and Self - Defense from the Perspective of International Law», *Journal of Politics and Law*, Vol. 10, No. 4, 2017, p. 44, URL : https://www.researchgate.net/publication/319399422_Cyber_Warfare_and_Self_-_Defense_from_the_Perspective_of_International_Law (visité le 20/06/2020).

que l'État-victime utilise légalement la force en prévision d'une attaque, ce dernier doit soit provoquer les mêmes conséquences qu'une attaque armée soit être imminent, ce qui s'applique également au cyberespace[246] :

> **RÈGLE 71 —** Imminence et immédiateté
>
> Le droit de recourir à la force en cas de légitime défense naît si une cyberattaque armée se produit ou elle est imminente. Il est en outre soumis à une exigence d'immédiateté.

Le problème majeur est qu'il existe peu de consensus sur ce qu'il faut entendre par « *imminence* » par rapport à des menaces contemporaines[247]. Parmi les événements qui peuvent indiquer la présence d'une menace imminente nous pouvons indiquer les suivantes : le renforcement des effectifs militaires, l'augmentation des achats de nouvelles armes, les déclarations belligérantes d'intention de déclencher une guerre[248]. D'après l'interprétation plus restrictive, pour que la riposte soit justifiée, elle doit se produire juste au moment où l'attaque est sur le point d'être lancée (c'est à ce moment-là que la menace doit être considérée comme imminente)[249]. Dans le cyberespace, cela signifierait le moment où l'adversaire est sur le point de cliquer sur le bouton qui exécute le code déjà écrit. Si nous adoptons cette vision restrictive de l'imminence, nous ne laissons pas de temps du tout pour l'État-victime pour réagir, parce que le code sera exécuté plus rapidement que, par exemple, la fusée atteindrait l'objectif. C'est pour cette raison que la majorité des experts du groupe du Manuel de Tallinn a rejeté cette interprétation. D'un côté, ils prescrivent à un État-victime potentiel à procéder à une analyse qui détermine si une simple hostilité est devenue une décision d'attaquer[250] et qu'un attaquant éventuel a commencé les préparatifs ou a exprimé implicitement ou explicitement l'intention

---

[246] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 73, p. 350.

[247] BETHLEHEM (Daniel), «Self-Defense Against an Imminent or Actual Armed Attack By Nonstate Actors», *The American Journal of International Law*, Vol. 106, No. 4, octobre 2012, p. 773, URL : https://www.cambridge.org/core/journals/american-journal-of-international-law/article/selfdefense-against-an-imminent-or-actual-armed-attack-by-nonstate-actors/BC9C62E3157202F50234A452A714A421 (visité le 13/06/2020).

[248] En particulier, l'Israël a invoqué ces observations (en vain) après le Conseil de sécurité après l'attaque du réacteur nucléaire de l'Irak en 1981 : «*In the light of Iraqi declarations and deeds, and Iraq's refusal even to sign an armistice agreement with Israel, Israel had full legal justification to exercise its inherent right of self-defense to abort the Iraqi nuclear threat to Israel*» : United Nations Security Council, Attack on Iraq – SecCo debate – Verbatim record, 2288th meeting, New York, le 19 juin 1981, par. 79, URL : https://www.un.org/unispal/document/auto-insert-177361/ (visité le 15/06/2020).

[249] SCHMITT (Michael), «Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework», *Columbia Journal of Transnational Law*, Vol. 37, 1998-1999, p. 930, URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800 (visité le 13/06/2020).

[250] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 73, par. 10, p. 353.

de mener une cyberattaque armée[251]. D'un autre côté, la possibilité de recourir au droit à la légitime défense dépend de l'existence de « *last possible window of opportunity* » qui peut émerger immédiatement avant l'attaque ou bien avant[252]. Dans ce cas, l'État-victime doit prendre en compte plusieurs probabilités avant de riposter[253] :

1) la probabilité que l'adversaire lance réellement une attaque ;
2) la probabilité que l'attaque atteigne réellement le seuil d'une attaque armée ;
3) la probabilité que le moment de *last possible window of opportunity* est venu.

Cependant, un élément déterminant dans ces conclusions — la connaissance d'une cyberattaque en préparation. Ceci est d'autant plus important que certains experts nient l'existence de la légitime défense préventive en soi dans le cyberespace en se référant sur le fait que les États ne savent pas quand une cyberattaque arrive et le temps entre le moment où elle est lancée et le moment où elle atteint sa cible sera minimal[254].

Enfin, une autre question qui se pose inévitablement est de savoir quel est le dernier moment pour exercer le droit à la légitime défense si le dommage, les morts ou les blessures se manifestent seulement après un certain temps et si l'initiateur de l'attaque ne peut être identifié qu'après le décryptage d'un code dans la plupart des cas, ce qui représente en soi l'un des plus grands défis[255]. Si nous examinons le cas du Stuxnet, nous pouvons voir que ce ver a été découvert en 2010, alors qu'il a été lancé en 2009 et il a détruit plus de 1000 centrifuges en Iran au cours de l'année[256]. Le Manuel de Tallinn ne donne pas une réponse précise à cette question et se limite à dire que « *[i]n such cases, the criterion of immediacy is not met unless the conditions described above [necessity and proportionnality] justify taking action* »[257]. Dinstein,

---

[251] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 73, par. 10, p. 353.

[252] *Ibid*, par. 4, p. 351.

[253] HAYWARD (Ryan), «Evaluating the "imminence" of a cyber attack for purposes of anticipatory self-defense», *Columbia Law Review*, Vol. 117, No. 2, pp. 414-415, URL : https://columbialawreview.org/wp-content/uploads/2017/03/399_low.pdf (visité le 12/06/2020).

[254] SCHULLER (Alan), «Inimical Inceptions of Imminence: A New Approach to Anticipatory Self-Defense Under the Law of Armed Conflict», *UCLA Journal of International Law and Foreign Affairs*, Vol. 18, No. 2, 2014, p. 161, URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2701499 (visité le 14/06/2020).

[255] «*The problem with cyber warfare is that technology makes it nearly impossible to attribute the attack to a specific source or to characterize the intent behind it*» : CONDRON (Sean), «Getting It Right: Protecting American Critical Infrastructure in Cyberspace», *Harvard Journal of Law and Technology*, Vol. 20, No 2, p. 415, URL : http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech403.pdf (visité le 13/06/2020).

[256] *Wired*, «An Unprecedented Look at Stuxnet, the World's First Digital Weapon», https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (visité le 10/06/2020).

[257] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 73, par. 14, p. 354 ; Voir aussi «*Cyber attacks can be conducted immediately, so to respond after days, weeks or months after the triggering attack might not be in line with the immediacy requirement*» : HOLMBERG (Elin Jansson),

à son tour, souligne que l'intervalle entre une attaque armée et un acte de légitime défense peut être long, si cette réponse tardive est objectivement justifiée[258]. Mais comme chaque cyberattaque et ses conséquences peuvent être uniques, il serait logiquement de supposer que l'interprétation de la proximité dans le temps entre ces deux actions dépend du contexte de chaque situation.

S'agissant de la proportionnalité de la légitime défense, Cassesse souligne que ce principe prévoit, d'une part, l'assurance de l'équilibre entre le préjudice causé par l'État attaquant et la riposte, ou du moins l'assurance que des attaques en réponse ne dépassent pas sérieusement le préjudice créé par le fait illicite, et d'autre part, l'assurance que le seul but de la légitime défense est de forcer l'attaquant à mettre fin à son comportement illicite[259]. Ce qui est important par rapport au cyberespace, c'est que le principe de proportionnalité n'exige pas que les armes utilisées pour la légitime défense soient les mêmes que celles qui ont été utilisées par l'État attaquant[260], si la riposte est proportionnelle à son acte[261]. La proportionnalité devrait donc apparemment être fondée sur une évaluation de la force utilisée par l'État-attaquant. À ce sujet, il n'est pas superflu de rappeler l'exemple d'Israël qui a lancé une frappe aérienne sur un bâtiment à Gaza où se trouvaient les hackers de Hamas en réponse à leur cyberattaque. Mais la question qui se pose est si l'attaque cinétique a été proportionnelle à la cyberattaque de Hamas ? Malheureusement, la seule chose que l'armée israélienne a publié sur Twitter à ce sujet est la suivante : « *We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work. HamasCyberHQ.exe has been removed* »[262].

Comme l'a déclaré l'armée israélienne, elle a réussi non seulement à neutraliser la menace, mais également à détruire un bâtiment. Par conséquent, plusieurs personnes ont été tuées. Cette situation nous amène à nous demander si la cyberattaque de Hamas consistait également à provoquer les morts parmi les Israliens ou son but n'était que d'établir un accès au

---

«Armed attacks in cyberspace : Do they exist and can they trigger the right to self-defence?», Thesis in International Law, Faculty of Law, Stockholm University, p. 42, URL : http://www.diva-portal.org/smash/get/diva2:854660/FULLTEXT01.pdf (visité le 10/06/2020).

[258] DINSTEIN (Yoram), *War, Aggression and Self-Defence*, op. cit., p. 243.

[259] CASSESE (Antonio), *International Law*, 2ème édition, op. cit., p. 306.

[260] GRAY (Christine), *International Law and the Use of Force*, Oxford, Oxford University Press, 2008, p. 150 ; Voir aussi SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 73, par. 5, p. 349.

[261] DINSTEIN (Yoram), «Computer Network Attacks and Self-Defense», op.cit., p. 109.

[262] Israel Defense Forces, Twitter, URL : https://twitter.com/IDF/status/1125066395010699264 (visité le 13/06/2020).

système la collecte de renseignements ? Il est peu probable qu'on ait une réponse prochainement, ce qui signifie que l'application du droit international aux cyberattaques demeure un majeur problème dans la pratique.

Toutefois, outre la légitime défense individuelle, l'État-victime peut compter sur celle collective en vertu de l'article 51 qui repose souvent sur des obligations mutuelles des États en vertu d'un traité de sécurité. L'existence de telles obligations joue un rôle préventif, car un agresseur potentiel en cas d'attaque armée ne traitera pas avec un, mais avec au moins plusieurs, voire avec tout un groupe d'États. Tout au long de l'histoire des relations internationales, le principe de la légitime défense collective a été au cœur de la plupart des alliances militaires. Nous pouvons citer à titre d'exemple les événements de la Première Guerre mondiale qui étaient largement déterminés par les engagements des alliés. Cependant, la base du principe de la légitime défense collective a été jetée simultanément avec la création de la Société des Nations qui a prévu dans sa Charte la disposition, en vertu de laquelle « *[l]es membres de la Société s'engagent à respecter et à maintenir contre toute agression extérieure l'intégrité territoriale et l'indépendance politique présente de tous les membres de la Société* »[263]. C'est sur la base de cet article que la Charte des Nations Unies a adopté la disposition sur le droit naturel de légitime défense collective dans son article 51.

Le groupe international d'experts du Manuel de Tallinn a exprimé l'opinion que cette norme est applicable au cyberespace[264] :

> **RÈGLE 74 —** Légitime défense collective
>
> Le droit de légitime défense peut être exercé collectivement. L'autodéfense collective contre une cyberopération équivalant à une attaque armée ne peut être exercée qu'à la demande de l'État victime et dans le cadre de la demande

S'agissant des conditions dans lesquelles les États peuvent recourir à ce droit, nous devons constater qu'elles reprennent en partie celles, prévues pour la légitime défense individuelle, à savoir l'existence d'une menace imminente, la nécessité d'une riposte et sa proportionnalité. Cependant, la détermination si la condition de l'imminence est remplie est laissée à la discrétion d'un État-victime. Donc, c'est après l'autorisation d'un État attaqué qu'un

[263] Traité de Versailles de 1919, Pacte de la Société des Nations, art. 10.

[264] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 74, p. 354.

autre Etat peut venir en aide. Ce qui est non moins important, c'est que l'État-victime doit envoyer une demande d'assistance avant trouver de l'aide dans la lutte contre l'État-agresseur[265].

Nous nous permettons d'attirer l'attention sur deux traités les plus connus prévoyant la légitime défense collective. Le premier exemple est le Traité de l'Atlantique Nord du 4 avril 1949 qui dispose ce qui suit :

> « ***Article 5.***
>
> *Les parties conviennent qu'une attaque armée contre l'une ou plusieurs d'entre elles survenant en Europe ou en Amérique du Nord sera considérée comme une attaque dirigée contre toutes les parties, et en conséquence elles conviennent que, si une telle attaque se produit, chacune d'elles, dans l'exercice du droit de légitime défense, individuelle ou collective, reconnu par l'article 51 de la Charte des Nations Unies, assistera la partie ou les parties ainsi attaquées en prenant aussitôt, individuellement et d'accord avec les autres parties, telle action qu'elle jugera nécessaire, y compris l'emploi de la force armée, pour rétablir et assurer la sécurité dans la région de l'Atlantique Nord* ».

En reconnaissant le cyberespace en tant que théâtre de guerre, l'Alliance atlantique a déclaré en septembre 2014 que « *la cyberdéfense relève de la tâche fondamentale de l'OTAN qu'est la défense collective. Il reviendrait au Conseil de l'Atlantique Nord de décider, au cas par cas, des circonstances d'une invocation de l'article 5 à la suite d'une cyberattaque* »[266]. Étant consciente du fait que les membres de l'OTAN partagent le même cyberespace et que la cybersécurité de tous entre eux en dépend, l'Alliance atlantique assume ses responsabilités renforcer les cybercapacités des États-parties et améliorer leur formation et entraînement à la cyberdéfense[267].

À ce jour, l'OTAN a recouru plusieurs fois à l'article 5, par exemple, vivement préoccupé par le conflit entre l'Ukraine et la Russie, l'Alliance atlantique a créé des fonds

---

[265] « *[L]a Cour note qu'en droit international coutumier, qu'il soit général ou particulier au système juridique interaméricain, aucune règle ne permet la mise en jeu de la Iégitime défense collective sans la demande de l'État se jugeant victime d'une agression armée. La Cour conclut que l'exigence d'une demande de l'État victime de l'agression alléguée s'ajoute à celle d'une déclaration par laquelle cet État se proclame agressé* » : CIJ, *Nicaragua c. États-Unis*, Arrêt, le 27 juin 1986, par. 199.

[266] OTAN, Déclaration du sommet du Pays de Galles, le 5 septembre 2014, par. 72, URL : https://www.nato.int/cps/fr/natohq/official_texts_112964.htm (visité le 15/06/2020).

[267] OTAN, Cyberdéfense, le 31 mars 2020, URL : https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=fr (visité le 15/06/2020).

fiduciaires en 2014 pour soutenir l'Ukraine dans six domaines : «*commandement, contrôle, communications et ordinateurs, logistique et standardisation, réadaptation médicale, transition de carrière pour les militaires, lutte contre les engins explosifs improvisés, cyberdéfense*»[268]. En 2015 et en 2016, l'OTAN a adopté les mesures d'assistance supplémentaires afin de renforcer des « *capacités techniques défensives de l'Ukraine pour lutter contre les cybermenaces* »[269]. Ces mesures incluaient la création du centre de gestion des incidents dans le but de surveiller les événements de cybersécurité, ainsi que la création des laboratoires pour enquêter sur les incidents de cybersécurité, la mise en œuvre de programmes de formation sur l'utilisation des cybertechnologies et équipements[270].

Un autre exemple qui mérite d'être cité est celui de l'Union européenne (ci-après l'UE) dont le traité prévoit également le droit à la légitime défense collective[271] :

> ***« Article 42, paragraphe 7.***
>
> *Au cas où un État membre serait l'objet d'une agression armée sur son territoire, les autres États membres lui doivent aide et assistance par tous les moyens en leur pouvoir, conformément à l'article 51 de la charte des Nations unies ».*

Comme l'OTAN, l'UE reconnaît que le droit international s'applique au cyberespace et, par conséquent, s'engage à défendre ses membres contre les cyberattaques depuis l'adoption des premières règles dans ce domaine en 2016[272]. Une nouvelle étape importante en cette matière a été franchie avec l'adoption d'une décision qui autorise des sanctions contre les cyberattaques qui menacent l'Union ou ses États membres. Dans ce texte, le Conseil a défini les cyberattaques qui relèvent de la compétence de l'UE, à savoir les attaques contre les infrastructures critiques, les services nécessaires au maintien d'activités critiques, les fonctions critiques des États, le stockage ou le traitement des informations classifiées et les équipes

---

[268] The White House, FACT SHEET: U.S. and NATO Efforts in Support of NATO Partners, including Georgia, Ukraine, and Moldova, le 9 juillet 2016, URL : https://obamawhitehouse.archives.gov/the-press-office/2016/07/09/fact-sheet-us-and-nato-efforts-support-nato-partners-including-georgia (visité le 15/06/2020).

[269] NATO, Comprehensive Assistance Package for Ukraine, juillet 2016, p. 2, URL : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_09/20160920_160920-compreh-ass-package-ukraine-en.pdf (visité le 15/06/2020).

[270] NATO, NATO's practical support to Ukraine, décembre 2015, p. 1, URL : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151130_1512-factsheet-nato-ukraine-supportr_en.pdf (visité le 15/06/2020).

[271] Traité sur l'Union Europeenne modifié jusqu'au traité de Lisbonne de 2009; entrée en vigueur le 1er décembre 2009, art. 42, par. 7.

[272] Union européenne, Directive 2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, URL : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148 (visité le 15/06/2020).

d'intervention d'urgence[273]. C'est contre ces cyberattaques l'UE a le droit d'imposer des sanctions pour défendre ses membres.

De plus, en tant que partenaire de l'OTAN depuis l'adoption de l'arrangement technique sur la cyberdéfense du 10 février 2016, l'UE coopère avec l'Allience atlantique, dans les domaines de l'échange d'informations, de la formation, de la recherche et des exercices, ainsi que le partage des pratiques de référence entre les équipes d'intervention d'urgence pour renforcer les capacités techniques mutuellement et mieux se préparer contre la menace potentielle qui pourrait provoquer l'exercice de l'article 51 de la Charte de l'ONU.

Néanmoins, l'autorisation unilatérale de recours à la force est une mesure garantissant l'intégrité des États jusqu'à ce que la communauté internationale puisse réagir, comme le prévoit la Charte : « *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* ». Ainsi, nous pouvons supposer que les actions des systèmes collectifs de protection ainsi que des États eux-mêmes dans le but de se défendre se limitent à l'autorité du Conseil de sécurité. Puisque le droit à la légitime défense est délégué à eux jusqu'à ce que le Conseil réagira à l'usage illégal de la force dans telle ou telle région du monde[274].

Section 2 – Les actions de Conseil de sécurité de l'ONU en réponse à des cyberopérations pour le maintien de la paix

Le processus visant à contenir les cybermenace au sein des Nations Unies a commencé en 1998 par la présentation du projet de résolution sur la cybersécurité par la Fédération de Russie[275]. À partir de ce moment, l'ONU est devenue le tremplin qui a lancé les discussions pour trouver les réponses politiques et juridiques qui reflètent l'urgence de ces menaces, pour empêcher la militarisation croissante du cyberespace et pour s'orienter vers une cyber paix. C'est à cette fin qu'en 2004,

[273] Conseil de l'Union européenne, Décision du Conseil concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, le 14 mai 2019, art. 1, URL : http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/fr/pdf (visité le 16/06/2020).

[274] « *Les États portent à la connaissance du Conseil les mesures prises* [en vertu de l'article 51] *et les cessent dès que ce dernier aura pris les mesures nécessaires pour le maintien de la paix internationale* » : Action en cas de menace contre la paix, de rupture de la paix et d'acte d'agression (Chapitre VII), article 51, URL : https://www.un.org/securitycouncil/fr/content/repertoire/actions (visité le 20/06/2020).

[275] La conséquence des discussion à ce sujet a été l'adoption de la Résolution 53/70 relative aux progrès de la téléinformatique dans le contexte de la sécurité internationale, voir Assemblée générale des Nations Unies, Résolution 53/70 (1999), le 4 janvier 1999, URL : https://undocs.org/fr/A/RES/53/70 (visité le 20/06/2020).

l'Assemblée générale des Nations Unies a créé le Groupe d'experts gouvernementaux (ci-après le GGE) dont le mandat englobe l'examen de la question « *des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information* »[276]. Les quatre sessions du GGE a permis de révéler de plusieurs problèmes qui pourraient constituer une menace à la paix et à la sécurité internationale. Parmi ces problèmes sont les attaques contre des infrastructures essentielles, le danger des déstabilisateurs qui, à son tour, peuvent provoquer un conflit[277]. Les conclusions présentées par un Groupe de travail à composition non limitée, qui a été crée en 2018, vont dans le même sens et ajoutent, entre outres, l'exploitation des fonctionnalités cachées nuisibles, l'interdépendance provoquée, en particulier, par le phénomène Internet des objets, la vulnérabilité des infrastructures critiques à la liste des menaces potentielles pour la paix et la sécurité[278]. Le rapport de l'Institut des Nations Unies pour la recherche sur le désarmement (ci-après UNIDIR) a montré une nouvelle fois la volonté de l'ONU de maintenir la paix dans le cyberespace[279]. De plus, la dépendance croissante de la société mondiale aux TIC et de leur utilisation malveillante notée par l'organisation a conduit à la nécessité de prendre en compte des TIC dans les missions de maintien de la paix et de la sécurité internationale par le haut responsable de l'ONU et les dirigeants des Nations Unies.

Nous devons également mentionner les efforts d'UNIDIR qui ont permis d'établir des règles et recommandations applicables dans le domaine des TIC[280] :

1. Le droit international, et en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité dans le cybercontexte ;
2. Les efforts visant à assurer la sécurité des TIC doivent aller de pair avec le respect des droits de l'Homme et des libertés fondamentales énoncés dans la Déclaration universelle des droits de l'Homme et d'autres instruments internationaux ;
3. Les États doivent coopérer contre l'utilisation des TIC à des fins criminelles qui représentent une menace sérieuse pour la population civile, notamment en harmonisant les approches juridiques et en renforçant la collaboration entre les services de répression et les services de poursuites ;

---

[276] Assemblée générale des Nations Unies, Résolution 58/32, le 18 décembre 2003, par. 4, URL : https://undocs.org/fr/A/RES/58/32 (visité le 20/06/2020).

[277] Assemblée générale des Nations Unies, Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, op. cit., paras. 5 et 7.

[278] OEWG on developments in the field of information and telecommunications in the context of international security, Second «Pre-draft» of the report, paras. 18, 21, 22, URL : https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf (visité le 20/06/2020).

[279] UNIDIR, « The United Nations, Cyberspace and International Peace and Security », Responding to Complexity in the 21st Century, 2017, p.3, URL : http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf (visité le 21/06/2020).

[280] UNIDIR, « The United Nations, Cyberspace and International Peace and Security », 2017, op. cit., pp. 20-23.

4. Les États doivent encourager le secteur privé et la société civile à améliorer la sécurité des TIC et leur utilisation, y compris la sécurité de la chaîne d'approvisionnement des produits et services des TIC ;
5. Les États doivent respecter, entre autres, les principes du droit international, la souveraineté des États, l'égalité souveraine, le règlement des différends par des moyens pacifiques et la non-intervention dans les affaires des autres États. En particulier, les États doivent respecter les obligations que leur impose le droit international en matière de respect des droits de l'Homme et des libertés fondamentales ;
6. Les États doivent prendre dûment en considération les principes d'humanité, de nécessité, de proportionnalité et de distinction ;
7. Les États ne doivent pas sciemment permettre que leur territoire soit utilisé pour des faits internationalement illicites utilisant les TIC ;
8. Les États doivent prendre les mesures appropriées pour protéger leurs infrastructures critiques des menaces liées aux TIC, en tenant compte de la résolution 58/199 de l'Assemblée générale sur la création d'une culture mondiale de la cybersécurité ;
9. Les États doivent s'efforcer d'empêcher la prolifération d'outils et de techniques TIC malveillants.

Cet état de choses montre à quel point le sujet des cyberattaques est important dans l'agenda de l'ONU, d'autant plus que l'organisation est devenue elle-même victime d'une attaque dans le cyberespace l'année dernière[281]. Dans le même temps, les préoccupations et les recommandations susmentionnées peuvent constituer une aide précieuse non seulement pour les États qui élaborent leurs propres stratégies nationales en matière de la cybersécurité. En particulier, elles peuvent être utilisées dans l'activité du Conseil de sécurité qui est le seul organe chargé de fixer « *l'existence d'une menace à la paix, d'une rupture de la paix ou d'un acte d'agression* »[282] et de prendre des mesures en vertu des articles 41 et 42 de la Charte des Nations Unies pour rétablir la paix et la sécurité internationales. Par ailleurs, le caractère obligatoire des résolutions prises par le Conseil à l'égard des

[281] ONU, «L'ONU précise que la cyberattaque dont elle a été victime n'a pas compromis de données sensibles», le 31 janvier 2020, URL : https://news.un.org/fr/story/2020/01/1060882 (visité le 25/06/2020) ; Voir aussi «*The damage related to this specific attack has been contained, and additional mitigation measures implemented. Nevertheless, the threat of future attacks continues, and the United Nations Secretariat detects and responds to multiple attacks of various level of sophistication often*» : *Reuters*, «UN offices in Geneva, Vienna targeted by 'well-resourced' cyber attack last year», le 29 janvier 2020, URL : https://fr.reuters.com/article/rbssTechMediaTelecomNews/idUKL1N29Y1BV (visité le 27/06/2020).

[282] Charte des Nations Unies, 1945, article 39.

parties au conflit et leur valeur juridique contraignante[283] permet d'assurer le respect du droit international humanitaire.

Il est entendu que le plan d'action de l'ONU pendant les conflits au cours desquels les parties utilisent les cyberarmes englobe les mêmes pas prévus par la Charte[284]. Cela signifie que le Conseil de sécurité doit, en premier lieu, déterminer s'il existe une « *menace pour la paix, une rupture de la paix ou un acte d'agression* » en vertu de l'article 39, et dans l'affirmative, faire des recommandations ou prendre des mesures provisoires, comme le prescrit l'article 40, et dans le cas de non-exécution de ces mesures, il devra déterminer quelles mesures seront prises conformément aux articles 41 et 42.

S'agissant du premier pas, il faut noter que, comme le CSNU a fait observer que la menace pour la paix existe « *uniquement dans des situations impliquant le recours à la force armée* »[285]. De nombreuses sessions du Conseil montrent que la détermination de l'existence d'une menace doit se reposer principalement sur les faits et les circonstances de la situation en question:

> *« Il peut y avoir des faits qui montrent qu'il existe une menace contre la paix et il est fort possible que la rupture effective de la paix ne se produise pas à ce moment. Tout dépend des circonstances et il faut procéder à une enquête pour établir les faits et les examiner.*
> *Dans le cas présent, le Sous-Comité chargé par le Conseil de sécurité d'examiner les faits a constaté, d'après les documents qui lui étaient soumis, que la situation ne tombait pas sous le coup de l'Article 39 et qu'il n'existait pas de menace contre la paix. Ce n'est donc pas une question d'interprétation juridique ; il s'agit de témoignages probants, il s'agit de prouver des faits »* [286]

[283] Voir les résolutions de Conseil de Sécurité de Nations unies suivantes : 1265 (1999), 1296 (2000), 1674 (2006), 1738 (2006), 1894 (2009), 2175 (2014), 2222 (2015), 2365 (2017), 2286 (2016) et 2417 (2018).

[284] UNIDIR, « The United Nations, Cyberspace and International Peace and Security », Responding to Complexity in the 21st Century, op. cit., p. 16 ; Voir aussi «*If the Security Council does qualify a cyber operation as a threat to the peace, breach of the peace, or act of aggression, it could make recommendations under Article 39, adopt measures aimed at preventing the worsening of the crisis under Article 40, and, more importantly, adopt coercive measures under Articles 41 and 42*» : ROSCINI (Marco), *Cyber Operations and the Use of Force in International Law*, OUP Oxford, 2014, p. 114.

[285] ONU, Répertoire de la pratique du Conseil de sécurité, par. 12, URL : https://www.un.org/fr/sc/repertoire/faq.shtml (visité le 22/06/2020).

[286] Conseil de sécurité, Quarante septième séance, le 18 juin 1946, Ordre du jour provisoire (document S/89), p. 376, URL : https://undocs.org/fr/S/PV.47 (visité le 22/06/2020).

Pour être au courant de toute menace, le Conseil suit lui-même l'évolution des conflits et des situations existants[287], mais les États-membres de l'ONU ont également l'obligation de porter à la connaissance du Conseil les mesures prises par eux dans l'exercice de ce droit de légitime défense[288].

Bien que le Conseil de sécurité n'ait jamais identifié les cyberopérations comme une menace pour la paix ou pouvant représenter une rupture de la paix ou un acte d'agression, nous pouvons noter que le Conseil, toutefois, admet cette possibilité[289]. À cet égard, nous nous permettons de rappeler la réunion qui a marqué la première fois que le sujet des cyberattaques a été soulevé au sein du CSNU. En février 2020 le ministère des Affaires étrangères de Géorgie a adressé une lettre au Secrétaire général et au Président du Conseil de sécurité pour examiner la cyberattaque contre l'infrastructure georgienne :

> *« On 28 October 2019, a large scale cyber-attack was launched against the websites, servers and other operating systems of the Administration of the President of Georgia, the courts, various municipal assemblies, state bodies, private sector organizations and media outlets. As a result of the cyber-attack, the servers and operating systems of these organizations were significantly damaged, severely affecting their functionality.*
> *The above-mentioned cyber-attack was targeted at Georgia's national security and was intended to harm Georgian citizens and government structures by disrupting and paralyzing the functionality of various organizations, thereby causing anxiety among the general public »*[290].

Dans sa lettre la Georgie a condamné la Fédération de Russie en invoquant les résultats de l'enquête menée à la fois par les autorités internes et par les « *partenaires* » de l'État[291]. Le 5 mars, lors de la réunion privée auprès le Conseil de sécurité, l'Estonie, les États-Unis et le Royaume-Uni ont adhéré à la déclaration georgienne et ajouté que c'était « *clear that Russia's military intelligence service - the GRU - conducted these cyber-attacks in an attempt to sow discord and disrupt the lives*

---

[287] Security Council, Repertoire of the Practice of the Security Council, Actions with respect to threats to the peace, breaches of the peace, and acts of aggression (Chapter VII of the Charter), Advance version, 21st Supplement, 2018, p. 8, URL : https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/scpcrb.repertoire.part_vii.21st_supplement_2018_for_webposting.pdf#page=8 (visité le 23/06/2020).

[288] Charte des Nations Unies, 1945, article 51.

[289] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 76, par. 2., p. 357.

[290] Security Council, Identical letters dated 21 February 2020 from the Permanent Representative of Georgia to the United Nations addressed to the Secretary-General and the President of the Security Council, le 24 février 2020, p. 2, URL : https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2020_135.pdf (visité le 23/06/2020); Voir aussi Statement of the Ministry of Foreign Affairs of Georgia, le 20 mars 2020, URL : https://mfa.gov.ge/cmsctx/culture/en-US/-/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5 (visité le 23/06/2020).

[291] *Ibid.*

of ordinary Georgian people »[292] et que « *[r]aising this issue today at the Security Council table is historic and shows that behaviour undermining the stability of cyberspace is not ignored. (…) We are convinced that the Security Council must deal with new issues that threaten international peace and security and are only gradually making their way to the agenda of the Security Council* »[293]. Bien que la décision du Conseil sur le caractère de cette cyberattaque et sur les responsables de ces actes demeure inconnue pour l'instant, elle montre la volonté des États – et donc celle du Conseil de sécurité – de prendre en compte les cyberattaques qui pourraient présenter une menace pour la paix et la sécurité internationales.

Cette constatation est renforcée par le fait que les États membres continuent à signaler la nécessité des actions de la part du CSNU. En particulier, le 22 mai 2020 à la réunion sur les défis de la cyber-paix et de la sécurité provoqués par la pandémie de COVID-19, le Japon a déclaré que le Conseil de sécurité devrait être « *prêt à agir* » conformément au Chapitre 6 ou au Chapitre 7 de la Charte afin de prévenir ou de réagir « *à une situation grave liée aux cyberactivités* »[294]. Tandis que le CICR a noté que le Conseil a déjà adopté de nombreuses résolutions exhortant les parties belligérantes à respecter les règles fondamentales du DIH, précisant qu'elles doivent également être respectées dans le cyberespace[295]. Enfin il est nécessaire de citer la position de l'Australie et celle de l'Irlande d'après lesquelles il y a une nécessité de mettre en œuvre des règles existantes et d'exiger « *une plus grande responsabilité pour leurs violations* » au lieu de fixer de nouvelles règles ce qui représente un vrai défi aujourd'hui[296].

Cependant, avant de passer à l'examen des mesures qui le Conseil peut prendre pour faire face aux cyberattaques menaçant la paix et la sécurité internationales dans le cybercontexte, il serait préférable de traiter les mesures « *classiques* » qui pourraient servir de point de départ pour les discussions sur leur application aux cyberattaques.

Parmi les mesures n'impliquant pas l'emploi de la force armée, la Charte de l'ONU prévoit « *l'interruption complète ou partielle des relations économiques et des communications ferroviaires,*

---

[292] United States Mission to the United Nations, Joint Statement by Estonia, the United Kingdom, and the United States at a Press Availability on Russian Cyberattacks in Georgia, le 5 mars 2020, URL : https://usun.usmission.gov/joint-statement-by-estonia-the-united-kingdom-and-the-united-states-at-a-press-availability-on-russian-cyberattacks-in-georgia/ (visité le 23/06/2020).

[293] Ministry of Foreign Affairs of Estonia, Estonia raised cybersecurity for the first time at the UN Security Council, le 5 mars 2020, URL : https://vm.ee/en/news/estonia-raised-cybersecurity-first-time-un-security-council (visité le 23/06/2020).

[294] Ministry of Foreign Affairs of Estonia, Signature Event of Estonia's UNSC Presidency: Cyber Stability, Conflict Prevention and Capacity Building, le 22 mai 2020, URL : https://vm.ee/en/activities-objectives/estonia-united-nations/signature-event-estonias-unsc-presidency-cyber (visité le 25/06/2020).

[295] Ministry of Foreign Affairs of Estonia, Signature Event of Estonia's UNSC Presidency: Cyber Stability, Conflict Prevention and Capacity Building, op.cit.

[296] *Ibid.*

maritimes, aériennes, postales, télégraphiques, radioélectriques et des autres moyens de communication, ainsi que la rupture des relations diplomatiques »[297] afin de protéger les États. Le Conseil de sécurité a utilisé l'article 41 pour régler des situations de conflits au Yémen, au Soudan du Sud, en Somalie, en Érythrée, en République démocratique du Congo, au Libéria, en Côte d'Ivoire, au Soudan, en Iraq, au Liban, en République de Corée et en Guinée Bissau, pour résoudre des conflits entre les talibans et Al-Qaida et s'est référé à cet article dans les préambules des résolutions 2141 (2014), 2159 (2014), 2206 (2015), 2207 (2015) et 2224 (2015), ainsi que dans les dispositions des résolutions 2231 (2015) et 2250 (2015) (Annexe 2 et Annexe 3)[298]. Par exemple, pour protéger des civils contre les conséquences du conflit au Darfour, dans sa résolution 2200 (2015) le Conseil a imposé un embargo sur les armes au Soudan[299] et a prévu des sanctions (la restriction de l'entrée sur le territoire du Soudan, le passage en transit par ce territoire et le gel des fonds, avoirs financiers et ressources économiques[300]) dans sa résolution 1591 (2005) à l'égard des personnes qui ont violé le droit international humanitaire.

Dans les situations où les mesures décrites à l'article 41 sont inadéquates, le Conseil a le droit de recourir aux moyens de « *forces aériennes, navales ou terrestres, pour toute action qu'il juge nécessaire au maintien ou au rétablissement de la paix et de la sécurité internationales. Cette action peut comprendre des démonstrations, des mesures de blocus et d'autres opérations exécutées par des forces aériennes, navales ou terrestres de Membres des Nations Unies* »[301]. La seule restriction de la mise en œuvre de cet article est le fait que les mesures susmentionnées devraient être prises « *dans le respect le plus strict du droit international (…) et de la politique de diligence voulut en matière de droits de l'Homme dans le contexte de la fourniture d'appui par l'ONU à des forces de sécurité non onusiennes* »[302]. Guidé par ce motif le Conseil a autorisé l'utilisation de la force par la Mission conjointe des Nations Unies et de l'Union africaine au Darfour (ci-après MINUAD), la Mission des Nations Unies au Soudan du Sud (ci-après MINUSS) et la Force intérimaire de sécurité des Nations Unies pour Abyei (ci-après FISNUA) et a souligné que l'autorisation de recourir à la force comprenait

[297] Charte des Nations Unies, 1945, article 41.

[298] Department of Political Affairs - Security Council Affairs Division Security Council Practices and Charter Research Branch, «Repertoire of the Practice of the Security Council », 19th Supplement, Part VII, «Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter)», 2014-2015, pp. 36-38, URL : https://www.un.org/en/sc/repertoire/2014-2015/Part_VII/2014-2015_Part_VII.pdf#page=36 (visité le 25/06/2020).

[299] Conseil de sécurité des Nations Unies, Résolution 2200 (2015), le 12 février 2015, p.4, URL : http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2200%20(2015)&Lang=F (visité le 20/06/2020).

[300] Conseil de sécurité des Nations Unies, Résolution 1591 (2005), le 29 mars 2005, par.4, URL : http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1591(2005)&Lang=F (visité le 20/06/2020).

[301] Charte des Nations Unies, 1945, article 42.

[302] Conseil de sécurité des Nations Unies, Résolution 2211 (2015) le 26 mars 2015, par. 9 (e), URL : http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2211%20(2015)&Lang=F (visité le 20/06/2020).

également la prise de « *toutes les mesures nécessaires* » pour maintenir la paix et la sécurité internationales.

Le Manuel de Tallinn réaffirme la légitimité de l'activité du Conseil de sécurité au cours d'un conflit armé et propose l'application de ces règles dans le cybercontexte :

> **RÈGLE 76 — Conseil de Sécurité des Nations Unies**
>
> Si le Conseil de Sécurité des Nations Unies décide qu'un acte constitue une menace pour la paix, une rupture de la paix ou un acte d'agression, il peut autoriser des mesures non-contraignantes, notamment des cyberopérations. Si le Conseil de Sécurité estime que ces mesures sont inadéquates, il peut décider de prendre des mesures coercitives, notamment des mesures cybernétiques.

S'agissant des mesures qui peuvent être prises en vertu de l'article 41 en réponse de l'attaque armée et, en particulier, en réponse d'une cyberattaque il est nécessaire de citer l'arrêt Tadic :

> *« Il est évident que les mesures visées à l'article 41 constituent simplement des exemples illustratifs qui, manifestement, n'excluent pas d'autres mesures. L'article exige simplement qu'elles ne fassent pas appel à «l'emploi de la force armée». C'est une définition négative.*
> *(…) L'article prescrit uniquement les caractéristiques que ces mesures ne peuvent pas revêtir. Il ne dit ni ne suggère ce qu'elles doivent être »*[303].

En se fondant sur ces dispositions, nous pouvons supposer que le Conseil de sécurité a le droit de recourir aux mesures d'une interruption totale ou partielle des cyber-communications de l'État responsable de la menace pour la paix, de la rupture de la paix ou de l'acte d'agression[304]. À cet effet, nous pouvons supposer que le Conseil va coopérer avec des acteurs locaux, par exemple, avec les fournisseurs de services Internet qui pourraient mettre sur liste noire des noms de domaine via lesquels une cyberattaque a été lancée ou faire le filtrage du routage des paquets. Mais les États eux-mêmes pourraient aussi adopter une législation ou une réglementation nationale obligeant les fournisseurs de services Internet soumis à leur juridiction à prendre ces mesures nécessaires[305].

---

[303] TPIY, *Le Procureur c. Duško Tadić*, Chambre d'Appel, Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, le 2 octobre 1995, par. 35.

[304] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 76, par. 4., p. 358 ; Voir aussi ICIW, Proceedings of the 6th International Conference on Information Warfare and Security, George Washington University, Washington, DC, USA, 2011, p. 202.

[305] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 76, par.5.

L'élargissement du régime de sanctions à l'utilisation de l'Internet a été déjà discuté au sein du Conseil de sécurité en 2006 dans le cadre des mesures qui pourraient affronter Al-Qaida et les États ont proposé, entre outre, le filtrage ou la fermeture des sites utilise par les membres de l'organisation terroriste[306] ce qui confirme que l'idée d'imposition des sanctions à l'utilisation d'Internet n'est pas nouvelle et correspond au nouveau contexte de sécurité dans le monde. De plus, nous pouvons évoquer le rapport du groupe d'experts qui a été institué en vertu de la résolution 1874 (2009) pour fournir au Conseil des conclusions et recommandations sur les sanctions. La résolution 1874 a été adoptée par le Conseil de sécurité afin d'imposer des sanctions économiques et commerciales à la Corée du Nord après la crise liée au programme d'armes nucléaires. En 2019 le groupe d'experts a découvert que l'État nord-coréen a lancé de nombreuses cyberattaques « *to engage in the theft of military technology in violation of an arms embargo; revenue operations; cyberblackmail and extortion campaigns; hacking for pay; and the movement of money* »[307]. Et même si ces cyberattaques n'ont pas présenté une attaque armée en soi, les experts ont recommandé que le Conseil de sécurité prenne en considération la gravité des cyberattaques lors du choix des sanctions futures contre la République populaire démocratique de Corée[308] ce qui également montre l'intention du CS de faire face aux cybermenaces.

En ce qui concerne l'entrée en vigueur de l'article 42 de la Charte de l'ONU, elle autorise à utiliser la force armée contre l'État qui a violé les normes du droit international seulement si les mesures prévues par l'article 41 « *seraient inadéquates ou qu'elles se sont révélées telles* ». L'interprétation évolutive de cet article étend son champ d'application également en matière d'utilisation des cyberattaques, d'après certains experts[309]. Ainsi, parallèlement à l'utilisation des

[306] Conseil de sécurité, Quatrième rapport de l'Équipe d'appui analytique et de surveillance des sanctions créée en application des résolutions 1526 (2004) et 1617 (2005) du Conseil de sécurité concernant l'organisation Al-Qaida et les Taliban et les personnes et entités qui leur sont associées, le 10 mars 2006, par. 124, URL : https://www.undocs.org/fr/S/2006/154 (visité le 27/06/2020).

[307] Security Council, Report of the Panel of Experts established pursuant to resolution 1874 (2009), le 30 août 2019, note de bas de page 27, URL : https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf (visité le 27/06/2020).

[308] *Ibid*, par. 72.

[309] «*Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate 301 it could authorize UN member states or UN peace forces to conduct cyber attacks amounting to a use of force in order to react against a threat to the peace*» : ROSCINI (Marco), *Cyber Operations and the Use of Force in International Law*, op. it., p. 114 ; «*[I]f the Security Council mandates a peace operation to maintain law and order, contributing States should use all means reasonably available to them to implement the mandate.41 Thus, the international force can deal with cyber threats that may destabilize the peace operation*» : KLEFFNER (Jann), HARRISON DINNISS (Heather), «Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations», Naval War College, *International Law Studies*, Vol. 89, 2013, p. 526, URL : https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1039&context=ils (visité le 27/06/2020).

« *forces aériennes, navales ou terrestres* » mentionnées, le Conseil de sécurité peut prendre des mesures coercitives/contraignantes par le biais de cybercapacités[310] :

> « *Obviously, if an Article 42 authorization justifies the use of armed force, it would justify any information operation intended to accomplish the same objective. The sole limitation would be that the operation would have to comply with international humanitarian law* ».

Finalement, il est indispensable de noter que les mesures mentionnées aux articles 41 et 42 de la Charte de l'ONU peuvent être prises par des organisations régionales, sous réserve qu'elles agissent dans le cadre d'un mandat ou d'une autorisation de la résolution du Conseil de sécurité même si elles sont en cours dans le cyberespace. En particulier, la règle du Manuel de Tallinn impose à ces organisations l'obligation de coordonner ses actions avec le Conseil de sécurité de l'ONU :

> **RÈGLE 77 — Organisations régionales**
>
> Les organisations internationales, les institutions ou les agences à caractère régional peuvent mener des actions coercitives, liées aux opérations cybernétiques ou en réponse à ces opérations, conformément à un mandat du Conseil de sécurité des Nations Unies ou à une autorisation de celui-ci.

Cette disposition revêt une importance primordiale puisque tous les États-membres des Nations Unies sont tenus de mettre en œuvre les décisions du Conseil de sécurité et dans le cas de sanctions impliquant des cybercommunications, la coopérations des organisations régionales avec les CSNU et la mise en œuvre des instructions du Conseil au niveau national serait indispensable. Par exemple, il peut être nécessaire d'imposer aux fournisseurs de services Internet (qu'ils soient gouvernementaux ou privés) d'adopter des mesures restrictives. En conséquence, les États pourraient être obligés d'adopter des lois ou des réglementations nationales en vertu desquelles les fournisseurs de services Internet devraient respecter les dispositions concernées.

Mais comme la majorité des États-membres du Conseil de sécurité notent que parfois la cyber-stabilité n'est pas menacée par l'absence de normes ou l'absence de cadre juridique, mais par le fait que certains États ne respectent pas les engagements qu'ils ont pris, il serait nécessaire d'examiner les moyens de la responsabilisation des auteurs des cyberattaques.

---

[310] SCHMITT (Michael), «*Computer Network Attack: The Normative Software*», p. 70, in FISCHER (Horst), Yearbook of International Humanitarian Law, Cambridge University Press, Vol. 4, 2001 ; Voir aussi SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 76 par. 8., p. 359 ; Voir aussi «*Article 42 allows military response using land, air, or sea forces. Thus, the door is open for a potential military response to another country's aggression via cyber attack*» : JONES (Jeffrey), *Studies Combined: Cyber Warfare In Cyberspace - National Defense, Workforce And Legal Issues*, U.S. Department Of Defense, 2018, p.100.

Chapitre 4 — L'engagement de la responsabilité des cyberattaques qui violent le DIH

Traduire en justice les responsables des attaques lancées lors des conflits armés internationaux est un important pas vers le respect de la garantie de la justice. L'Assemblée générale de l'ONU reconnaît également la pertinence de ce pas et prévoit dans les Principes fondamentaux et directives concernant le droit à un recours et à réparation des victimes de violations flagrantes du droit international des droits de l'Homme et de violations graves du droit international humanitaire que « *l'obligation de respecter, de faire respecter et d'appliquer le droit international des droits de l'Homme et le droit international humanitaire* » est inséparable de l'obligation « *d'enquêter de manière efficace, rapide, exhaustive et impartiale sur les violations et de prendre, le cas échéant, des mesures contre leur auteur présumé, conformément au droit national et international* »[311].

Il apparaît donc nécessaire de se pencher sur la définition de la responsabilité des cyberattaques prévue par le droit international (Section 1) et déterminer les difficultés qui empêcheraient de traduire les auteurs de crimes en justice en raison de la nature spécifique des cyberopérations (Section 2).

Section 1 – La spécificité de la responsabilisation des auteurs des cyberattaques

Le droit international prévoit deux régimes distincts de la responsabilité garantis par les instances judiciaires pour des actes internationalement illicites. Le premier se rapporte à la responsabilité d'État et se traduit par le fait que les États sont responsables du comportement des personnes ou des groupes de personnes qui agissent en leur nom ou avec leur autorisation, tandis que le seconde est lié à la responsabilité pénale individuelle des personnes soupçonnées de crimes internationaux. Il apparaît donc nécessaire d'examiner l'application du principe de la responsabilité à la fois étatique et individuelle dans le cybercontexte.

Dans les conflits armés internationaux, la responsabilité de l'État pour les violations commises s'étend à « *tous actes commis par les personnes faisant partie de sa force armée* » et il « *ne pourra*

[311] Principes fondamentaux et directives concernant le droit à un recours et à réparation des victimes de violations flagrantes du droit international des droits de l'homme et de violations graves du droit international humanitaire, 60/147 Résolution adoptée par l'Assemblée générale le 16 décembre 2005, par. II, b), URL : https://www.ohchr.org/fr/professionalinterest/pages/remedyandreparation.aspx (visité le 18/06/2020).

s'exonérer il-même, ni exonérer une autre Partie contractante, des responsabilités »[312]. Au sens des normes du droit international humanitaire, les opérations militaires menées au nom d'un État peuvent être directement attribuées à cet État. Les experts de Tallinn déclarent par analogie que les cyberopérations qui ont été lancées par l'un des États-parties au conflit, s'il y a des preuves irréfutables, engagent la responsabilité de cet État. De plus, l'État demeure responsable des violations du DIH même si les auteurs ont été punis, parce qu'il reste, par exemple, tenu de payer une indemnité[313].

Le droit international prévoit que l'État non belligérant peut également être tenu responsable par son assistance ou ses encouragements de violations du DIH commises par État-partie au conflit dans les trois cas[314] :

1) L'État qui assiste un autre État a eu des connaissances que le comportement de l'État assisté était illicite ;

2) L'aide ou l'assistance de l'État sont prêtées dans l'intention de faciliter la commission du fait illicite par l'État assisté, et qu'elles l'ont effectivement facilitées ;

3) Le fait perpétré doit être tel qu'il aurait été internationalement illicite s'il avait été commis par l'État qui assiste lui-même.

Il faut noter que l'aide ou l'assistance de l'État ne sont pas nécessairement essentielles à la commission du fait internationalement illicite – il suffit qu'elles y contribuent de façon significative[315].

Bien que les cyberopérations enregistrées à ce jour en Estonie, en Géorgie ou en Iran ne semblent pas avoir eu de graves conséquences[316], elles démontrent, néanmoins, qu'il est techniquement possible d'intervenir dans les systèmes de contrôle du trafic aérien, terrestre ou maritime, des barrages ou des centrales nucléaires depuis le cyberespace. Par conséquent, il est impossible d'exclure les

---

[312] Règlement de La Haye, article 3 ; PA I, article 91 ; Convention de Genève (I), article 51 ; Convention de Genève (II), article 52 ; Convention de Genève (III), article 131 ; Convention de Genève (IV), article 148.

[313] Commentary of 1958, Convention (IV) de Genève relative à la protection des personnes civiles en temps de guerre, 12 août 1949, Responsabilité des parties contractantes, commentaire à l'article 148, URL : https://ihl-databases.icrc.org/applic/ihl/dih.nsf/Comment.xsp?action=openDocument&documentId=D99F33F4E37172F2C12563BD002D3075 (visité le 24/06/2020).

[314] Nations Unies, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, op. cit., art. 16, commentaire, par. 3, p. 165.

[315] Nations Unies, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, op. cit., par. 5.

[316] SCHMITT (Michael), *Tallinn Manual on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2013, p.56, URL : http://csef.ru/media/articles/3990/3990.pdf (visité le 02/05/2020).

scénarios potentiellement catastrophiques, tels que les collisions entre aéronefs, le rejet de substances toxiques par les usines chimiques ou la perturbation des infrastructures et des services essentiels tels que les systèmes d'approvisionnement en eau, en électricité. Mais ce qui est plus important, ce que ce sont les civils qui risquent de devenir les principales victimes de ces opérations ce qui violerait les codes de guerre.

En conséquence, le Manuel de Tallinn reconnaît la responsabilité des États des cyberattaques et dispose :

> **RÈGLE 14 — Cyberactes internationalement illicites**
> Un État assume la responsabilité internationale d'un acte cybernétique qui lui est imputable et qui constitue une violation d'une obligation juridique internationale.

La transposition du principe de responsabilité pour « *fait internationalement illicite* » dans le cyberespace s'explique par sa nature coutumière :

> « *Il est au demeurant bien établi que, dès lors qu'un État a commis un acte internationalement illicite, sa responsabilité internationale est susceptible d'être engagée, quelle que soit la nature de l'obligation méconnue* »[317].

La violation d'une obligation juridique internationale prévue par le traité ou par le droit international coutumier peut consister en une action ou en une omission[318]. Dans le cyberespace, une action internationalement illicite peut consister notamment en une violation de la Charte des Nations Unies[319] (par exemple, un recours à la force par des cyberarmes) ou en violation des obligations du droit des conflits armés (par exemple, une cyberattaque contre des civils).

En plus d'être internationalement illicite, un fait doit être imputable à un État pour entraîner une responsabilité. Tous les actes ou omissions d'organes d'un État sont automatiquement et nécessairement imputables à cet État[320]. La notion d'« *organes d'un État* » comprend « *toute*

---

[317] CIJ, *Affaire relative au projet Gabcikovo-Nagymaros (Hongrie/Slovaquie)*, Arrêt, le 25 septembre 1997, par. 47 ; Voir aussi « *S'agissant d'un acte imputable à l'État et décrit comme contraire aux droits conventionnels d'un autre État, la responsabilité internationale s'établirait directement dans le plan des relations entre ces États* » : CPJI, *Italie c. France*, Affaire des Phosphates du Maroc (exceptions préliminaires), Arrêt, le 14 juin 1938, p. 28.

[318] HENCKAERTS (Jean-Marie), DOSWALD-BECK (Louise), *Droit international humanitaire coutumier, Volume I : règles*, op. cit., Règle 149, p. 698 ; Voir aussi Nations Unies, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, op. cit., article 2, commentaire, p. 72, par. 4.

[319] Charte des Nations Unies, 1945, article 2 dispose 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* ».

[320] Nations Unies, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, op. cit., article 4, par. 1, p. 88.

personne ou entité qui a ce statut d'après le droit interne de l'État »[321], indépendamment de sa fonction ou de sa place dans la hiérarchie gouvernementale. Toute cyberactivité exercée par les services de renseignement, l'armée, la sécurité intérieure, les douanes ou d'autres organismes d'État engageront la responsabilité des États en vertu du droit international s'il enfreint une obligation juridique internationale applicable à cet État.

Les experts qui ont élaboré les normes de Manuel de Tallinn supposent que le comportement d'acteurs non-étatiques peut également être attribué à un État et, par conséquent, donner lieu à la responsabilité juridique internationale de cet État[322]. Leur réflexion s'appuie sur l'article 8 de Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite qui prévoit la responsabilité d'État si une personne ou un groupe de personnes agit en fait sur les instructions ou les directives ou sous le contrôle de cet État[323]. Dans le cybercontexte ce seraient les États qui ont conclu des contrats avec des entreprises privées ou simplement ont donné des instructions, des ordres ou exercé un contrôle sur ces entreprises[324] pour mener des cyberopérations et qui seraient responsable de ses actions.

Toutefois, le lieu où des activités illicites se déroulent ou les acteurs se localisent n'affecte pas la détermination de la responsabilité éventuelle de l'État. Par exemple, dans le conflit international où le groupe de personne, situé dans l'État A, lance une série de cyberattaques contre les civils de l'État B à l'aide des ordinateurs situés dans l'État C en suivant les instructions de l'État D c'est le comportement de l'État D qui tombe sous le coup de sanctions fixées par le droit international, en premier lieu, et puis le comportement de l'État C en vertu de la due diligence.

Un autre aspect de la responsabilité étatique qu'il est nécessaire d'examiner est lié aux cyberattaques qui ont été lancées à partir d'une infrastructure gouvernementale. Le Manuel de Tallinn exprime clairement sa position :

> « *Le simple fait qu'une cyberopération a été lancée ou provient d'une autre infrastructure gouvernementale ne constitue pas une preuve suffisante pour imputer l'opération à cet État, mais une indication que l'État en question est associé à l'opération* »[325].

[321] Nations Unies, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, op. cit., article 4, par. 2.

[322] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 17, pp. 94-95.

[323] Nations Unies, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, op. cit., article 8, p. 72.

[324] Éléments publics de doctrine militaire de lutte informatique offensive, op. cit., p. 8.

[325] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 15, par. 13, p. 91.

En d'autres termes, le lien entre la cyberattaque et l'utilisation d'une infrastructure gouvernementale pour la lancer ne donne pas de base légale pour engager des poursuites contre l'État ou pour le tenir responsable des actes en question. Cette réflexion diffère complètement d'une approche traditionnelle d'après laquelle l'utilisation de l'équipement militaire aurait normalement été attribuée à l'État en raison de l'improbabilité de leur utilisation par des personnes autres que des organes de l'État ou des individus autorisés d'effectuer ses fonctions gouvernementales. Telle différence entre l'approche appliquée dans le cybercontexte et celle traditionnelle s'explique par le fait qu'il est fort possible que la cyberinfrastructure gouvernementale puisse être capturée par des acteurs non-étatiques qui l'utiliseront dans l'avenir pour mener des cyberopérations.

En définitive, la jurisprudence internationale prévoit que l'État qui a violé les dispositions du droit international pendant un conflit armé doit être traduit en justice pour qu'il réponde de ses crimes et pour prévenir des violations éventuelles. Pour ce faire l'ONU a établi en juin 1945 un organe judiciaire, à savoir la CIJ. Le cadre des actions de la CIJ est régi par son Statut et par la Charte des Nations Unies et prévoit sa compétence pour régler tout différend que les États lui soumettent, relatif à la nature et l'étendue des réparations dues en raison de la violation de leurs engagements internationaux[326]. Depuis sa création, la CIJ a examiné les situations liées au respect des principes de non-intervention, de non-recours à la force et de souveraineté des États. Dans l'affaire *Nicaragua contre États-Unis d'Amérique* du 27 juin 1986 notamment, le Nicaragua a saisi la juridiction de La Haye en raison de l'ingérence militaire des États-Unis et le soutien de Washington à des groupes armés agissant sur le territoire du Nicaragua. La Cour a rendu une décision dans laquelle elle a reconnu les États-Unis coupables et leur a ordonné de « *mettre immédiatement fin et de renoncer à tout acte constituant une violation de leurs obligations juridiques, et qu'ils devaient réparer tout préjudice* »[327]. Le groupe international des experts de Tallinn a reconnu que ces dispositions peuvent être appliquées dans le cybercontexte et a décidé que « *si l'État A fourni des outils de piratage qui seraient ensuite utilisés par un groupe d'insurgés de sa propre initiative contre l'État B (le groupe n'agit pas sous le contrôle de l'État A), la simple fourniture de ces outils est insuffisante pour*

[326] Statut de la CIJ, article 36.

[327] CIJ, *Nicaragua c. États-Unis*, Arrêt, Vue d'ensemble de l'affaire, le 27 juin 1986, URL : https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-FR.pdf (visité le 20/07/2020).

attribuer les attaques du groupe à l'État A. Néanmoins, cette assistance peut elle-même constituer une violation du droit international »[328].

Une autre ligne de conduite de la Cour pour mettre en place le respect des normes du droit international est de déterminer les responsabilités et les sanctions pour un génocide. Sous le terme « génocide » nous entendons la commission d'un acte « *avec l'intention de détruire, ou tout ou en partie, un groupe national, ethnique, racial ou religieux* » qui peut prendre la forme de meurtre de membres du groupe, d'atteinte grave à l'intégrité physique ou mentale de membres du groupe, de soumission intentionnelle du groupe à des conditions d'existence devant entraîner sa destruction physique totale ou partielle, de mesures visant à entraver les naissances au sein du groupe ou de transfert forcé d'enfants du groupe à un autre groupe[329]. En vertu de cette définition, l'effacement de données des personnes civiles (par exemple, les données sur la santé) appartenant à certains groupes ethniques dans l'intention de porter atteinte à leur intégrité physique peut être considéré comme génocide par analogie. La Cour prévoit la prise de sanctions pénales à l'égard des personnes qui ont commis de tels actes et la responsabilité des États de procéder « *à l'arrestation des personnes accusées de génocide se trouvant sur leur territoire − même si le crime dont elles sont accusées a été commis hors de celui-ci − et que, à défaut de les traduire devant leurs propres juridictions, ils les défèrent devant la cour internationale compétente pour les juger* »[330]. Cette clarification est particulièrement importante parce que l'activité de la Cour est basée sur le consentement des États, c'est-à-dire que la Cour sera compétente seulement si les parties ont accepté qu'elle règlera leur différend[331].

C'était le cas de la guerre de Bosnie-Herzégovine, conflit armé international, qui a débuté le 6 avril 1992 entre les Serbes et les Croates, d'une part, et les Bosniaques, d'autre part, suite à la proclamation d'indépendance de la Bosnie-Herzégovine. Les décisions du Conseil de sécurité concernant le règlement pacifique du conflit prises par le Conseil précédemment[332] avaient échoué

[328] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 17, par. 19, p. 100.

[329] Convention pour la prévention et la répression du crime de génocide, le 9 décembre 1948, article 2.

[330] CIJ, *Bosnie-Herzégovine c. Serbie-et-Monténégro*, Application de la convention pour la prévention et la répression du crime de génocide, le 26 février 2007, paras. 426 et 443, URL : https://jusmundi.com/en/document/decision/fr-application-de-la-convention-pour-la-prevention-et-la-repression-du-crime-de-genocide-bosnie-herzegovine-c-serbie-et-montenegro-arret-monday-26th-february-2007 (visité le 10/07/2020).

[331] Département fédéral des affaires étrangères DFAE, Direction du droit international public, « Guide pratique sur la reconnaissance de la compétence de la Cour internationale de Justice », Berne, 2014, p.6, URL : https://www.eda.admin.ch/dam/eda/fr/documents/publications/Voelkerrecht/handbook-jurisdiction-international-court_fr (visité le 11/07/2020).

[332] Le Conseil de Sécurité a mis en œuvre un « *embargo général et complet sur toutes les livraisons d'armements et d'équipements militaires à la Yougoslavie* » par sa Résolution 713 (1993) du 25 septembre 1991 et a créé une force de protection des Nations unies (ci-après FORPRONU) en Yougoslavie Résolution 743 (1992) du 21 février 1992.

ainsi que la création d'une « *zone protégée* » à Srebrenica en 1993. Cette guerre est à l'origine d'environ cent mille morts, dont la moitié sont des civiles[333]. Le procès initié par la Bosnie-Herzégovine le 20 mars 1993 devant la Cour a dû établir la responsabilité de ces actes au titre de l'application de la Convention pour la prévention et la répression du crime de génocide. La décision de la CIJ a reconnu le génocide à Srebrenica en 1995 réalisé par des « *membres de l'état-major de la VRS (l'armée de la Republika Srpska)* »[334].

Dans le cybercontexte nous faisons face à un autre genre de problème. Bien que nous puissions supposer que les normes susmentionnées peuvent être appliquées aux cyberattaques pour traduire en justice les États en question, la question plus globale est de savoir quelle est la cour qui sera compétente ? À ce jour, aucune cour, y compris la CIJ, n'a poursuivi un État pour les crimes commis dans le cyberespace pendant le conflit armé international ce qui est le reflet d'une compréhension commune des problèmes juridiques :

> « *It is a feature of the human predicament, not only of the legislator but of anyone who attempts to regulate some sphere of conduct by means of general rules, that he labours under one supreme handicap – the impossibility of foreseeing all possible combinations of circumstances that the future may bring* »[335].

Considérons maintenant le cas de la responsabilité individuelle. Les violations graves du droit international commises pendant la Seconde Guerre mondiale et leurs conséquences ont eu un impact important sur le développement de protection à l'encontre des victimes de conflits armés internationaux. En particulier, les tribunaux militaires internationaux de Nuremberg et de Tokyo qui ont pour but de traduire en justice les responsables des violations ont instauré que le principe de la responsabilité pénale individuelle pour les crimes de guerre est une règle de droit international

[333] IDC, Victim statistics in Novi Travnik, Vitez, Kiseljak and Busovača, archive, URL : https://web.archive.org/web/20071023095215/http://www.idc.org.ba/aboutus/Overview_of_jobs_according_to_%20centers.htm (visité le 10/07/2020).

[334] CIJ, *Bosnie-Herzégovine c. Serbie-et-Monténégro*, Application de la convention pour la prévention et la répression du crime de génocide, le 26 février 2007, par. 413, URL : https://jusmundi.com/en/document/decision/fr-application-de-la-convention-pour-la-prevention-et-la-repression-du-crime-de-genocide-bosnie-herzegovine-c-serbie-et-montenegro-arret-monday-26th-february-2007 (visité le 10/07/2020).

[335] WALDRON (Jeremy), «Vagueness in Law and Language: Some Philosophical Issues», *California Law Review*, Vol. 82, No. 3, mai 1994, p. 537, URL : https://www.jstor.org/stable/3480971?seq=1 (visité le 14/07/2020).

coutumier[336]. Reconnu par les statuts des autres tribunaux (TPIY[337], TPIR[338], TSSR[339]) et par les documents juridiques, comme les traités de DIH[340] ou par le Statut de Rome servant de base pour la CPI[341], le principe de responsabilité individuelle permet d'affirmer qu'elle est applicable aujourd'hui et de supposer qu'il serait appliqué pour réglementer des cyberattaques.

L'engagement de ce régime est intrinsèquement lié, en premier lieu, aux notions des crimes graves. En premier lieu, nous parlons de crimes de guerre, comme nous avons affaire aux conflits armés. Le crime de guerre comprend « *les violations des lois et coutumes de la guerre* », y compris « *l'assassinat, les mauvais traitements ou la déportation, pour des travaux forcés ou pour tout autre but, des populations civiles dans les territoires occupés, l'assassinat ou les mauvais traitements des prisonniers de guerre ou des personnes en mer, l'exécution des otages, le pillage des biens publics ou privés, la destruction sans motif des villes et des villages ou la dévastation que ne justifie pas la nécessité militaire* »[342]. Ces crimes figurent dans les Conventions de Genève de 1949[343], dans le Protocole additionnel I[344], ainsi que dans le Statut de Rome[345] et dans les règles du droit coutumier[346].

---

[336] Assemblée générale des Nations Unies, Commission du droit international, Le statut et le jugement du Tribunal de Nuremberg, Historique et analyse (Mémorandum du Secrétaire général), Lake Success, New-York, 1949, p. 66, URL : https://digitallibrary.un.org/record/160809/files/A_CN.4_5-FR.pdf (visité le 30/06/2020) ; Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, and Charter of the International Military Tribunal, August 8, 1945, article 6, p. 286, URL : https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.2_Charter%20of%20IMT%201945.pdf (visité le 30/06/2020) ; International military tribunal for the Far East, Special proclamation by the Supreme Commander tor the Allied Powers at Tokyo January 19, 1946, article 5, p. 22, URL : https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.3_1946%20Tokyo%20Charter.pdf (visité le 30/06/2020).

[337] Statut actualisé du tribunal pénal international pour l'ex-Yougoslavie, articles 2, 3, p. 5, URL : http://www.icty.org/x/file/Legal%20Library/Statute/statute_sept09_fr.pdf (visité le 02/07/2020).

[338] Statut du Tribunal pénal international pour le Rwanda, article 5, article 6, p. 63, URL : http://unictr.irmct.org/sites/unictr.org/files/legal-library/100131_Statute_en_fr.pdf (visité le 02/07/2020).

[339] Accord entre l'Organisation des Nations Unies et le Gouvernement sierra-léonais et Statut du Tribunal spécial pour la Sierra Leone, le 16 janvier 2002, article 2, URL : https://ihl-databases.icrc.org/applic/ihl/dih.nsf/INTRO/605?OpenDocument (visité le 30/06/2020).

[340] Convention de Genève (I), article 49 ; Convention de Genève (II), article 50 ; Convention de Genève (III), article 129 ; Convention de Genève (IV), article 146 ; PA I, article 85. Bien que la Convention sur les mines antipersonnel (article 9) et la Convention sur les armes à sous-munitions (article 9) ne créent pas par elles-mêmes une responsabilité inter nationale individuelle pour crimes de guerre, mais obligent les États à prendre des mesures pour réprimer les violations de ces conventions.

[341] Statut de Rome, article 5, article 8, article 25.

[342] Assemblée générale des Nations Unies, Commission du droit international, Le statut et le jugement du Tribunal de Nuremberg, Historique et analyse (Mémorandum du Secrétaire général), op. cit., article 6, par. b), pp. 100-101

[343] Convention de Genève (I), article 50 ; Convention de Genève (II), article 51 ; Convention de Genève (III), article 130 ; Convention de Genève (IV), article 147.

[344] PA (I), article 85.

[345] Statut de Rome, article 8, par. 2 a) et b).

[346] HENCKAERTS (Jean-Marie), DOSWALD-BECK (Louise), *Droit international humanitaire coutumier, Volume I : règles*, op. cit., Règle 156, p. 751.

La responsabilité pénale individuelle est prévue également pour les autres crimes internationaux, à savoir pour le crime contre l'humanité, et le crime du génocide. Les crimes contre l'humanité comprennent 11 actes commis « *dans le cadre d'une attaque généralisée ou systématique dirigée contre toute population civile et en connaissance de l'attaque* »[347]. Il s'agit des actes suivants : l'extermination ; la réduction en esclavage ; la déportation ou le transfert forcé de population ; l'emprisonnement ou autre forme de privation grave de liberté physique en violation des dispositions fondamentales du droit international ; la torture ; le viol, l'esclavage sexuel, la prostitution forcée, la grossesse forcée, la stérilisation forcée ou toute autre forme de violence sexuelle de gravité comparable ; la persécution de tout groupe ou de toute collectivité identifiable pour des motifs d'ordre politique, racial, national, ethnique, culturel, religieux ou sexiste, ou en fonction d'autres critères universellement reconnus comme inadmissibles en droit international, en corrélation avec tout acte visé dans le présent paragraphe ou tout crime relevant de la compétence de la Cour ; la disparition forcée de personnes ; le crime d'apartheid ; d'autres actes inhumains de caractère analogue causant intentionnellement de grandes souffrances ou des atteintes graves à l'intégrité physique ou à la santé physique ou mentale.

En ce qui concerne la notion de crime de génocide, elle a été consacrée en 1948 dans Convention pour la prévention et la répression du crime de génocide qui lui a défini comme un meurtre de membres du groupe, ou une atteinte grave à l'intégrité physique ou mentale de membres du groupe, ou une soumission intentionnelle du groupe à des conditions d'existence devant entraîner sa destruction physique totale ou partielle ou des mesures visant à entraver les naissances au sein du groupe, ou un transfert forcé d'enfants du groupe à un autre groupe « *commis dans l'intention de détruire, ou tout ou en partie, un groupe national, ethnique, racial ou religieux, comme tel* »[348].

Finalement, le crime d'agression, ou crime contre la paix, elle a été élaborée par le Tribunal de Nuremberg et a été définie comme « la direction, la préparation, le déclenchement ou la poursuite d'une guerre d'agression, ou d'une guerre de violation des traités, assurances ou accords internationaux, ou la participation à un plan concerté ou à un complot pour l'accomplissement dé l'un quelconque des actes qui précèdent »[349]. Il est particulièrement significatif que depuis 2017 la CPI soit compétente pour les crimes d'agression.

[347] Statut de Rome, article 7.
[348] Convention pour la prévention et la répression du crime de génocide, art. 2.
[349] Assemblée générale des Nations Unies, Commission du droit international, Le statut et le jugement du Tribunal de Nuremberg, Historique et analyse (Mémorandum du Secrétaire général), Lake Success, New-York, 1949, article 6, par. a), p. 100, URL : https://digitallibrary.un.org/record/160809/files/A_CN.4_5-FR.pdf (visité le 30/03/2019).

La question majeure est de savoir si nous pouvons assimiler les conséquences des cyberattaques aux celles des crimes de guerre, crimes contre l'humanité, crimes d'agression ou du génocide pour comprendre si les responsables doivent être traduits en justice devant la CPI. À cet égard, Anne-Laure Chaumette propose d'examiner *ratione materiae* de la Cour en fonction d'une approche choisie : « *means approach* » ou « *effect approach* ». La première approche est plus stricte, d'après laquelle le conflit armé existe s'il est mené au moyen de techniques de guerre cinétique conventionnelles[350], et, par conséquent, la CPI n'est pas compétente en matière de cyber. En faveur de cette conclusion nous pouvons également citer les dispositions du Statut de Rome qui soulignent que « *[l]a personne n'est responsable pénalement en vertu du présent Statut que si son comportement constitue, au moment où il se produit, un crime relevant de la compétence de la Cour* »[351], et « *[l]a définition d'un crime est d'interprétation stricte et ne peut être étendue par analogie* »[352]. En raison de cette rigidité, les cyberattaques qui n'étaient pas explicitement mentionnées dans les articles 6, 7, 8, 8 *bis* seraient peu susceptibles d'être qualifiées les crimes relevant de la compétence de la Cour pénale internationale[353].

Mais d'après d'autre approche — « *effect approach* » — que nous utilisons dans notre étude, les cyberattaques qui produisent les mêmes effets que ceux des attaques cinétiques peuvent être assimilées à des crimes graves énumérés dans le Statut de Rome. Dans ce cas, la cyberattaque pourrait constituer un crime de guerre, crime contre l'humanité ou crime de génocide soit si elle représente les actes susmentionnés commis par des cybermoyens soit, pour les experts du Manuel de Tallinn, les actes spécifiques, par exemple, l'intrusion dans le réseau pour obtenir les noms d'individus enregistrés comme les représentants d'une certaine race pour exercer le génocide[354] ou l'utilisation d'archives historiques numérisées concernant une population pour déterminer l'origine ethnique d'individus en vue de faciliter le génocide, les crimes contre l'humanité ou les crimes de guerre[355]. En ce qui concerne le crime d'agression, nous avons déjà vu dans le Chapitre 1 que les cyberattaques sont susceptibles de déclencher conflit et, à cet égard, nous pouvons supposer qu'elles peuvent constituer un crime contre la paix. Cela signifie que les personnes qui utilisent les cybermoyens lors

[350] CHAUMETTE (Anne-Laure), «International Criminal Responsibility of Individuals in Case of Cyberattacks», *International Criminal Law Review,* Brill Academic Publishers, 2018, p.11, URL : https://brill.com/view/journals/icla/18/1/article-p1_1.xml (visité le 20/07/2020).

[351] Statut de Rome, art. 22, par. 1.

[352] *Ibid*, par. 2.

[353] BROWN (Davis), « A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict», *Harvard International Law Journal*, Vol. 47, No. 1, 2006, p. 212, URL : https://heinonline.org/HOL/LandingPage?handle=hein.journals/hilj47&div=8&id=&page= (visité le 21/07/2020).

[354] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 10, par. 18, p. 66.

[355] *Ibid*, Règle 142, par. 7, p. 536.

d'un conflit armé international doivent également assumer la responsabilité pénale individuelle[356]. Le 22 mai 2020, pendant une réunion virtuelle organisée par le Conseil de sécurité des Nations Unies, la Belgique et le Liechtenstein se sont tenus se tient très fermement à cette position et le dernier a proposé une initiative visant à créer un *Council of advisers* afin d'explorer le rôle que la Cour pénale internationale pourrait jouer dans ce nouveau cadre réglementaire[357] ce qui réaffirme la volonté de la communauté internationale de réglementer le comportement des États dans le cyberespace.

Un examen plus détaillé des normes du droit international nous montre qu'une personne physique est pénalement responsable dans les cas ou elle commet les crimes décrits ci-dessus, planifie, ordonne, sollicite ou encourage la commission d'un tel crime, apporte son aide pour faciliter l'activité criminelle[358]. Par exemple, la personne qui fournit des logiciels malveillants ou des informations sur les vulnérabilités qui sont nécessaires pour faciliter de commettre un crime de guerre serait tenue pour responsable de ce crime. De la même manière, celui qui a incité à poursuivre, par exemple, le massacre de civils d'un groupe religieux particulier pendant un conflit armé international par les exhortations postées en ligne est passible de poursuites pénales si ces exhortations étaient susceptibles d'être efficaces.

De plus, le fait que le subordonné a obéi à un ordre supérieur de mener ces actes ou des cyberopérations qui constitueraient un crime de guerre ne le dégage pas de la responsabilité pénale si le subordonné savait que l'acte ordonné était illégal ou s'il aurait dû le savoir en raison de son caractère manifestement illégal[359].

Le combattant dont les actions dans le cybercontexte constituent les crimes de guerre, d'agression, de génocide ou crime contre l'humanité ne peut pas se référer au privilège du combattant prévu pour des actes de guerre licites. De la même manière, aucun privilège ne peut s'attacher au « *chef d'État ou de gouvernement, d'un membre d'un gouvernement ou d'un parlement, d'un représentant élu ou d'un agent d'un État* » pour s'exonérer de la responsabilité pénale[360]. Toutefois, les situations dans lesquelles un subordonné a exécuté les ordres d'un supérieur sous peine de mort

[356] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 84, p. 391.

[357] Ministry of Foreign Affairs of Estonia, Signature Event of Estonia's UNSC Presidency: Cyber Stability, Conflict Prevention and Capacity Building, op. cit.

[358] Statut de Rome, article 25 ; Statut du TPIY, article 7 ; Statut du TPIR, article 6 ; Statut du TSSL, article 6.

[359] HENCKAERTS (Jean-Marie), DOSWALD-BECK (Louise), *Droit international humanitaire coutumier, Volume I : règles*, op. cit., Règle 154, 155, pp. 744-746 ; Voir aussi Statut de Rome, article 33.

[360] Statut de Rome, article 27.

ou d'atteinte grave à l'intégrité physique du subordonné, ou même en état d'intoxication involontaire ou en état de légitime défense constituent les motifs d'exonération de la responsabilité pénale[361].

Néanmoins, le champ d'application de la responsabilité pénale individuelle ne se limite pas aux actions violées le droit international. Ce régime de responsabilité prévoit également les sanctions pour « *l'omission coupable d'un acte requis en vertu d'une règle de droit pénal* »[362] qui a provoqué les crimes[363]. En particulier, le droit humanitaire prévoit le devoir des supérieurs et des commandants « *d'empêcher que soient commises des infractions (…) et, au besoin, de les réprimer et de les dénoncer aux autorités compétentes* »[364]. Cette règle étend son champ d'application au cybercontexte [365]:

> **RÈGLE 85 — Responsabilité pénale des commandants et des supérieurs**
>
> a) Les commandants et autres supérieurs hiérarchiques sont pénalement responsables d'avoir ordonné des cyberopérations constituant des crimes de guerre.
> b) Les commandants sont également pénalement responsables s'ils savaient ou, vu les circonstances de l'époque, auraient dû savoir que leurs subordonnés étaient en train de commettre, étaient sur le point de commettre ou avaient commis des crimes de guerre et n'avaient pas pris toutes les mesures raisonnables et disponibles pour empêcher leur commission ou de punir les responsables.

Un bon exemple de l'application de cette règle est l'ordonnance d'un supérieur ou d'un commandant, ne participant pas directement aux hostilités, de lancer des cyberattaques contre des civils. Cet ordre de lancer des cyberattaques sans distinction engagerait la responsabilité pénale de la personne qui l'ordonnait, peu importe que cette personne ait ou non pris une part personnelle dans le déroulement réel de la cyberopération.

---

[361] Statut de Rome, article 31, par. c) et d).

[362] TPIY, *Le Procureur c. Radislav Krstić*, Chambre de Première instance, Jugement, le 2 août 2001, par. 601 ; Voir aussi TPIY, *Le Procureur c. Radovan Karadžić et Ratko Mladić*, Chambre de Première instance, Examen des actes d'accusation dans le cadre de l'article 61 du Règlement de procédure et de preuve, le 11 juillet 1996, par.82 ; TPIY, *Le Procureur c. Dragoljub Kunarac, Radomir Kovač et Zoran Vuković*, Chambre de Première instance, Jugement, le 22 février 2001, par. 395 ; TPIY, *Le Procureur c. Zejnil Delalić, Zdravko Mucić, Hazim Delić et Esad Landžo*, Chambre de Première instance, Jugement, le 16 novembre 1998, par. 346

[363] « *Les commandants et autres supérieurs hiérarchiques sont pénalement responsables des crimes de guerre commis par leurs subordonnés s'ils savaient, ou avaient des raisons de savoir, que ces subordonnés s'apprêtaient à commettre ou commettaient ces crimes et s'ils n'ont pas pris toutes les mesures nécessaires et raisonnables qui étaient en leur pouvoir pour en empêcher l'exécution ou, si ces crimes avaient déjà été commis, pour punir les responsables* » : HENCKAERTS (Jean-Marie), DOSWALD-BECK (Louise), *Droit international humanitaire coutumier, Volume I : règles*, op. cit., Règle 153, p. 737 ; Voir aussi PA (I), article 86, par. 1.

[364] *Ibid*, article 87, par.1.

[365] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 85, pp. 396-397.

Ainsi l'engagement de la responsabilité des supérieurs repose sur trois éléments cumulatifs élaborés par des tribunaux militaires internationaux[366] :

1) l'existence d'un lien de subordination entre le supérieur et l'auteur du crime, qui confère au supérieur un contrôle effectif sur la conduite des auteurs du crime ;

2) la connaissance par le supérieur du fait que son subordonné avait commis le crime ou s'apprêtait à le commettre ;

3) l'absence d'intervention du supérieur pour empêcher ou sanctionner le crime.

Bien que les caractéristiques techniques des cyberopérations compliquent les choses, ce fait n'exonère pas des commandants ou des supérieurs de la responsabilité d'exercer un contrôle sur leurs subordonnés parce qu'ils (commandants ou supérieurs) sont supposés avoir le même degré de compréhension de la situation que lors des conflits armés *classiques*[367].

Comme nous voyons, les doutes initiaux quant à l'application du principe de la responsabilité des États et des individus des actes internationalement illicites ont été dissipés. En témoignent, entre autres, les conclusions faites par le groupe d'experts gouvernementaux représentant 20 États de toutes les régions géographiques du monde qui a décidé à l'unanimité que la responsabilité pour le comportement illicite s'applique au cyberespace[368]. Mais comme nous pouvons voir, de nombreuses cyberattaques restent impunies sans la cour ou le tribunal pénal qui permettraient au principe de la responsabilité pénale individuelle être appliqué globalement[369]. À cet égard, le *Cybercrime Legal Working Group* qui travaille sous la supervision de l'EastWest Institute a proposé en 2012 de créer le Tribunal pénal international pour le cyberespace (International Criminal Tribunal for Cyberspace) sur la base d'une décision du Conseil de sécurité des Nations Unies conformément au Chapitre VII

[366] TPIY, *Le Procureur c. Dario Kordić et Mario Čerkez*, Chambre d'appel, Arrêt, le 17 décembre 2004, par.827 ; Voir aussi TPIY, *Le Procureur c. Sefer Halilović*, Chambre de première instance I, Jugement, le 16 novembre 2005, paras. 38-100, 747, 751-752 ; TPIY, *Le Procureur c. Tihomir Blaškić*, Chambre d'appel, Arrêt, le 29 juillet 2004, paras. 62, 91, 218, 417, 484, 632 ; TPIR, *Le Procureur c. Clement Kayishema et Obed Ruzindana*, Chambre de première instance II, Jugement, 21 mai 1999, paras. 209-210, 216-218, 222-225, 228-229, 231.

[367] Délégation à l'information et à la communication de la défense, Droit international appliqué aux opérations dans le cyberespace, op.cit.,p. 16.

[368] Assemblée générale, Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, op. cit., p.3.

[369] Nous pouvons citer à titre d'exemple la déclaration de la Fédération de Russie qui a signalé un manque de recours dans l'application des normes, comme l'absence d'une cyber cour de justice : UN Open-ended working group on developments in the field of information and telecommunications in the context of international security; Second substantive session; Agenda item «International law», URL : http://webtv.un.org/search/3rd-meeting-open-ended-working-group-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-second-substantive-session-10%E2%80%9314-february-2020/6131646836001/?term=2020-02-12&lan=english&sort=date (visité le 07/06/2020).

de la Charte des Nations Unies, soit créer une Cour pénale internationale spéciale pour le cyberespace en tant que subdivision de la CPI à La Haye qui sera régie par les dispositions du Statut de Rome[370]. Bien que cette idée puisse considérablement faciliter l'administration de la justice, elle a, néanmoins, un inconvénient majeur : le Statut de futur tribunal ne mentionne pas explicitement les crimes graves et se limite aux actes suivants[371] :

Article 2

Massive and coordinated global cyberattacks against communications and information infrastructures

Article 3

Violations of the Global Treaty on Cybercrime

a) illegal access

b) illegal interception

c) data interference

d) system interference

e) misuse of devices

f) forgery

g) fraud h) offences related to child pornography

Article 4

Spam and Identity Theft

Article 5

Preparatory acts of provisions in the Global Treaty on Cybercrime

[370] SCHJOLBERG (Stein), A paper for the EastWest Institute (EWI), Cybercrime Legal Working Group, Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes, An International Criminal Tribunal for Cyberspace (ICTC), Prosecution for the Tribunal, Police investigation for the Tribunal, mars 2012, pp. 15-17, URL : https://www.cybercrimelaw.net/documents/ICTC.pdf (visité le 26/07/2020).

[371] SCHJOLBERG (Stein), Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes, An International Criminal Tribunal for Cyberspace (ICTC), op. cit., pp. 26-28.

Cet état de choses risque de soulever plus de questions qu'il n'apporte de réponse. Cependant, l'absence de consensus sur les juridictions qui seront compétentes pour examiner les crimes commis pendant les conflits armés internationaux n'est pas le seul problème. La partie technique de l'attribution de responsabilité et rassemblement des preuves des auteurs présumés représente un autre défi pour la communauté internationale.

Section 2 — Les obstacles dans la répression internationale des violations du DIH dans le cybercontexte

En février de 2018, Paul Rascagneres, analyste spécialisé dans les logiciels malveillants de Cisco Talos, organisation de renseignements sur les cybermenaces, a déclaré : « *Alors que les acteurs progressent en compétences et en moyens, il est probable que nous observerons ces derniers adopter des ruses pour compliquer et brouiller l'attribution. L'attribution est déjà difficile. Il est peu probable qu'elle devienne plus simple* »[372].

En effet, l'établissement d'un lien entre la cyberopération et le conflit armé et, par conséquent, l'identification d'auteur d'une cyberopération afin de le poursuivre en justice, reste la priorité immédiate du droit international aujourd'hui. « *Du moment que le DIH se fonde sur l'attribution de responsabilité à des personnes et à des parties au conflit, cela pose d'importantes difficultés* »[373] pour les instances judiciaires parce que sans l'identification de l'auteur de l'attaque la pleine application du droit international humanitaire n'est pas possible.

Considérons tout d'abord les règles générales qui permettent d'identifier les responsables. Les conflits armés internationaux classiques prévoient le port d'uniforme militaire[374] ainsi que le port des armes ouvertement par le combattant[375]. Grâce à ces normes, nous pouvons non seulement faire une distinction entre les combattants et la population civile en vue de garantir la protection renforcée pour la dernière, mais également identifier les parties au conflit. Entre outres, cela permet de rattacher des combattants à un État déterminé et de les sanctionner en cas de violation de droit international. Toutefois, le caractère anonyme des cyberattaques pose un problème du rattachement d'une activité cybernétique à une partie au conflit. Mais comme nous avons déjà vu, l'anonymat est la règle plutôt

[372] RASCAGNERES (Paul), « Who Wasn't Responsible for Olympic Destroyer? », le 26 février 2018, URL : https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html (visité le 23/07/2020).

[373] CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », Rapport, XXXI[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge, op. cit., p.42.

[374] PA (I), article 44, par.7.

[375] *Ibid*, article 44, par.3.

que l'exception, tandis que le régime juridique actuel ne tient pas compte de la nature intangible et anonyme du cyberespace[376].

La situation de l'État-victime dont la population a été attaquée est encore aggravée par l'incertitude de contre-mesures et le recours à la force dans le cadre de la légitime défense. Aujourd'hui, un État qui décide à recourir à l'une de ces mesures le ferait à ses propres risques parce qu'il s'appuie sur l'appréciation unilatérale de la cyberattaque et en cas de faute dans son analyse il encourrait une « *responsabilité à raison de son propre comportement illicite dans l'hypothèse d'une appréciation inexacte* »[377].

Jusqu'à récemment, le problème de l'attribution technique dans le cyberespace était considéré comme quasi insoluble sauf si l'État ou l'individu a confessé une cyberattaque[378] ou si une attaque cinétique consécutive clairement a permis de lier et révéler l'auteur de la cyberopération en question[379]. Cependant les États s'abstiennent de se prononcer sur la responsabilité de leurs « *homologues* ».

Néanmoins, nous pouvons voir des évolutions positives. En 2002 le Conseiller Spécial pour la cybersécurité et le cyberterrorisme de la Maison Blanche aux États-Unis, Richard Clarke, a déclaré publiquement que les États-Unis n'avaient encore aucune preuve établissant un lien entre un État et une cyberattaque[380]. Toutefois, après quelques années, James Clapper, à l'époque le directeur du renseignement national, a constaté des progrès considérables dans ce domaine : « *Although cyber operators can infiltrate or disrupt targeted ICT networks, most can no longer assume that their activities will remain undetected. Nor can they assume that if detected, they will be able to conceal*

[376] La position de l'Indonésie : UN Open-ended working group on developments in the field of information and telecommunications in the context of international security; Second substantive session; Agenda item «International law», op. cit.

[377] ACDI 2001, supra note 19, p. 139, par. 3, cité par Observatoire du Monde Cybernétique, Lettre mensuelle de L'OMC, No. 63, juin 2017, p.8, URL : https://www.defense.gouv.fr/content/download/509768/8608366/file/OBS_Monde%20cybernétique_201706.pdf (visité le 24/07/2020).

[378] Bien que jusqu'à présent, aucun État avait décidé de plaider coupable, il ne faut pas nier la tendance à parler ouvertement de renforcement des capacités. En 2013 le Royaume-Uni était le premier à le faire. Voir Gouvernement du Royaume-Uni, « New cyber reserve unit created », le 29 septembre 2013, URL : https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (visité le 23/07/2020).

[379] DINSTEIN (Yoram), « Computer Network Attacks and Self Defense », Naval War College, *International Law Studies*, Computer Network Attack and International Law, Volume 76, 2002, p. 112, URL : https://digital-commons.usnwc.edu/ils/vol76/iss1/20/ (visité le 23/07/2020).

[380] Testimony of Richard Clarke, Special Advisor to the President for Cyberspace Security, Senate Judiciary Committee, Administrative Oversight and the Courts Subcommittee, hearing titled « Administrative Oversight: Are We Ready For A Cyber Terror Attack? », le 13 février 2002, URL : http://www.techlawjournal.com/security/20020213.asp (visité le 23/07/2020).

their identities. Governmental and private-sector security professionals have made significant advances in detecting and attributing cyber intrusions »[381].

Mais pour certains États la situation reste complexe et s'explique par les inégalités en matière de développement de la cyberinfrastructure : les pays les moins développés n'ont pas des cybercapacités suffisantes pour détecter les responsables des cyberattaques, tandis que le progrès technologique des pays les plus développés leur permet de lancer des cyberattaques en ne laissant aucune trace. La situation est la même pour l'Iran et l'Estonie. L'Iran a payé un lourd tribut au ver informatique Stuxnet, qui avait causé la destruction d'environ 20 % des centrifugeuses nucléaires iraniennes[382], mais ses représentants n'ont pas toujours trouvé les preuves pour imputer la responsabilité à l'auteur de cyberattaque. Quant'à la cyberopération contre Estonie en 2007, le gouvernement estonien en la personne du ministre des Affaires étrangères a déclaré d'abord que l'Union européenne était attaquée (il est probable que l'Estonie espérait obtenir une assistance de l'UE par ces déclarations fortes), car la Russie attaquait l'Estonie[383]. Toutefois, cette déclaration audacieuse a rapidement été atténuée par le discours d'un autre membre du gouvernement dans lequel il a noté que l'Estonie n'avait pas suffisamment de preuves établissant un lien entre les cyberattaques et les autorités russes[384].

Ainsi dans le cybercontexte la disposition de l'affaire *Nicaragua c. États-Unis d'Amérique* d'après laquelle « *le problème, dans ces conditions, n'est pas l'opération juridique consistant à imputer le fait à un État déterminé aux fins d'établir sa responsabilité, mais l'opération préalable de recherche des preuves matérielles permettant d'en identifier l'auteur* »[385] devient particulièrement pertinente.

Maintenant la charge de preuve de la cyberattaque dans le cybercontexte « *se heurte cependant à deux obstacles : la difficulté de prouver de façon certaine l'attribution d'une cyberattaque et l'intervention controversée des entreprises du numérique dans les mécanismes d'attribution* »[386]. La difficulté d'attribution d'une cyberattaque est liée étroitement au caractère anonyme de nombreuses

[381] Office of the Director of National Intelligence of the USA, Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee, le 26 février 2015, p. 2, URL : https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (visité le 25/07/2020).

[382] *Business Insider*, « The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought », le 20 novembre 2013, URL : https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11 (visité le 22/07/2020).

[383] PAU (Aivar), « Statement by the Foreign Minister Urmas Paet », 1er mai 2007, URL : https://epl.delfi.ee/news/eesti/statement-by-the-foreign-minister-urmas-paet?id=51085399 (visité le 23/07/2020).

[384] *The New York Times*, « Estonia says cyber-assault may involve the Kremlin », le 17 mai 2005, URL : https://www.nytimes.com/2007/05/17/world/europe/17iht-estonia.4.5758556.html?smid=pl-share (visité le 23/07/2020).

[385] CIJ, *Nicaragua c. États-Unis d'Amérique*, le 27 juin 1986, par. 57.

[386] Observatoire du Monde Cybernétique, Lettre mensuelle de L'OMC, No. 63, op. cit., p.9.

attaques et à une certaine opacité favorisée par l'Internet[387]. Les auteurs de la cyberattaque visent à « *altérer leur adresse IP ou de faire transiter leurs communications par des serveurs innocents pour les utiliser comme des « zombies »* »[388]. La technique *spoofing* qui désigne l'usurpation d'identité électronique d'un autre individu ou d'une autre organisation illustre cette situation. Cette pratique vise à masquer une identité réelle (par exemple, adresse IP) afin d'attaquer des objets en usurpant l'adresse d'un autre ordinateur. D'après le groupe international d'experts qui a élaboré le Manuel de Tallinn, c'est cette pratique qui a été utilisée par les malfaiteurs non-étatiques pendant l'incident en l'Estonie en 2007[389]. C'est pourquoi les cyberattaques, dont les traces ont révélé « *les adresses IP coïncidant avec celles d'ordinateurs de l'administration centrale russe* »[390], n'ont pas provoqué la responsabilisation de la Fédération de Russie. Mais il existe de nombreux autres moyens qui peuvent être utilisés par l'auteur de la cyberattaque, par exemple, « *dissimuler l'origine d'une cyberattaque en modifiant les fuseaux horaires dans les métadonnées d'un malware* »[391] ce qui complique également l'attribution de la responsabilité.

La participation des entreprises spécialisées du numérique dans les cyberattaques pendant le conflit international entre États rend encore plus difficile la responsabilisation. Les États pourraient échapper à leurs responsabilités simplement en externalisant leur « *travail inférieur* »[392] à des groupes privés et à des particuliers. Tout comme la reine Elizabeth Ier d'Angleterre a officiellement autorisé les pirates à piller les trésors de son rival Philippe II d'Espagne au XVIe siècle, les États visent à armer et encourager de plus en plus des groupes criminels et activistes à se doter des cyberarmes nécessaires pour nuire à leurs adversaires, tout en restant à bout de bras[393]. Cette opinion est partagée par l'amiral Michael Rogers, à l'époque chef d'United States Cyber Command et directeur de l'Agence de sécurité nationale, qui a souligné à plusieurs reprises que le problème d'attribution de responsabilité provoquée par le

[387] WAXMAN (Matthew), « Cyber-Attacks and the Use of Force : Back to the Future of Article 2(4) », *Yale Journal of International Law*, 2011, pp. 443-444, URL : https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1403&context=yjil (visité le 22/07/2020).

[388] O'CONNELL (Mary Ellen), « Cyber Security without Cyber War », *Journal of Conflict & Security Law*, 2012, p. 202, URL : https://www.law.upenn.edu/live/files/3474-oconnell-m-cyber-security-without-cyber-war-2012 (visité le 22/07/2020).

[389] SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, op. cit., Règle 15, par. 15, p. 92.

[390] CHALVIN (Antoine), « L'ombre du soldat de bronze », *Le Courrier des pays de l'Est*, 2007/4 (No. 1062), p. 12, URL : https://www.cairn.info/revue-le-courrier-des-pays-de-l-est-2007-4-page-6.htm (visité le 8/07/2020).

[391] Observatoire du Monde Cybernétique, Lettre mensuelle de L'OMC, No. 63, op. cit., p.9.

[392] REUTER (Paul), *Le développement de l'ordre juridique international: Écrits de droit international*, Economica, 1995, p. 377.

[393] *Financial Times*, « Cyber crime: states use hackers to do digital dirty work », le 4 septembre 2015, URL : https://www.ft.com/content/78c46db4-52da-11e5-b029-b9d50a74fd14 (visité le 25/07/2020).

recours des États au secteur privé était l'une des tendances les plus importantes à développer dans le domaine de la sécurité numérique aujourd'hui, parce que les États-nations utilisent des substituts comme moyen de surmonter nos capacités en matière d'attribution[394].

Toutefois, bien que l'utilisation des logiciels et techniques spécifiques par des auteurs des cyberattaques complique les choses considérablement ou même rende parfois impossible la poursuite des auteurs de crimes et l'administration de la justice, les technologies qui visent à suivre les traces des responsables ne cessent d'évoluer. D'après les observations de David Grout, Directeur technique Europe du Sud de FireEye, entreprise de sécurité informatique, « *nous suivons au quotidien 18 000 groupes malveillants et nous attribuons un peu moins de 10 % des attaques observées : c'est le résultat d'un processus qui attend de recueillir suffisamment d'éléments techniques et politiques avant de se prononcer* »[395].

Sans entrer dans les détails techniques, nous pourrions commencer par des moyens plus faciles pour trouver les criminels de guerre. À cet égard, Jason Healy, directeur de la Cyber Statecraft Initiative du Conseil de l'Atlantique, propose les 14 questions auxquelles les réponses peuvent aider dans l'engagement de la responsabilité[396] :

1. L'attaque a-t-elle été rattachée à une adresse IP d'État ?
2. L'attaque a-t-elle été attribuée à une entité ou organisation d'État ?
3. Les outils servant aux attaques ont-ils été écrits dans la langue nationale d'un État ?
4. Les attaques ont-elles été attribuées à un État qui détient le contrôle exclusif de sa cyberinfrastructure et d'Internet ?
5. Quel était le degré de sophistication technique de l'attaque par rapport aux attaques standard ?
6. À quel point le ciblage de l'attaque était-il sophistiqué, par exemple, de grande portée ou précis ?
7. Quel était l'état d'esprit d'un État accusé et de ses citoyens ?
8. Un avantage commercial a-t-il été tiré de l'attaque ?
9. L'État accusé soutient-il directement les hackers ?
10. Existe-t-il une corrélation entre des attaques et des déclarations publiques ?

---

[394] *Financial Times*, « Cyber crime: states use hackers to do digital dirty work », op. cit.

[395] DURAND (Corentin), « Attribution des cyberattaques : le jeu toujours plus compliqué de la dissuasion », *Numerama*, le 23 novembre 2018, URL : https://cyberguerre.numerama.com/64-attribution-des-cyberattaques-le-jeu-toujours-plus-complique-de-la-dissuasion.html (visité le 25/07/2020).

[396] HEALEY (Jason), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, 2013, p. 266.

11. L'État accusé a-t-il coopéré à l'enquête sur l'agression ?
12. Qui profite le plus de l'attaque (*cui bono*) ?
13. Existe-t-il une corrélation avec la politique nationale d'un État en matière de cyberattaques / espionnage / guerre ?
14. L'attaque était-elle un élément accessoire des attaques cinétiques ou a-t-elle été associée à eux ?

Toutefois, il serait difficile à trouver les réponses à ces questions sans recours aux moyens plus pointues permettant attribuer la responsabilité des cyberattaques. Ils peuvent être divisés en deux groupes : techniques et politiques.

Les techniques d'attribution principales d'aujourd'hui ont été identifiées par Andrew Nicholson, spécialiste de la cybersécurité à l'Université de Warwick, et Neil Rowe, professeur d'informatique au Naval Postgraduate School. Ils notent que les techniques les plus connues pa sont *payload attribution*, *traceback techniques*, par exemple *honeypots*[397] et *attribution of files* et *attribution of Internet traffic*[398].

L'identification, que Rowe a appelé *attribution of files* ou « *attribution de fichiers* », englobe l'identification du fait qu'un système a été attaqué ou est en train d'être attaqué et l'identification des outils utilisés pour mener cette attaque[399]. L'information recueillie lors de l'attribution des fichiers peut donner des pistes sur l'auteur potentiel : les métadonnées du code peuvent indiquer la langue utilisée par les auteurs, le fuseau horaire de l'auteur et d'autres détails qui sont susceptibles d'être utilisés pour faire un portrait du suspect. Toutefois, cette technique ne donne pas des données toujours précises, car le code et les extraits de code sont systématiquement achetés et vendus ou piratés et réutilisés par plusieurs auteurs. Les connaissances acquises grâce à une telle attribution ne démontreront vraisemblablement pas qui est l'auteur, mais peuvent être utilisées pour attribuer l'attaque à un État indirectement.

La principale méthode utilisée aujourd'hui pour attribuer des attaques informatiques est *attribution of Internet traffic* ou « *attribution de trafic réseau* ». En réalité, le trafic Internet est composé de *paquets* d'informations. Seule l'adresse source fournit des informations sur l'origine du

[397] NICHOLSON (Andrew), « A Taxonomy of Technical Attribution Techniques for Cyber Attacks », Proceedings of the 11th European Conference on Information Warfare and Security, janvier 2012, pp. 188- 198.

[398] ROWE (Neil), « The Attribution of Cyber Warfare », in: GREEN (James), Cyber Warfare: A Multidisciplinary Analysis, 2016, pp. 62-67, URL : http://opac.lib.idu.ac.id/unhan-ebook/assets/uploads/files/4cc80-045.cyber-warfare.pdf (visité le 25/07/2020).

[399] *Ibid*, p. 62.

paquet sous la forme d'une adresse IP. Les différents moyens, par exemple, Tor, peuvent délibérément changer les paquets pour dissimuler leurs origines, tandis que la technologie *backward tracing* permet de déterminer l'adresse IP d'auteur de l'attaque, même si elle a été masquée. Pour ce faire, il faut contacter l'administrateur du dernier site par le bias duquel la cyberattaque a été lancée, lui demander de récupérer les informations d'origine mises en cache et vérifier ces données jusqu'à ce que la source d'origine soit trouvée. C'est exactement ce qu'a fait la police du Royaume-Uni qui a prié le fournisseur de VPN de fournir des données des utilisateurs du service. Grâce à cette coopération, la police a réussi à arrêter un membre supposé des groupes de hackers Lulzsec et Anonymous[400]. Cependant, il faut toujours garder à l'esprit que les enregistrements de paquet de données ne sont conservés que pendant un temps limité et parfois cette période ne dépassant pas 30 jours.

Les méthodes d'attrubition de trafic réseau se développent rapidement et deviennent accessibles au public. En particulier, Rick Hofstede, spécialiste Université de Twente, l'Institut de Centre for Telematics and Information Technology, a mis au point un logiciel « SSHCure » disponible en *open source*, pour les équipes d'intervention en cas d'urgence informatique. Sa méthode s'avère efficace et diminue le nombre d'incidents, avec une précision de détection pouvant atteindre 100 %, en fonction de l'application réelle et du type de réseau[401].

Traceback techniques peuvent être divisés en deux catégories : *preventive traceback* et *reactive traceback*[402]. *Preventive traceback* vise à empêcher les adresses IP falsifiées ou les adresses IP illégitimes d'accéder à des systèmes spécifiques, par exemple, à des infrastructures civiles, cependant, ce technique ne peut pas identifier la source des attaques et ne fournit donc pas de base pour l'identification de l'attaquant, mais peut servir d'une méthode de protection pour des infrastructures civiles[403]. La technique de réactive traceback, au contraire, offre la possibilité de tracer une attaque. Par exemple, la méthode de link testing ou « *test de liens* » fonctionne à rebours à l'égard du système attaqué, en demandant des informations de chaque routeur afin de trouver le routeur qui avait transféré les paquets falsifiés. Ceci est répété jusqu'à ce que l'adresse IP d'origine soit localisée. Toutefois, les données tirées par ce moyen ne sont pas suffisantes pour l'attribution juridique, car le malware chargé

[400] *ZDNet*, «Hide My Ass throws light on 'LulzSec' logs», le 27 septembre 2011, URL : https://www.zdnet.com/article/hide-my-ass-throws-light-on-lulzsec-logs/ (visité le 26/07/2020).

[401] Université de Twente, « New method for monitoring internet traffic to detect cyber attacks », le 29 juin 2016, URL : https://phys.org/news/2016-06-method-internet-traffic-cyber.html (visité le 10/07/2020).

[402] TENALI (Naga Mani), JYOSYULA (Bala Savitha), « IP Traceback Scenarios », *Global Journal of Computer Science and Technology Network, Web & Security*, Vol. 13, 2013, p. 20, URL : https://computerresearch.org/index.php/computer/article/download/373/373/ (visité le 11/07/2020).

[403] *Ibid.*

d'installer la charge sur le système infecté proviendra probablement d'une autre source. Le logiciel malveillant devra, donc, être analysé afin d'identifier l'auteur du logiciel, ce qui pourrait donner des indices quant à l'origine de la cyberattaque.

La technique *Honeypot* ou « *pot de miel* », comme représentant de *traceback techniques*, est susceptible d'identifier un événement d'attaque, d'identifier les vecteurs d'attaque, d'analyser de nouveaux types d'attaques et les suivre par régions. Honeypots eux-mêmes ne sont pas nécessairement un outil d'attribution, mais servent de mécanisme d'aide à l'attribution. Cette technique représente un « *serveur configuré pour détecter un intrus en reflétant (par effet de miroir) un système de production réel* »[404]. C'est-à-dire Honeypots est un dispositif mobile fonctionnant sur Internet qui semble être une véritable série d'adresses IP configurées pour piéger les attaques entrantes à diverses fins[405]. Ses principaux avantages résident dans le fait que Honeypots peuvent être utilisés non seulement pour identifier l'adresse IP d'origine, mais également pour protéger des civils et les infrastructures vitales contre les attaques DDoS en mettant cette adresse IP sur liste noire et en empêchant ces adresses IP d'avoir accès à la cible visée par l'attaque[406].

Ces techniques de traçage de l'adresse IP sont conçus pour fonctionner contre les attaques DoS ou DDoS, comme celles subies par la Géorgie en 2008 et l'Estonie en 2007. En ce qui concerne Stuxnet, cette cyberattaque diffère de celles évoquée précédemment en ce que le vecteur d'attaque ne dépend pas nécessairement d'Internet. Par conséquent, il faut recourir à d'autres voies techniques qui se focalisent sur le code malveillant et pas sur l'adresse IP afin d'identifier l'auteur de la cyberattaque.

Une de ces techniques est *payload attribution*. Les cyberarmes laissent une charge de code informatique malveillant sur chaque système qu'elles infectent, ce qui permet de procéder à un examen scientifique de cette charge après sa découverte afin de fournir des preuves des créateurs de la cyberattaque, de ses origines et de son but. Les preuves tirées de l'examen de la charge peuvent être utilisées pour faciliter l'attribution des cyberattaques aux États responsables de leur création et de leur utilisation. Cependant, les preuves seules, sans autre piste d'implication de l'État, ne suffisent pas pour attribuer l'attaque à un État. L'examen de la charge utile d'une cyberarme peut être effectué

[404] SHUKLA (Shantanu), SINHA (Sonal), « Use of Honeypot and IP Tracing Mechanism for Prevention of DDOS Attack », *International Journal of Scientific Engineering and Research*, 2015, p. 95, URL : http://docplayer.net/8988379-Use-of-honeypot-and-ip-tracing-mechanism-for-prevention-of-ddos-attack.html (visité le 26/07/2020).

[405] JOLLEY (Jason), « Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law », Thèse de doctorat, Université de Glasgow, 2017, p. 164, URL : http://theses.gla.ac.uk/8452/1/2017JolleyPhD.pdf (visité le 21/07/2020).

[406] *Ibid*, p. 165.

par le biais de l'investigation numérique et de l'ingénierie inverse. Les preuves recueillies permettent de recevoir les informations suivantes : le type de clavier utilisé, le langage utilisé, par exemple, Lua, Python, C / C ++, le fuseau horaire de l'ordinateur ou des logiciels malveillants. Par exemple, cette méthode a permis de supposer que c'étaient les Etats-Unis et l'Israël, qui ont développé un ver Stuxnet[407].

Même si le processus d'attribution n'est pas 100 % fiable, la corrélation d'informations entre attaques peut être une étape utile vers une attribution ultérieure. Les attaquants, tant criminels qu'engagés dans la cyberguerre, ont tendance à répéter certaines méthodes d'attaque (*modus operandi*), ainsi que les codes d'attaque.

Ainsi la cyberattaque peut être identifiée en vertu du « *type de malware, des moyens financiers, humains et techniques utilisés pour mettre en œuvre l'attaque, du but poursuivi par l'attaquant* »[408]. Cependant, aucune technique d'attribution de responsabilité n'est pas capable de fournir des preuves solides pour imputer la cyberattaque à un État ou à un individu. Chaque technique d'attribution a ses forces et ses faiblesses, et le succès de l'attribution dépend de l'utilisation de plusieurs techniques conjointement[409].

Certains entreprises et États évitent les accusations à l'égard des auteurs des cyberattaques à cause des raisons politiques. Dans ce cas, d'après l'Observatoire du monde cybernétique, réalisé par la Compagnie européenne d'intelligence stratégique à la demande de la Délégation aux affaires stratégiques du Ministère de la défense de la France, l'une des solutions au problème pourrait être la création d'une « *instance internationale disposant de l'expertise technique nécessaire qui serait alors chargée d'enquêter sur l'attribution, de manière fiable et indépendante, des cyberattaques pouvant constituer une violation du droit international* »[410]. Ce mécanisme international d'attribution pourrait devenir une nouvelle façon de canaliser les disputes politiques. Dans son activité cet organe peut tirer parti de l'expérience à la fois de l'Agence internationale de l'énergie atomique et de l'Organisation internationale pour l'interdiction des armes chimiques qui « *disposent d'une expertise technique dans leur domaine et la capacité de procéder à des vérifications, notamment en ce qui concerne les*

[407] *L'OBS*, « Stuxnet : comment les Etats-Unis et Israël ont piraté le nucléaire iranien », le 4 juin 2012, URL : https://www.nouvelobs.com/rue89/rue89-internet/20120604.RUE0433/stuxnet-comment-les-etats-unis-et-israel-ont-pirate-le-nucleaire-iranien.html (visité le 02/08/2020).

[408] Observatoire du Monde Cybernétique, Lettre mensuelle de L'OMC, No. 63, op. cit., p.9.

[409] WHEELER (David), LARSEN (Gregory), LEADER (Task), « Techniques for Cyber Attack Attribution », Institute for Defense Analysis, octobre 2003, p.3., URL : https://www.researchgate.net/publication/235170094_Techniques_for_Cyber_Attack_Attribution (visité le 24/07/2020).

[410] Observatoire du Monde Cybernétique, Lettre mensuelle de L'OMC, NO. 63, op. cit., p.10.

déclarations des États »[411] et encourager la coopération technique et scientifique nécessaire pour l'évolution des moyens de l'expertise.

Si l'État présumé d'avoir fait une cyberattaque refuse de coopérer, la capacité d'attribuer une cyberattaque est faible, voire nulle[412]. Pour l'éviter, il est nécessaire d'accroître la transparence dans le domaine des TIC et, pour les États, de prendre des engagements pour l'avenir. À cet égard, l'UNIDIR recommande aux États de favoriser[413] :

1. L'échange de vues et d'informations sur une base volontaire sur les stratégies et politiques nationales, les meilleures pratiques, les processus décisionnels, et les mesures visant à améliorer la coopération internationale ;
2. La création de cadres consultatifs bilatéraux, régionaux et multilatéraux pour l'instauration de la confiance, ce qui pourrait comprendre des ateliers, des séminaires et des exercices pour affiner les délibérations nationales sur les moyens de prévenir les incidents perturbateurs résultant de l'utilisation des TIC par les États ;
3. L'amélioration du partage d'informations entre États sur les incidents de sécurité des TIC, impliquant une utilisation plus efficace des canaux existants ou la mise en place de nouveaux canaux et de mécanismes appropriés pour recevoir, collecter, analyser et partager les informations relatives aux incidents de TIC, en vue d'une intervention, d'une récupération et d'une atténuation des actes rapides ;
4. Le renforcement de la coopération pour faire face aux incidents pouvant affecter les TIC ou les infrastructures critiques. Cela pourrait inclure des directives et des pratiques des États visant à prévenir les attaques causées par des acteurs non-étatiques ;
5. L'amélioration des dispositifs pour la coopération entre les services de détection et les services de répression afin de réduire les cyberincidents ;
6. La détermination des points de contact aux niveaux politique et technique pour régler les problèmes liés aux TIC ;
7. L'échange de vues des États aux catégories d'infrastructures qu'ils considèrent critiques et aux efforts nationaux qui visent à les protéger.

Ainsi la somme des preuves reçues sous réserve du travail conjoint des cercles techniques et politiques et présentées devant des instances juridiques compétentes permettra d'engager la

[411] Observatoire du Monde Cybernétique, Lettre mensuelle de L'OMC, NO. 63, op. cit., p. 10.
[412] JOLLEY (Jason), « Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law », Thèse de doctorat, op. cit., p. 142.
[413] UNIDIR, « The United Nations, Cyberspace and International Peace and Security », op. cit., pp. 22-23.

responsabilité de violations commises par États et individus et, par conséquent, de réduire les cyberattaques en général[414].

[414] JOLLEY (Jason), « Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law », Thèse de doctorat, op. cit., p. 143.

Conclusion

L’augmentation du nombre de cyberattaques est notable depuis ces deux dernières décennies. Les observations montrent que le domaine d’utilisation des cyberarmes s’est progressivement étendu et les parties aux conflits armés internationaux recourent de plus en plus à des cyberopérations.

La cyberattaque constitue une opération lancée à des fins hostiles contre un ennemi et destinée à nuire à l’adversaire en utilisant un ordinateur et prendre l'avantage militaire. Nonobstant la nature virtuelle des cyberattaques, elles sont capables d’infliger des pertes graves et irréparables, notamment, sur le plan humain et même déclencher un conflit armé international. C’est pourquoi nous faisons face aujourd’hui à un problème de l’application des normes du DIH au cyberespace.

Ce problème s’explique par plusieurs raisons : l’absence de consensus sur la définition d’une cyberattaque dans la communauté internationale, la complexité de transposer les normes du DIH dans le cybercontexte, le manque de capacités techniques pour attribuer des cyberopérations et parfois, l’absence de volonté politique chez certains États de régler les conflits dans le cyberespace afin de se soustraire à la justice.

L’un des moyens qui existent aujourd’hui pour combler un vide juridique est de recourir aux normes du droit international humanitaire coutumier et de les transposer dans le cybercontexte comme l’ont fait les experts du Manuel de Tallinn. Ces règles obligent les parties au conflit armé international à respecter les principes fondamentaux du droit humanitaire à savoir les principes de discrimination, de proportionnalité, de précaution, d’humanité, d’équilibre entre la nécessité militaire et le principe d’humanité, d’interdiction des maux superflus et des souffrances inutiles, d’égalité des belligérants et de non-réciprocité des obligations humanitaires. L’application de ces principes permet considérablement d’atténuer les conséquences des conflits armés.

Entre outres, les normes du DIH coutumier donnent aux parties au conflit le droit de légitime défense en cas d’attaque et confirment la pertinence des critères établis par le cas de Caroline dans le cybercontexte qui doivent pris en compte avant la réponse, à savoir la nécessité, la proportionnalité de la défense, la présence ou l’imminence de la menace qui ne laisse ni le choix des moyens ni le temps de délibérer. Conscient de la nature spécifique du cyberespace qui permet de lancer une attaque

avec un clic et détruire des infrastructures critiques en quelques secondes, de plus en plus sont d'avis que les États attaqués peuvent exercer son droit de défense non seulement après une cyberattaque, mais bien avant. Ces dispositions s'appliquent à la légitime défense individuelle et collective, comme en attestent les textes de l'OTAN et l'UE et aussi conserve le droit du Conseil de sécurité d'intervenir afin maintenir la paix et la sécurité internationales.

Toutefois, le problème de l'engagement de la responsabilité est à moitié résolu. D'une part, nous pouvons constater l'existence de consensus sur l'application des principes de responsabilité étatique et individuelle établis par le droit coutumier et complétés par les décisions des tribunaux internationaux par rapport aux États et individus ayant commis des crimes prévus par le droit international dans le cybercontexte.

Mais d'autre part, le processus d'attribution de la responsabilité se complexifie à cause des caractéristiques spécifiques des cyberattaques et le comportement de leurs auteurs dans le cyberespace. Les opérateurs des cyberopérations ne respectent pas toujours les obligations du droit humanitaire qui les obligent à faire la distinction entre la population civile et les combattants à cause de l'interconnectivité des cyberinfrastructures civiles et militaires. Ils ne suivent pas les règles d'après lesquelles les hackers sont tenus de porter l'uniforme militaire et les armes ouvertement à cause de la nature anonyme de leur activité. Cela, à son tour, s'accompagne d'une absence de pistes et de preuves matérielles pour trouver et traduire en justice les responsables de la part des instances judiciaires.

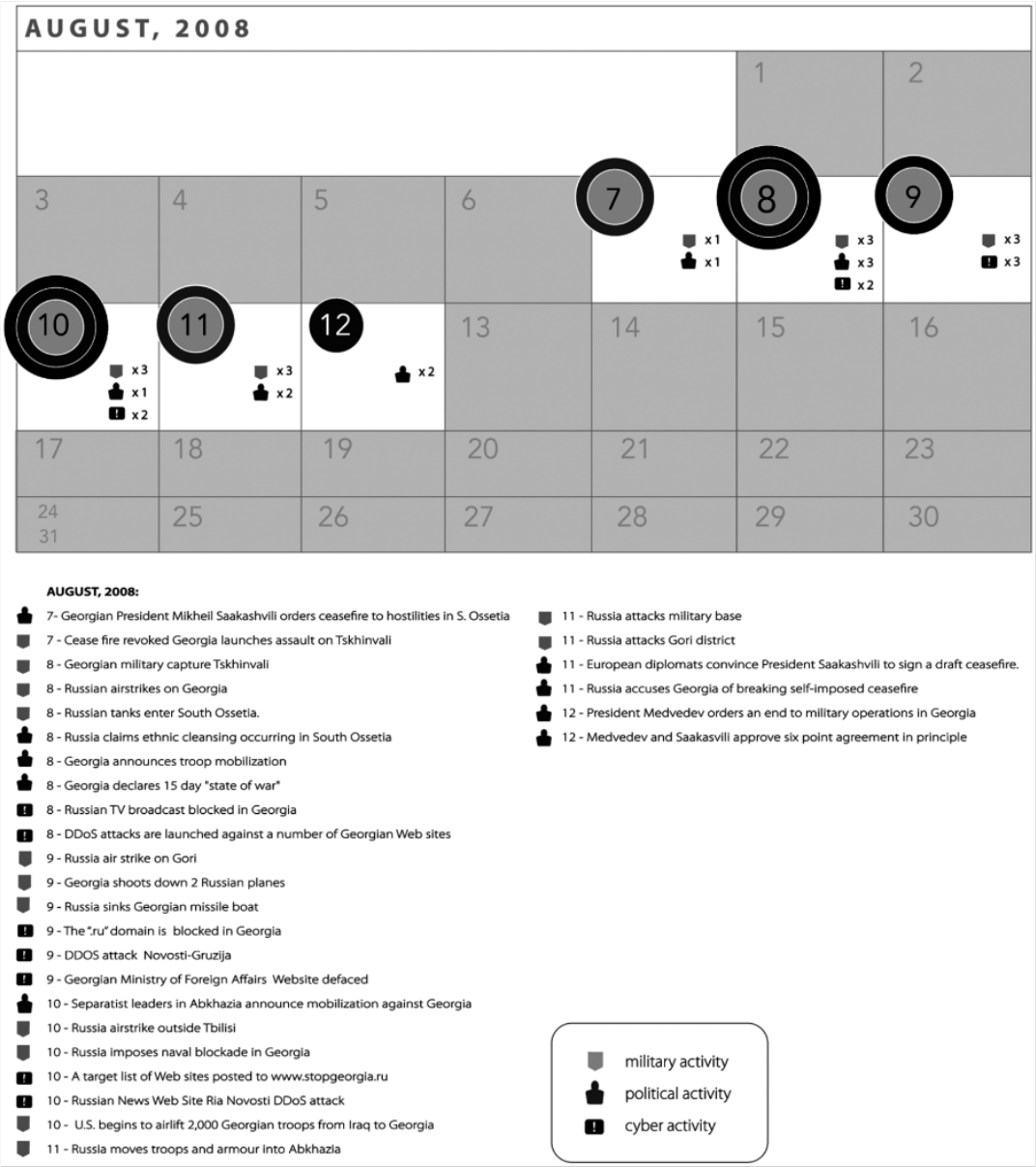
Conscient du fait que la dimension cyber est venue accroître les risques que courent, la communauté internationale doit agir sur le plan technique pour assurer le respect du DIH face aux cyberopérations. Cet état de choses conduit à la nécessité pour les États, les instances judiciaires et les organisations internationales de coopérer avec la communauté informatique pour mieux résoudre ce problème. L'un des axes prioritaires de ce travail doit être la coopération des ONG avec les acteurs du secteur technique (Miscrosoft, Google etc.) d'autant que ces derniers disposent certaine expérience en la matière[415]. Ainsi en réunissant les aspects juridique, politique, informatique et humanitaire et en étant armé des techniques spéciales comme *honeypots*, *payload analysis* et les autres moyens visant à tracer les auteurs de crimes, la communauté internationale pourrait compter sur le respect des règles du DIH en temps de conflit armé.

[415] Voir, par exemple, Microsoft, « PROTECTING PEOPLE IN CYBERSPACE: The Vital Role of the United Nations in 2020», le 1er avril 2020, pp. 3-7, URL : https://www.microsoft.com/security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-what-to-do/ (visité le 29/07/2020).

Annexes

Annexe 1

Tableau des attaques russes pendant le conflit entre la Russie et la Georgie en 2008 (la combinaison des attaques militaires et les cyberattaques)



Annexe 2

Tableau des mesures imposées ou appliquées en vertu de l'article 41 en 2014- 2015

Table 6
Overview of measures imposed pursuant to Article 41 or in place in 2014-2015

	Measures															
Measures taken in connection with	*Somalia and Eritrea*	*Taliban*	*ISIL (Da'esh) and Al-Qaida*	*Iraq*	*Liberia*	*Democratic Republic of the Congo*	*Côte d'Ivoire*	*Sudan*	*Lebanon*	*Democratic People's Republic of Korea*	*Islamic Republic of Iran*	*Libya*	*Guinea-Bissau*	*Central African Republic*	*Yemen*[89]	*South Sudan*[90]
Arms embargo	X	X	X	X	X	X	X	X	X	X	X	X		X	X	
Travel ban or restrictions	X	X	X			X	X	X	X	X	X	X	X	X	X	X
Asset freeze	X	X	X	X		X	X	X	X	X	X	X		X	X	X
Ban on arms exports by target state										X	X	X				
Business restrictions	X (Eritrea)										X	X				
Financial restrictions	X (Eritrea)	X	X							X	X	X				
Non-proliferation measures										X	X					
Prohibition on bunkering services										X	X	X				
Public financial support for trade restrictions										X	X					

[89] Imposition of new measures pursuant to resolution 2140 (2014) of 26 February 2014.
[90] Imposition of new measures pursuant to resolution 2206 (2015) of 3 March 2015.

Annexe 3

Tableau des mesures imposées ou appliquées en vertu de l'article 41 en 2014- 2015

Restrictions on ballistic missiles				X	X		
Transport and aviation sanctions				X			
Diamond embargo							
Diplomatic/overseas representation restrictions				X			
Luxury goods embargo				X			
Oil/petroleum embargo		X				X	
Trade ban on cultural goods		X					
Charcoal ban	X						

Bibliographie

I. OUVRAGES GÉNÉRAUX

1. ALLAND (Denis), CHETAIL (Vincent), DE FROUVILLE (Olivier), *Unité et diversité du droit international : écrits en l'honneur du professeur Pierre-Marie Dupuy*, Leiden, Boston, Martinus Nijhoff Publishers, 2014, 1022 p. ;
2. AUST (Anthony), *Handbook of International Law*, Cambridge University Press, 2010, 592 p. ;.
3. BURROWS (Mathew), *The Future, Declassified : Megatrends That Will Undo the World Unless We Take Action*, Mann, Ivanov and Ferber Publisher, Moscow, 2015, 352 p. ;
4. CARRON (Djemila), *L'acte déclencheur d'un conflit armé international*, Schulthess, Genève, 2016, 522 p. ;
5. CASSESE (Antonio), *International Law*, 2ème édition, Oxford, Oxford University Press, 2005, 558 p. ;
6. CLARKE (Richard Alan), KNAKE (Robert), *Cyber War: The Next Threat to National Security and What to Do About It*, Harper Collins Publishers, 2010, 312 p. ;
7. DAVID (Eric), *Principes de droit des conflits armés*, Bruylant, Bruxelles, 2012, 1412 p. ;
8. DE FROUVILLE (Olivier), *Droit international pénal : sources, incriminations, responsabilité*, Pedone, 2012, 522 p. ;
9. DE VATTEL (Emeric), *Le Droit des gens ou Principes de la loi naturelle appliqués à la conduite et aux affaires des nations et des souverains* [1757], Livre II, Tome II, Chap. IV, Paris, Chez Janet et Cotelle, 1820, 864 p. ;
10. DECAUX (Emmanuel), DE FROUVILLE (Olivier), *Droit international public*, 11 édition, Dalloz, 2018, 647 p. ;
11. DINSTEIN (Yoram), *War, Aggression and Self-Defence*, Cambridge University Press, Cambridge, 2011, 408 p. ;
12. GRAY (Christine), *International Law and the Use of Force*, Oxford, Oxford University Press, 2008, 455 p.;
13. GRIGNON (Julia), *L'applicabilité temporelle du droit international humanitaire*, Schulthess, Genève, 2014, 487 p. ;
14. HEALEY (Jason), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, 2013, 356 p. ;

15. HENCKAERTS (Jean-Marie), DOSWALD-BECK (Louise), *Droit international humanitaire coutumier, Volume I : règles*, CICR, 2006, 961 p. ;
16. JONES (Jeffrey), *Studies Combined: Cyber Warfare In Cyberspace - National Defense, Workforce And Legal Issues*, U.S. Department Of Defense, 2018, 2822 p. ;
17. MELZER (Nils), *Droit international humanitaire : introduction détaillée*, CICR, Genève, 2018, 404 p. ;
18. PICTET (Jean), *Development and principles of international humanitarian law*: course given in July 1982 at the University of Strasbourg as part of the courses organized by the International Institute of Human Rights, Springer, 1985, 108 p. ;
19. REUTER (Paul), *Le développement de l'ordre juridique international: Écrits de droit international*, Economica, 1995, 643 p. ;
20. ROSCINI (Marco), *Cyber Operations and the Use of Force in International Law*, OUP Oxford, 2014, 336 p. ;
21. SASSOLI (Marco), BOUVIER (Antoine) et QUINTIN (Anne), *How Does Law Protect in War ?*, CICR, 2014, 401 p. ;
22. SCHMITT (Michael), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, 616 p. ;
23. SCHMITT (Michael), *Tallinn Manual on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2013, 215 p. ;
24. SHARP (Walter Gary), *Cyberspace and the use of force*, Aegis Research Corporation, 1999, 250 p. ;
25. WERLE (Gerhard), *Principles of international criminal law*, TMC Asser Press, Haye, 2005, 488 p. ;

II. THÈSES ET DOCUMENTS SPÉCIAUX

1. Action en cas de menace contre la paix, de rupture de la paix et d'acte d'agression (Chapitre VII), URL : https://www.un.org/securitycouncil/fr/content/repertoire/actions (visité le 20/06/2020) ;
2. Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, and Charter of the International Military Tribunal, August 8, 1945, URL : https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.2_Charter%20of%20IMT%201945.pdf (visité le 30/06/2020) ;
3. Assemblée générale des Nations Unies, Commission du droit international, Le statut et le jugement du Tribunal de Nuremberg, Historique et analyse (Mémorandum du Secrétaire

général), Lake Success, New-York, 1949, 117 p., URL : https://digitallibrary.un.org/record/160809/files/A_CN.4_5-FR.pdf (visité le 30/06/2020) ;

4. Assemblée générale des Nations Unies, Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, le 22 juillet 2015, URL : https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&Lang=F (visité le 11/05/2020) ;
5. Assemblée générale des Nations Unies, Résolution A/RES/73/266, le 22 décembre 2018, URL : https://undocs.org/fr/A/RES/73/266 (visité le 11/05/2020) ;
6. Assemblée générale des Nations Unies, Résolution 53/70 (1999), le 4 janvier 1999, URL : https://undocs.org/fr/A/RES/53/70 (visité le 20/06/2020) ;
7. Assemblée Générale des Nations Unies, Résolution 3314 (XXIX), le 14 décembre 1974, URL : https://undocs.org/fr/A/RES/3314 (XXIX) (visité le 21/01/2020) ;
8. Assemblée Nationale, Commission de la Défense Nationale et des Forces Armées, Rapport d'information, le 4 juillet 2018, 147 p., URL : http://www.assemblee-nationale.fr/15/pdf/rap-info/i1141.pdf (visité le 28/11/2019) ;
9. Australia's OEWG Non Paper: Case studies on the application of international law in cyberspace, 11 p., URL : https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf (visité le 12/05/2020) ;
10. Australian Government, Australia's Cyber security strategy, 2016, 68 p., URL : https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf (visité le 28/11/2019) ;
11. Austrian Cyber Security Strategy, 2013, 25 p., URL : https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf (visité le 28/11/2019) ;
12. Belgian National Cyber Security Strategy, le 23 novembre 2012, 15 p., URL : https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en (visité le 28/11/2019) ;
13. CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », Rapport, XXXIIème Conférence internationale de la Croix-Rouge et du Croissant-Rouge, 8-10 décembre 2015, Genève, Suisse, 72 p., URL:

https://www.icrc.org/fr/download/file/15110/32ic-report-on-ihl-and-challenges-of-armed-conflicts-fre.pdf (visité le 02/12/2019) ;

14. CICR, Les Commentaires sur la Convention de Genève pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne de 1949, 2018 ;
15. CICR, Les Commentaires sur la Convention de Genève pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne de 1949, 2016 ;
16. CICR, Les Commentaires sur le Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux de 1977, 1987 ;
17. CICR, Les Commentaires sur Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux de 1977, 1987 ;
18. CICR, Les principes fondamentaux de la Croix-Rouge et du Croissant-Rouge, 20 p., URL : https://www.icrc.org/fre/assets/files/other/icrc_001_0513_principes_fondamentaux_cr_cr.pdf (visité le 16/05/2020) ;
19. Commentary of 1958, Convention (IV) de Genève relative à la protection des personnes civiles en temps de guerre, 12 août 1949, Responsabilité des parties contractantes, URL : https://ihl-databases.icrc.org/applic/ihl/dih.nsf/Comment.xsp?action=openDocument&documentId=D99F33F4E37172F2C12563BD002D3075 (visité le 24/06/2020) ;
20. Conseil de l'Union européenne, Décision du Conseil concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres, le 14 mai 2019, URL : http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/fr/pdf (visité le 16/06/2020) ;
21. Conseil de Sécurité des Nations Unies, Résolution 1296 (2000), le 19 avril 2000, URL : https://undocs.org/fr/S/RES/1296(2000) (visité le 27/06/2020) ;
22. Conseil de Sécurité des Nations Unies, Résolution 1674 (2006), le 28 avril 2006, URL : https://undocs.org/fr/S/RES/1674(2006) (visité le 27/06/2020) ;
23. Conseil de Sécurité des Nations Unies, Résolution 1265 (1999), le 17 septembre 1999, URL : https://undocs.org/fr/S/RES/1265(1999) (visité le 27/06/2020) ;
24. Conseil de sécurité des Nations Unies, Résolution 1591 (2005), le 29 mars 2005, URL : http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1591(2005)&Lang=F (visité le 20/06/2020) ;
25. Conseil de Sécurité des Nations Unies, Résolution 1738 (2006), le 23 décembre 2006, URL : https://undocs.org/fr/S/RES/1738(2006) (visité le 27/06/2020) ;
26. Conseil de Sécurité des Nations Unies, Résolution 1894 (2009), le 16 novembre 2009, URL : https://undocs.org/fr/S/RES/1894(2009) (visité le 27/06/2020) ;

27. Conseil de Sécurité des Nations Unies, Résolution 2175 (2014), le 29 août 2014, URL : https://undocs.org/fr/S/RES/2175(2014) (visité le 27/06/2020) ;
28. Conseil de sécurité des Nations Unies, Résolution 2200 (2015), le 12 février 2015, URL : http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2200%20(2015)&Lang=F (visité le 20/06/2020) ;
29. Conseil de sécurité des Nations Unies, Résolution 2211 (2015), le 26 mars 2015, URL : http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2211%20(2015)&Lang=F (visité le 20/06/2020) ;
30. Conseil de Sécurité, Nations Unies, Résolution 2222 (2015), le 27 mai 2015, URL : https://undocs.org/fr/S/RES/2222(2015) (visité le 27/06/2020) ;
31. Conseil de Sécurité, Nations Unies, Résolution 2286 (2016), le 3 mai 2016, URL : https://undocs.org/fr/S/RES/2286(2016) (visité le 27/06/2020) ;
32. Conseil de Sécurité, Nations Unies, Résolution 2365 (2017), le 30 juin 2017, URL : https://undocs.org/fr/S/RES/2365(2017) (visité le 27/06/2020) ;
33. Conseil de Sécurité, Nations Unies, Résolution 2417 (2018), le 24 mai 2018, URL : https://undocs.org/fr/S/RES/2417(2018) (visité le 27/06/2020) ;
34. Conseil de sécurité, Quarante septième séance, le 18 juin 1946, Ordre du jour provisoire (document S/89), URL : https://undocs.org/fr/S/PV.47 (visité le 22/06/2020) ;
35. Conseil de sécurité, Quatrième rapport de l'Équipe d'appui analytique et de surveillance des sanctions créée en application des résolutions 1526 (2004) et 1617 (2005) du Conseil de sécurité concernant l'organisation Al-Qaida et les Taliban et les personnes et entités qui leur sont associées, le 10 mars 2006, 54 p., URL : https://www.undocs.org/fr/S/2006/154 (visité le 27/06/2020) ;
36. Cyber Security Strategy of the United Kingdom : safety, security and resilience in cyber space, juin 2009, 32 p., URL : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (visité le 28/11/2019) ;
37. Cybersecurity Enhancement Act of 2014 (S.1353) proposé par sénateurs Rockefeller et Thune, URL : https://www.congress.gov/113/plaws/publ274/PLAW-113publ274.pdf (visité le 06/04/2020) ;
38. Declaration of the Minister of Foreign Affairs of the Republic of Estonia, le 1er mai, URL : https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia (visité le 07/04/2020) ;

39. Délégation à l'information et à la communication de la défense, Droit international appliqué aux opérations dans le cyberespace, 20 p., URL : https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf (visité le 10/01/2020) ;
40. Département fédéral des affaires étrangères DFAE, Direction du droit international public, « Guide pratique sur la reconnaissance de la compétence de la Cour internationale de Justice », Berne, 2014, 28 p., URL : https://www.eda.admin.ch/dam/eda/fr/documents/publications/Voelkerrecht/handbook-jurisdiction-international-court_fr (visité le 11/07/2020) ;
41. Department of Political Affairs - Security Council Affairs Division Security Council Practices and Charter Research Branch, «Repertoire of the Practice of the Security Council », 19th Supplement, Part VII, «Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter)», 2014-2015, 117 p., URL : https://www.un.org/en/sc/repertoire/2014-2015/Part_VII/2014-2015_Part_VII.pdf#page=36 (visité le 25/06/2020) ;
42. DESARNAUD (Gabrielle), «Cyberattaques et systèmes énergétiques. Faire face au risque », Études de l'Ifri, janvier 2017, 62 p, URL : https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cybersecurite_2017_2.pdf (visité le 26/03/2020) ;
43. Éléments publics de doctrine militaire de lutte informatique offensive, 12 p., URL : https://www.defense.gouv.fr/content/download/551555/9394645/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf (visité le 25/11/2019) ;
44. Federal Ministry of the Interior, Cyber Security Strategy for Germany, février 2011, 20 p., URL : https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (visité le 28/11/2019) ;
45. GALLAGHER (Patrick), «The Partnership Between the NIST and the Private Sector: Improving Cybersecurity», U.S. Government printing office, Washington, 2014, 58 p. ;
46. GENDRON (Angela), RUDNER (Martin), « Évaluation des cybermenaces pesant contre les infrastructures du Canada », Rapport préparé pour le service canadien du renseignement de sécurité, mars 2012, 72 p, URL : https://www.canada.ca/content/dam/csis-scrs/documents/publications/CyberTrheats_AO_Booklet_FRA.pdf (visité le 18/03/2020) ;

47. Gouvernement du Royaume-Uni, « Foreign Office Minister condemns Russia for NotPetya attacks », le 15 février 2018, URL : https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (visité le 12/04/2020) ;
48. Gouvernement du Royaume-Uni, « New cyber reserve unit created », le 29 septembre 2013, URL : https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (visité le 23/07/2020) ;
49. HOLMBERG (Elin Jansson), «Armed attacks in cyberspace : Do they exist and can they trigger the right to self-defence?», Thesis in International Law, Faculty of Law, Stockholm University, 70 p., URL : http://www.diva-portal.org/smash/get/diva2:854660/FULLTEXT01.pdf (visité le 10/06/2020) ;
50. ICIW, Proceedings of the 6th International Conference on Information Warfare and Security, George Washington University, Washington, DC, USA, 2011, 324 p. ;
51. ICRC, Expert Meeting 14–16 novembre 2018 – Geneva, The potential human cost of cyber operations, mai 2019, 80 p., URL : https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf (visité le 02/12/2019) ;
52. ICRC, Principles of IHL (distinction, proportionality) have direct bearing on cyber operations, Statement to the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security; Second substantive session; Agenda item « International law », le 12 février 2020, URL : https://www.icrc.org/en/document/principles-international-humanitarian-law-distinction-proportionality-have-direct-bearing (visité le 02/05/2020) ;
53. IDC, Victim statistics in Novi Travnik, Vitez, Kiseljak and Busovača, archive, URL : https://web.archive.org/web/20071023095215/http://www.idc.org.ba/aboutus/Overview_of_jobs_according_to_%20centers.htm (visité le 10/07/2020) ;
54. International military tribunal for the Far East, Special proclamation by the Supreme Commander tor the Allied Powers at Tokyo January 19, 1946, URL : https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.3_1946%20Tokyo%20Charter.pdf (visité le 30/06/2020) ;
55. Israel Defense Forces, Twitter, URL : https://twitter.com/IDF/status/1125066395010699264 (visité le 13/06/2020) ;
56. JOLLEY (Jason), « Attribution, State Responsibility, and the Duty to Prevent Malicious Cyber-Attacks in International Law », Thèse de doctorat, Université de Glasgow, 2017, 325 p., URL : http://theses.gla.ac.uk/8452/1/2017JolleyPhD.pdf (visité le 21/07/2020) ;

57. LABORDE (Françoise), « Intensifier la lutte contre le cyberterrorisme sur les réseaux sociaux », 15e législature, 2017, URL : https://www.senat.fr/questions/base/2017/qSEQ170800939.html (visité le 18/03/2020) ;
58. LASNIER (Virginie), « Le mouvement de jeunes « nachi » ou une progéniture de la démocratie dirigée russe (2005-2009) », mémoire, Université du Québec à Montréal, octobre 2009, 146 p., URL : https://archipel.uqam.ca/2460/1/M11085.pdf (visité le 03/04/2020) ;
59. Ministère des Armées de France, La cyberdéfense : enjeu majeur pour le ministère, le 17 octobre 2018, URL : https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation (visité le 28/11/2019) ;
60. Ministry of Foreign Affairs of Estonia, Estonia raised cybersecurity for the first time at the UN Security Council, le 5 mars 2020, URL : https://vm.ee/en/news/estonia-raised-cybersecurity-first-time-un-security-council (visité le 23/06/2020) ;
61. Ministry of Foreign Affairs of Estonia, Signature Event of Estonia's UNSC Presidency: Cyber Stability, Conflict Prevention and Capacity Building, 22 mai 2020, URL : https://vm.ee/en/activities-objectives/estonia-united-nations/signature-event-estonias-unsc-presidency-cyber (visité le 25/06/2020) ;
62. National Cyber Security Strategy, Canada's Vision for Security and Prosperity in the Digital Age, URL : https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx (visité le 28/11/2019) ;
63. Nations unies, Assemblée générale, Résolution 58/32, le 18 décembre 2003, URL : https://undocs.org/fr/A/RES/58/32 (visité le 20/06/2020) ;
64. Nations Unies, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, 2001, URL : http://legal.un.org/ilc/texts/instruments/french/commentaries/9_6_2001.pdf (visité le 19/06/2020) ;
65. NATO, Comprehensive Assistance Package for Ukraine, juillet 2016, 2 p., URL : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_09/20160920_160920-compreh-ass-package-ukraine-en.pdf (visité le 15/06/2020) ;
66. NATO, NATO's practical support to Ukraine, décembre 2015, 2 p., URL : https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151130_1512-factsheet-nato-ukraine-supportr_en.pdf (visité le 15/06/2020) ;
67. Observatoire du Monde Cybernétique, Lettre mensuelle de L'OMC, No. 63, juin 2017, p.9, URL : https://www.defense.gouv.fr/content/download/509768/8608366/file/OBS_Monde%20cybernétique_201706.pdf (visité le 24/07/2020) ;

68. Observatoire du Monde Cybernétique, Lettre mensuelle de L'OMC, No. 63, juin 2017, 12 p., URL : https://www.defense.gouv.fr/content/download/509768/8608366/file/OBS_Monde%20cybernétique_201706.pdf (visité le 24/07/2020) ;
69. OEWG on developments in the field of information and telecommunications in the context of international security, Second «Pre-draft» of the report, 17 p., URL : https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf (visité le 20/06/2020) ;
70. Office of the Director of National Intelligence of the USA, Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee, le 26 février 2015, 29 p., URL : https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (visité le 25/07/2020) ;
71. ONU, Répertoire de la pratique du Conseil de sécurité, URL : https://www.un.org/fr/sc/repertoire/faq.shtml (visité le 22/06/2020) ;
72. OTAN, Cyberdéfense, le 31 mars 2020, URL : https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=fr (visité le 15/06/2020) ;
73. OTAN, Déclaration du sommet du Pays de Galles, le 5 septembre 2014, URL : https://www.nato.int/cps/fr/natohq/official_texts_112964.htm (visité le 15/06/2020) ;
74. PAU (Aivar), « Statement by the Foreign Minister Urmas Paet », 1er mai 2007, URL : https://epl.delfi.ee/news/eesti/statement-by-the-foreign-minister-urmas-paet?id=51085399 (visité le 23/07/2020) ;
75. PICTET (Jean), Commentary on the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, ICRC, Geneva, 1952, 477 p. ;
76. Principes fondamentaux et directives concernant le droit à un recours et à réparation des victimes de violations flagrantes du droit international des droits de l'homme et de violations graves du droit international humanitaire, 60/147 Résolution adoptée par l'Assemblée générale le 16 décembre 2005, URL : https://www.ohchr.org/fr/professionalinterest/pages/remedyandreparation.aspx (visité le 18/06/2020) ;
77. Radware, Global Application & Network Security Report 2019-2020, 2020, 40 p., URL : https://www.radware.com/ert-report-2020/ (visité le 06/04/2020) ;
78. Réponse de la France à la résolution 73/27 relative aux « Progrès de l'informatique et des télécommunications et sécurité internationale » et à la résolution 73/266 relative à « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité

internationale », 2019, 14 p., URL : https://www.un.org/disarmament/wp-content/uploads/2019/09/France-2019.pdf (visité le 12/05/2020) ;

79. Report of the Secretary-General, «In larger freedom: towards development, security and human rights for all», le 21 mars 2005, 72 p., URL : https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=4abcac0e2 (visité le 03/06/2019) ;
80. Republic of Estonia, Information System Authority, Cyber Security in Estonia 2020, 52 p., URL : https://www.ria.ee/sites/default/files/cyber_aastaraamat_eng_web_2020.pdf (visité le 21/07/2020) ;
81. SCHJOLBERG (Stein), A paper for the EastWest Institute (EWI), Cybercrime Legal Working Group, Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes, An International Criminal Tribunal for Cyberspace (ICTC), Prosecution for the Tribunal, Police investigation for the Tribunal, mars 2012, 41 p., URL : https://www.cybercrimelaw.net/documents/ICTC.pdf (visité le 26/07/2020) ;
82. Security Council, Identical letters dated 21 February 2020 from the Permanent Representative of Georgia to the United Nations addressed to the Secretary-General and the President of the Security Council, le 24 février 2020, URL : https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2020_135.pdf (visité le 23/06/2020) ;
83. Security Council, Repertoire of the Practice of the Security Council, Actions with respect to threats to the peace, breaches of the peace, and acts of aggression (Chapter VII of the Charter), Advance version, 21st Supplement, 2018, 123 p., URL : https://www.un.org/securitycouncil/sites/www.un.org.securitycouncil/files/scpcrb.repertoire.part_vii.21st_supplement_2018_for_webposting.pdf#page=8 (visité le 23/06/2020) ;
84. Security Council, Report of the Panel of Experts established pursuant to resolution 1874 (2009), le 30 août 2019, 142 p., URL : https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf (visité le 27/06/2020) ;
85. SEGAL (Adam), «Cyberspace Governance: The Next Step» (Policy innovation memorandum no. 2), Council on foreign relations, International Institutions and Global Governance Program, le 14 novembre 2011, 4 p., URL : https://cdn.cfr.org/sites/default/files/pdf/2011/03/Policy_Innovation_Memo2_Segal.pdf (visité le 29/03/2020) ;
86. Senator the Hon George Brandis QC Attorney-General of Australia, «The right of self-defence against imminent armed attack in international law», Lecture delivered at the T C Beirne School of Law The University of Queensland, 11 April 2017, 13 p., URL :

https://law.uq.edu.au/files/25365/2017%2004%2011%20-%20Attorney-General%20-%20Speech%20-%20The%20Right%20of%20Self-Defence%20Against%20Imminent%20Armed%20Attack%20in%20International%20Law%20-%20for%20publication.pdf (visité le 10/06/2020) ;

87. SGDSN, *Revue stratégique de cyberdéfense*, le 12 février 2018, 167 p., URL : http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf (visité le 03/06/2020) ;
88. Statement of the Ministry of Foreign Affairs of Georgia, le 20 mars 2020, URL : https://mfa.gov.ge/cmsctx/culture/en-US/-/News/Statement-of-the-Ministry-of-Foreign-Affairs-o-(7).aspx?CatID=5 (visité le 23/06/2020) ;
89. Statut actualisé du Tribunal pénal international pour l'ex-Yougoslavie, septembre 2009 ;
90. Statut actualisé du Tribunal pénal international pour le Rwanda, décembre 2009 ;
91. Statut du Tribunal spécial pour la Sierra Leone, janvier 2002 ;
92. Testimony of Richard Clarke, Special Advisor to the President for Cyberspace Security, Senate Judiciary Committee, Administrative Oversight and the Courts Subcommittee, hearing titled « Administrative Oversight: Are We Ready For A Cyber Terror Attack? », le 13 février 2002, URL : http://www.techlawjournal.com/security/20020213.asp (visité le 23/07/2020) ;
93. The Secretary-General's High-level Panel Report on Threats, Challenges and Change, «A more secure world: our shared responsibility», le 2 décembre 2004, 99 p., URL : https://www.un.org/ruleoflaw/files/gaA.59.565_En.pdf (visité le 03/03/2019) ;
94. The United States Department of Defense, Quadrennial Defense Review Report, 128 p., 2010, URL : https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf (visité le 13/05/2020) ;
95. The White House, FACT SHEET: U.S. and NATO Efforts in Support of NATO Partners, including Georgia, Ukraine, and Moldova, le 9 juillet 2016, URL : https://obamawhitehouse.archives.gov/the-press-office/2016/07/09/fact-sheet-us-and-nato-efforts-support-nato-partners-including-georgia (visité le 15/06/2020) ;
96. UNAL (Beyza), LEWIS (Patricia), International Security Department, « Cybersecurity of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences », Research Paper, janvier 2018, 26 p., URL : https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf (visité le 23/01/2020) ;
97. UNIDIR, « The United Nations, Cyberspace and International Peace and Security », Responding to Complexity in the 21st Century, 2017, 82 p., URL :

http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf (visité le 21/06/2020) ;

98. Union européenne, Directive 2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, URL : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148 (visité le 15/06/2020) ;
99. United Nations Security Council, Attack on Iraq – SecCo debate – Verbatim record, 2288th meeting, New York, le 19 juin 1981, URL : https://www.un.org/unispal/document/auto-insert-177361/ (visité le 15/06/2020) ;
100. United States Mission to the United Nations, Joint Statement by Estonia, the United Kingdom, and the United States at a Press Availability on Russian Cyberattacks in Georgia, le 5 mars 2020, URL : https://usun.usmission.gov/joint-statement-by-estonia-the-united-kingdom-and-the-united-states-at-a-press-availability-on-russian-cyberattacks-in-georgia/ (visité le 23/06/2020) ;
101. Verint, Thales, *The Cyberthreat Handbook*, octobre 2019, 232 p., URL : https://thalesgroup-myfeed.com/THECYBERTHREATHANDBOOK (visité le 24/03/2020) ;
102. White House, Cyber space policy review : Assuring a Trusted and Resilient Information and Communications Infrastructure, 76 p., URL : https://fas.org/irp/eprint/cyber-review.pdf (visité le 04/04/2020) ;
103. White House, International Strategy For Cyberspace, Prosperity, Security, and Openness in a Networked World, mai 2011, 30 p., URL : https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (visité le 12/06/2020) ;
104. White House, Statement from the Press Secretary, le 15 février 2018, URL : https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ (visité le 12/04/2020) ;
105. White House, The national strategy to secure cyberspace, février 2003, 76 p., URL : https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf (visité le 18/03/2020) ;

III. ARTICLES

1. ABI-SAAB (Rosemary), « Les "Principes généraux" du droit humanitaire selon la Cour internationale de justice », *Revue Internationale de la Croix-Rouge*, 1987, pp. 381-389, URL :

https://international-review.icrc.org/sites/default/files/S0035336100091449a.pdf (visité le 15/05/2020) ;

2. BACHMANN (Julien), OBERLI (Nicolas), « Le framework Metasploit », *MISC*, No. 52, novembre 2010, URL : https://connect.ed-diamond.com/MISC/MISC-052/Le-framework-metasploit (visité le 13/02/2020) ;
3. BARADARAN (Nazanin), HABIBI (Homayoun), «Cyber Warfare and Self - Defense from the Perspective of International Law», *Journal of Politics and Law*, Vol. 10, No. 4, 2017, 15 p., URL : https://www.researchgate.net/publication/319399422_Cyber_Warfare_and_Self_-_Defense_from_the_Perspective_of_International_Law (visité le 20/06/2020) ;
4. BARAT-GINIES (Oriane), « Existe-t-il un droit international du cyberespace ? », *Hérodote*, janvier 2014, 21 p., URL : https://www.cairn.info/revue-herodote-2014-1-page-201.htm (visité le 23/09/2019) ;
5. BARAT-GINIES (Oriane), FERRO (Coline), « Le cyberespace : un nouveau champ de conflictualité », *Revue géostratégique*, No. 38, le 17 avril 2016, URL : http://www.academiedegeopolitiquedeparis.com/le-cyberespace-un-nouveau-champ-de-conflictualite/ (visité le 23/09/2019) ;
6. BETHLEHEM (Daniel), «Self-Defense Against an Imminent or Actual Armed Attack By Non-State Actors», *The American Journal of International Law*, Vol. 106, No. 4, octobre 2012, 10 p., URL : https://www.cambridge.org/core/journals/american-journal-of-international-law/article/selfdefense-against-an-imminent-or-actual-armed-attack-by-nonstate-actors/BC9C62E3157202F50234A452A714A421 (visité le 13/06/2020) ;
7. BROWN (Davis), « A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict», *Harvard International Law Journal*, Vol. 47, No. 1, 2006, 43 p., URL : https://heinonline.org/HOL/LandingPage?handle=hein.journals/hilj47&div=8&id=&page= (visité le 21/07/2020) ;
8. *Business Insider*, « The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought », le 20 novembre 2013, URL : https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11 (visité le 22/07/2020) ;
9. Center for Security Studies, « Hotspot Analysis: Stuxnet », Cyber Defense Project, Zürich, octobre 2017, 17 p., URL : https://www.researchgate.net/publication/323199431_Stuxnet (visité le 09/02/2020) ;

10. Center for Strategic and International Studies, Significant Cyber Incidents, décembre 2019, URL : https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (visité le 23/01/2020) ;
11. CHALVIN (Antoine), « L'ombre du soldat de bronze », *Le Courrier des pays de l'Est*, 2007/4 (No. 1062), 12 p., URL : https://www.cairn.info/revue-le-courrier-des-pays-de-l-est-2007-4-page-6.htm (visité le 8/07/2020) ;
12. CHAN-TUNG (Ludovic), « Le droit international à l'épreuve de la cyberguerre - le cas de Stuxnet », Université Grenoble, janvier 2018, 27 p., URL : https://www.researchgate.net/publication/323855978_Le_droit_international_a_l'epreuve_de_la_cyberguerre_-_le_cas_de_Stuxnet (visité 22/01/2020) ;
13. CHAUMETTE (Anne-Laure), «International Criminal Responsibility of Individuals in Case of Cyberattacks», *International Criminal Law Review*, Brill Academic Publishers, 2018, 35 p., URL : https://brill.com/view/journals/icla/18/1/article-p1_1.xml (visité le 20/07/2020) ;
14. CICR, « Guerre informatique », le 1er septembre 2011, URL : https://www.icrc.org/fr/doc/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.htm (visité le 24/01/2020) ;
15. CICR, « Le droit international humanitaire et les cyberopérations pendant les conflits armés », novembre 2019, 11 p., URL : https://www.icrc.org/fr/document/le-droit-international-humanitaire-et-les-cyberoperations-pendant-les-conflits-armes (visité le 12/05/2020) ;
16. CICR, « Les cyberopérations en période de conflit armé : 7 questions juridiques et politiques essentielles », le 3 avril 2020, URL : https://www.icrc.org/fr/document/les-cyberoperations-en-periode-de-conflit-arme-7-questions-juridiques-et-politiques (visité le 09/05/2020) ;
17. CICR, « Pas de vide juridique dans le cyberspace », le 16 août 2011, URL : https://www.icrc.org/fr/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm (visité le 15/02/2020) ;
18. CICR, « Quelles limites le droit de la guerre impose-t-il aux cyberattaques ? », le 28 juin 2013, URL : https://www.icrc.org/fr/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm (visité le 24/01/2019) ;
19. CONDRON (Sean), «Getting It Right: Protecting American Critical Infrastructure in Cyberspace», *Harvard Journal of Law and Technology*, Vol. 20, No 2, 20 p., URL : http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech403.pdf (visité le 13/06/2020) ;
20. DAHAN (Michael), «Hacking for the homeland: Patriotic hackers versus hacktivists», in: HART (Doug), ICIW 2013 8th International Conference on Information Warfare and Security, Denver, Colorado, USA, 2013, 292 p. ;

21. DE FROUVILLE (Olivier), MARTELLY (Olivia), « La juridictionnalisation du droit des conflits armés : Les tribunaux internationaux mixtes », Permanence et mutations du droit des conflits armés, Colloque, Université Lyon 3, 2-3 octobre 2008, 26 p., URL : http://www.frouville.org/Publications_files/Art-Lyon-mainDocFINAL-1.pdf (visité le 05/03/2020) ;
22. DEIBERT (Ronald), ROHOZINSKI (Rafal), CRETE-NISHIHATA (Masashi), « Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war », *Security Dialogue*, Vol 43 (I), février 2012, 22 p., URL : https://www.researchgate.net/publication/258186818_Cyclones_in_Cyberspace_Information_Shaping_and_Denial_in_the_2008_Russia-Georgia_War (visité le 17/01/2020) ;
23. Département fédéral de la défense, de la protection de la population et des sports, Le portail du Gouvernement Suisse, « Protection de récepteurs GPS contre des cyberattaques », le 23 février 2018, URL : https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-69896.html (visité le 09/02/2020) ;
24. DINSTEIN (Yoram), « Computer Network Attacks and Self Defense », Naval War College, *International Law Studies*, Computer Network Attack and International Law, Vol. 76, 2002, 21 p., URL : https://digital-commons.usnwc.edu/ils/vol76/iss1/20/ (visité le 23/07/2020) ;
25. DINSTEIN (Yoram), «Computer Network Attacks and Self-Defense», in: SCHMITT (Michael), O'DONNELL (Brian), Computer network attack and international law, Symposium on Computer Network Attack and International Law, *International Law Studies*, Vol. 76, Naval War College, 21 p., URL : https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1397&context=ils (visité le 10/05/2020) ;
26. DURAND (Corentin), « Attribution des cyberattaques : le jeu toujours plus compliqué de la dissuasion », *Numerama*, le 23 novembre 2018, URL : https://cyberguerre.numerama.com/64-attribution-des-cyberattaques-le-jeu-toujours-plus-complique-de-la-dissuasion.html (visité le 25/07/2020) ;
27. *Financial Times*, « Cyber crime: states use hackers to do digital dirty work », le 4 septembre 2015, URL : https://www.ft.com/content/78c46db4-52da-11e5-b029-b9d50a74fd14 (visité le 25/07/2020) ;
28. *Forbes*, « Critical Windows Warning Gets Real As Wormable Exploit Weaponized », le 7 septembre 2019, URL : https://www.washingtontimes.com/news/2018/oct/10/government-hackers-using-publicly-available-tools-/ (visité le 13/02/2020) ;

29. GEISS (Robin), LAHMANN (Henning), «Cyber warfare: applying the principle of distinction in an interconnected space», *Israel Law Review*, Vol. 45 (3), 2012, 20 p., URL : https://eprints.gla.ac.uk/78067/1/78067.pdf (visité le 12/02/2020) ;
30. GERVAIS (Michael), « Cyber Attacks and the Laws of War », *Berkeley Journal of International Law*, 2012, 55 p., URL : https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1422&context=bjil (visité le 22/01/2020) ;
31. GREENWOOD (Christopher), «Scope of Application of Humanitarian Law», in: FLECK (Dieter), The Handbook of International Humanitarian Law, Oxford, 2008, 34 p. ;
32. GUTERRES (António), « La multiplication des conflits a aggravé l'insécurité mondiale », le 16 février 2018, URL : https://news.un.org/fr/story/2018/02/1005952 (visité le 29/09/2019) ;
33. HAYWARD (Ryan), «Evaluating the "imminence" of a cyber attack for purposes of anticipatory self-defense», *Columbia Law Review*, Vol. 117, No. 2, 36 p., URL : https://columbialawreview.org/wp-content/uploads/2017/03/399_low.pdf (visité le 12/06/2020);
34. HECKER (Marc), TENENBAUM (Élie), « Quel avenir pour le djihadisme ? Al-Qaïda et. Daech après le califat », *Focus stratégique*, No. 87, Ifri, janvier 2019, 51 p., URL : https://www.ifri.org/sites/default/files/atoms/files/fs87_hecker_tenenbaum.pdf (visité le 18/03/2020) ;
35. HRNJAZ (Miloš), The War Report « The United States of America and the Islamic Republic of Iran: An international armed conflict of low intensity », Académie de droit international humanitaire et de droits humains à Genève, décembre 2019, 8 p., URL : https://www.geneva-academy.ch/joomlatools-files/docman-files/The%20United%20States%20Of%20America%20And%20Islamic%20Republic%20Of%20Iran%20An%20International%20Armed%20Conflict%20Of%20Low%20Intensity.pdf (visité le 17/12/2019) ;
36. ICRC, « Cyberwarfare and international humanitarian law: the ICRC's position », 4 p., URL : https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf (visité le 07/02/2020) ;
37. JENSEN (Eric Talbot), « Cyber Warfare and Precautions Against the Effects of Attacks », *Texas Law Review*, Vol. 88, 2010, 37 p., URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1661218 (visité le 13/02/2020).
38. Kaspersky, « Top 5 most notorious cyberattacks », novembre 2018, URL : https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/ (visité le 09/04/2020) ;

39. KLEFFNER (Jann), HARRISON DINNISS (Heather), «Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations», Naval War College, *International Law Studies*, Vol. 89, 2013, 25 p., URL : https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1039&context=ils (visité le 27/06/2020) ;
40. KOZLOWSKI (Andrzej), «Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan», International Scientific Forum, 12-14 December 2013, Tirana, Albania Proceedings, Vol.3, 10 p., URL : https://www.researchgate.net/profile/Nnedinma_Umeokafor/publication/260107032_International_Scientific_Forum_ISF_2013vol3/links/02e7e52f964505c201000000.pdf#page=246 (visité le 17/01/2020) ;
41. *L'OBS*, « Stuxnet : comment les Etats-Unis et Israël ont piraté le nucléaire iranien », le 4 juin 2012, URL : https://www.nouvelobs.com/rue89/rue89-internet/20120604.RUE0433/stuxnet-comment-les-etats-unis-et-israel-ont-pirate-le-nucleaire-iranien.html (visité le 02/08/2020) ;
42. *Le Figaro*, « Le G7 va mener une simulation de cyberattaque dans la finance », le 10 mai 2019, URL : https://www.lefigaro.fr/flash-eco/le-g7-va-mener-une-simulation-de-cyberattaque-dans-la-finance-20190510 (visité le 23/05/2020) ;
43. *Le Figaro*, « Une cyberattaque coupe l'électricité », le 5 janvier 2016, URL : https://www.lefigaro.fr/flash-actu/2016/01/05/97001-20160105FILWWW00381-ukraine-une-cyberattaque-coupe-l-electricite.php (visité le 02/12/2019) ;
44. *Le Monde*, « Israël dit avoir déjoué une cyberattaque du Hamas à Gaza, avant de frapper le site d'origine », le 6 mai 2019, URL : https://www.lemonde.fr/pixels/article/2019/05/06/israel-dit-avoir-replique-a-une-attaque-informatique-par-une-frappe-aerienne-une-premiere_5459063_4408996.html (visité le 10/11/2019) ;
45. *Le Point*, « La France tente de relancer les négociations internationales sur le cyberspace », le 12 novembre 2018, URL : https://www.lepoint.fr/economie/la-france-tente-de-relancer-les-negociations-internationales-sur-le-cyberespace-12-11-2018-2270549_28.php (visité le 07/11/2019) ;
46. *Lenta*, « "Идущие вместе" наступили на грабли », 24 février 2005, URL : https://lenta.ru/articles/2005/02/23/young/ (visité le 03/04/2020) ;
47. LIN (Herbert), « Cyber conflict and international humanitarian law », *International Review of Red Cross*, Vol. 94, No. 886, 2012, 17 p., URL : https://e-brief.icrc.org/wp-content/uploads/2016/09/29.-Cyber-conflict-and-international-humanitarian-law.pdf (visité le 26/10/2019) ;

48. LOBEL (Hannah), «Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict», *Texas International Law Journal*, Vol. 47, Issue 3, 24 p., URL : https://heinonline.org/HOL/LandingPage?handle=hein.journals/tilj47&div=28&id=&page= (visité le 04/04/2020) ;
49. MACAK (Kubo), RODENHÄUSER (Tilman), GISEL (Laurent), « Cyber attacks against hospitals and the COVID-19 pandemic: How strong are international law protections? », le 2 avril 2020, URL : https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/ (visité le 15/05/2020) ;
50. *Mediapart*, « Une cyberguerre dans le conflit russo-géorgien ? », le 29 août 2008, URL : https://blogs.mediapart.fr/edition/les-invites-de-mediapart/article/290808/une-cyberguerre-dans-le-conflit-russo-georgien (visité le 19/01/2020) ;
51. MELZER Nils, «Cyber operations and jus in bello», pp. 3-17, in: UNIDIR, «Confronting cyberconflict», Disarmament Forum, 2011, URL : https://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf (visité le 11/05/2020) ;
52. MOORE (David), PAXSON (Vern), SAVAGE (Stefan), SHANNON (Colleen), STANIFORD (Stuart), WEAVER (Nicholas), « Inside the slammer worm », *IEEE Security & Privacy Magazine*, No. 1(4), 2003, 7 p., URL : https://www.researchgate.net/publication/3437498_Inside_the_Slammer_worm (visité le 13/02/2020) ;
53. NICHOLSON (Andrew), « A Taxonomy of Technical Attribution Techniques for Cyber Attacks », Proceedings of the 11th European Conference on Information Warfare and Security, janvier 2012, 10 p. ;
54. O'CONNELL (Mary Ellen), « Cyber Security without Cyber War », *Journal of Conflict & Security Law*, 2012, 23 p., URL : https://www.law.upenn.edu/live/files/3474-oconnell-m-cyber-security-without-cyber-war-2012 (visité le 22/07/2020) ;
55. ONU, « L'ONU précise que la cyberattaque dont elle a été victime n'a pas compromis de données sensibles », le 31 janvier 2020, URL : https://news.un.org/fr/story/2020/01/1060882 (visité le 25/06/2020) ;
56. PICTET (Jean), «The principles of international humanitarian law», *International Review of the Red Cross*, Vol. 6, Issue 66, septembre 1966, pp. 455-469, URL : https://www.loc.gov/law/mlr/pdf/RC_Sep-1966.pdf (visité le 17/05/2020) ;
57. Radware, « A Higher Percentage of Companies Say They've Been Targeted By Nation-State Hackers, Radware Survey Finds », le 14 janvier 2020, URL :

https://www.radware.com/newsevents/pressreleases/2020/global-application-network-security-report (visité le 06/04/2020) ;

58. RASCAGNERES (Paul), « Who Wasn't Responsible for Olympic Destroyer? », le 26 février 2018, URL : https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html (visité le 23/07/2020) ;
59. RAYMOND (David), CONTI (Gregory), CROSS (Tom), FANELLI Robert, «A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons», 5th International Conference on Cyber Conflict, 2013, 16 p., URL : https://ccdcoe.org/uploads/2018/10/8_d1r2s6_raymond.pdf (visité le 15/05/2020) ;
60. *Reuters*, « Kremlin loyalist says launched Estonia cyber-attack », le 11 mars 2019, https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313 (visité le 28/03/2020) ;
61. *Reuters*, « UN offices in Geneva, Vienna targeted by 'well-resourced' cyber attack last year », le 29 janvier 2020, URL : https://fr.reuters.com/article/rbssTechMediaTelecomNews/idUKL1N29Y1BV (visité le 27/06/2020) ;
62. RICHMOND (Jeremy), « Evolving Battlefields : Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict ? », *Fordham International Law Journal*, Vol. 35, Issue 3, 2012, p. 844, URL : https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2433&context=ilj (visité le 14/09/2019) ;
63. ROBERTSON (Horace), «Self-Defense against Computer Network Attack under International Law», Symposium on Computer Network Attack and International Law, *International Law Studies*, Vol. 76, Naval War College, 25 p., URL : https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1396&context=ils (visité le 12/06/2020) ;
64. ROSCINI (Marco), «Cyber Operations as a Use of Force», Research Paper No. 16-05, University of Westminster School of Law, le 31 mars 2014, 39 p., URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2631078 (visité le 10/05/2020) ;
65. ROWE (Neil), « The Attribution of Cyber Warfare », in: GREEN (James), *Cyber Warfare: A Multidisciplinary Analysis*, 2016, 12 p., URL : http://opac.lib.idu.ac.id/unhan-ebook/assets/uploads/files/4cc80-045.cyber-warfare.pdf (visité le 25/07/2020) ;
66. SASSOLI (Marco), «Le droit international humanitaire mis à mal en Syrie», *Plaidoyer*, No. 2, 2017, 7 p., URL : https://archive-ouverte.unige.ch/unige:93489 (visité le 02/04/2020) ;

67. SCHMITT (Michael), « Wired warfare: Computer network attack and jus in bello », CICR, 2002, 36 p., URL : https://www.icrc.org/en/doc/assets/files/other/365_400_schmitt.pdf (visité le 10/05/2020) ;
68. SCHMITT (Michael), «Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework», *Columbia Journal of Transnational Law*, Vol. 37, 1998-1999, 54 p., URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1603800 (visité le 13/06/2020) ;
69. SCHMITT (Michael), «Computer Network Attack: The Normative Software», 32 p., in FISCHER (Horst), Yearbook of International Humanitarian Law, Cambridge University Press, Vol. 4, 2001, 850 p. ;
70. SCHULLER (Alan), «Inimical Inceptions of Imminence: A New Approach to Anticipatory Self-Defense Under the Law of Armed Conflict», *UCLA Journal of International Law and Foreign Affairs*, Vol. 18, No. 2, 2014, 46 p., URL : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2701499 (visité le 14/06/2020) ;
71. SHUKLA (Shantanu), SINHA (Sonal), « Use of Honeypot and IP Tracing Mechanism for Prevention of DDOS Attack », *International Journal of Scientific Engineering and Research*, 2015, 5 p., URL : http://docplayer.net/8988379-Use-of-honeypot-and-ip-tracing-mechanism-for-prevention-of-ddos-attack.html (visité le 26/07/2020) ;
72. STEYL (Matthew), Cybersecurity and Rising China: Analysis of Policy Proposals, Curriculum in Global Studies, University of North Carolina at Chapel Hill, 2014, 78 p., URL : https://cdr.lib.unc.edu/concern/honors_theses/vt150p11z (visité le 04/04/2020) ;
73. TENALI (Naga Mani), JYOSYULA (Bala Savitha), « IP Traceback Scenarios », *Global Journal of Computer Science and Technology Network, Web & Security*, Vol. 13, 2013, 9 p., URL : https://computerresearch.org/index.php/computer/article/download/373/373/ (visité le 11/07/2020) ;
74. *The Hacker News*, « Philippines-Malaysia Cyber war over Sabah land dispute », le 4 mars 2013, URL : https://thehackernews.com/2013/03/philippines-malaysia-cyber-war-over.html (visité le 03/04/2020) ;
75. *The Huffington Post*, « Pourquoi l'appli Telegram, utilisée par Adel Kermiche pour annoncer son attentat, échappe toujours à la surveillance », le 28 juillet 2016, URL : https://www.huffingtonpost.fr/2016/07/28/telegram-messagerie-adel-kermiche-eglise-attentat-saint-etienne-du-rouvray_n_11239130.html (visité le 24/03/2020) ;

76. *The New York Times*, « A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try », le 15 mars 2018, URL : https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html (visité le 02/12/2019) ;
77. *The New York Times*, « U.S. Carried Out Cyberattacks on Iran », le 22 juin 2019, URL : https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html (visité le 19/12/2019) ;
78. *The New York Times*, « Estonia says cyber-assault may involve the Kremlin », le 17 mai 2005, URL : https://www.nytimes.com/2007/05/17/world/europe/17iht-estonia.4.5758556.html?smid=pl-share (visité le 23/07/2020) ;
79. *The Telegraph*, « NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history », 20 mai 2017, URL : https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/ (visité le 23/01/2020) ;
80. *The Washington Post*, « Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists », le 3 avril 2019, URL : https://www.washingtonpost.com/gdpr-consent/?destination=%2ftechnology%2f2019%2f04%2f03%2fhospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists%2f%3futm_term%3d.de95da701f32&utm_term=.de95da701f32 (visité le 02/12/2019) ;
81. Université de Twente, « New method for monitoring internet traffic to detect cyber attacks », le 29 juin 2016, URL : https://phys.org/news/2016-06-method-internet-traffic-cyber.html (visité le 10/07/2020) ;
82. WALDRON (Jeremy), «Vagueness in Law and Language: Some Philosophical Issues», *California Law Review*, Vol. 82, No. 3, mai 1994, 32 p., URL : https://www.jstor.org/stable/3480971?seq=1 (visité le 14/07/2020) ;
83. WAXMAN (Matthew), « Cyber-Attacks and the Use of Force : Back to the Future of Article 2(4) », *Yale Journal of International Law*, 2011, 40 p., URL : https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1403&context=yjil (visité le 22/07/2020) ;
84. WĘGLIŃSKI (Konrad), «Cyberwarfare and responsibility of states», *Torun International Studies*, No. 1 (9), février 2017, 8 p., URL : https://www.researchgate.net/publication/316838873_CYBERWARFARE_AND_RESPONSIBILITY_OF_STATES (visité le 01/04/2020) ;
85. WHEELER (David), LARSEN (Gregory), LEADER (Task), « Techniques for Cyber Attack Attribution », Institute for Defense Analysis, octobre 2003, 85 p., URL :

https://www.researchgate.net/publication/235170094_Techniques_for_Cyber_Attack_Attribution (visité le 24/07/2020) ;

86. *Wired*, «An Unprecedented Look at Stuxnet, the World's First Digital Weapon», https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (visité le 10/06/2020) ;
87. *ZDNet*, « Hide My Ass throws light on 'LulzSec' logs », le 27 septembre 2011, URL : https://www.zdnet.com/article/hide-my-ass-throws-light-on-lulzsec-logs/ (visité le 26/07/2020) ;

IV. TRAITÉS INTERNATIONAUX

1. Convention (II) de la Haye concernant les lois et coutumes de la guerre sur terre, La Haye ; entrée en vigueur le 4 septembre 1900 ;
2. Convention (IV) de la Haye concernant les lois et coutumes de la guerre sur terre et son Annexe : Règlement concernant les lois et coutumes de la guerre sur terre ; entrée en vigueur le 26 janvier 1910 ;
3. Convention de Genève pour l'amélioration du sort des blessés, des malades et des naufragés des forces armées sur mer ; entrée en vigueur le 21 octobre 1950 ;
4. Convention pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne (Première Convention de Genève) du 12 août 1949 ; entrée en vigueur le 21 octobre 1950 ;
5. Convention relative à la protection des personnes civiles en temps de guerre (Quatrième Convention de Genève) ; entrée en vigueur le 21 octobre 1950 ;
6. Convention relative au traitement des prisonniers de guerre (Troisième Convention de Genève) du 12 août 1949 ; entrée en vigueur le 21 octobre 1950 ;
7. Déclaration à l'emploi, en temps de guerre, des explosifs sous Projectiles 400 Grammes Poids ; entrée en vigueur le 11 décembre 1868 ;
8. Statut la Cour Internationale de Justice ; entrée en vigueur le 24 octobre 1945 ;
9. Traité de Versailles de 1919, Pacte de la Société des Nations du 28 juin 1919 ; entrée en vigueur le 10 janvier 1920 ;
10. Traité sur l'Union Europeenne modifié jusqu'au traité de Lisbonne de 2009; entrée en vigueur le 1er décembre 2009 ;
11. Convention pour la prévention et la répression du crime de génocide du le 9 décembre 1948 ; entrée en vigueur le 12 janvier 1951 ;
12. Convention de Budapest sur la cybercriminalité du 23 novembre 2001 ; entrée en vigueur le 1er janvier 2007 ;

13. Accords de Locarno, 1925 ; entrée en vigueur le 10 septembre 1926 ;
14. Charte des Nations Unies, San Francisco, 26 juin 1945 ; entrée en vigueur le 24 octobre 1945 ;
15. Traité de l'Atlantique Nord du 4 avril 1949 ; entrée en vigueur le 24 août 1949 ;
16. Statut de Rome du 17 juillet 1998 ; entrée en vigueur le 1er juillet 2002 ;

V. JURISPRUDENCE CITÉE

a) Nationale

États-Unis:

Circuit Court of Illinois :

1. Circuit Court of Illinois, *Mondelez International v. Zurich American Insurance Company*, le 10 octobre 2018

Cour de district des États-Unis :

1. U.S. District Court, Western District of Pennsylvannia, *Unites States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui*, Grand Jury, Indictment, 1 May 2014

Congrès des États-Unis :

1. Cybersecurity Enhancement Act of 2014 (S.1353) proposé par sénateurs Rockefeller et Thune

France :

Sénat :

1. Loi no. 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense

b) Régionale

Union européenne

Conseil de l'Union européenne :

1. Directive 2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

c) Internationale

Cour Internationale de Justice :

1. CIJ, *Affaire relative au projet Gabcikovo-Nagymaros (Hongrie/Slovaquie)*, Arrêt, le 25 septembre 1997 ;
2. CIJ, *Bosnie-Herzégovine c. Serbie-et-Monténégro*, Application de la convention pour la prévention et la répression du crime de génocide, le 26 février 2007 ;
3. CIJ, Licéité de la menace ou de l'emploi d'armes nucléaires, Avis consultatif, le 8 juillet 1996 ;
4. CIJ, *Nicaragua c. États-Unis*, Arrêt, le 27 juin 1986 ;
5. CIJ, *République démocratique du Congo c. Ouganda*, Jugement, le 19 décembre 2005 ;
6. CIJ, *République islamique d'Iran c. États-Unis d'Amérique*, Jugement, le 6 novembre 2003 ;
7. CIJ, *République islamique d'Iran c. États-Unis d'Amérique*, le 6 novembre 2003, Opinion individuelle de M. Simma

Cour pénale internationale :

1. CPI, *Le Procureur c. Bosco Ntaganda*, Chambre de première instance VI, Jugement, le 8 juillet 2019

Cour permanente de Justice internationale :

1. CPJI, *Italie c. France*, Affaire des Phosphates du Maroc (exceptions préliminaires), Arrêt,le 14 juin 1938

Tribunal militaire international pour l'Extrême-Orient :

1. TMIEO, In re Hirota et autres, 1948

Tribunal pénal international pour le Rwanda :

1. TPIR, *Le Procureur c. Clement Kayishema et Obed Ruzindana*, Chambre de première instance II, Jugement, 21 mai 1999

Tribunal pénal international pour l'ex-Yougoslavie :

1. TPIY, *Le Procureur c. Dario Kordić et Mario Čerkez*, Chambre d'appel, Arrêt, le 17 décembre 2004 ;
2. TPIY, *Le Procureur c. Dragoljub Kunarac, Radomir Kovač et Zoran Vuković*, Chambre de Première instance, Jugement, le 22 février 2001 ;
3. TPIY, *Le Procureur c. Dragoljub Kunarac, Radomir Kovač et Zoran Vuković*, Chambre d'Appel, Arrêt, le 12 juin 2002 ;

4. TPIY, *Le Procureur c. Duško Tadić*, Chambre d'Appel, Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, le 2 octobre 1995 ;
5. TPIY, *Le Procureur c. Duško Tadić*, Chambre d'Appel, Arrêt, le 15 juillet 1999 ;
6. TPIY, *Le Procureur c. Radislav Krstić*, Chambre de Première instance, Jugement, le 2 août 2001 ;
7. TPIY, *Le Procureur c. Radovan Karadžić et Ratko Mladić*, Chambre de Première instance, Examen des actes d'accusation dans le cadre de l'article 61 du Règlement de procédure et de preuve, le 11 juillet 1996 ;
8. TPIY, *Le Procureur c. Sefer Halilović*, Chambre de première instance I, Jugement, le 16 novembre 2005 ;
9. TPIY, *Le Procureur c. Stanislav Galić*, Chambre de Première Instance I, Jugement et opinion, le 5 décembre 2003 ;
10. TPIY, *Le Procureur c. Tihomir Blaškić*, Chambre de Première Instance I, Jugement, le 3 mars 2000 ;
11. TPIY, *Le Procureur c. Tihomir Blaškić*, Chambre d'appel, Arrêt, le 29 juillet 2004 ;
12. TPIY, *Le Procureur c. Zejnil Delalić, Zdravko Mucić, Hazim Delić et Esad Landžo*, Chambre de Première instance, Jugement, le 16 novembre 1998 ;
13. TPIY, *Le Procureur c. Zejnil Delalić, Zdravko Mucić, Hazim Delić et Esad Landžo*, Chambre d'Appel, Arrêt, le 20 février 2001