101th REGULAR SESSION
August 1 to 10, 2022
Rio de Janeiro, Brazil

OEA/Ser. Q
CJI/doc. 671/22 rev.2 corr.1
October 21 2022
Original: Spanish

REPORT OF THE INTER-AMERICAN JURIDICAL COMMITTEE.

SECOND REPORT: INTERNATIONAL LAW APPLICABLE TO CYBERSPACE

1. INTRODUCTION

This report was originally elaborated by Dr. Mariana Salazar Albornoz, in her capacity as rapporteur. It is her second report on the subject; a document that was approved by consensus by all members of the Committee in its last review before the plenary. The report begins by describing the concepts of cyberspace and cyber operations, before delving into an analysis of the implications that such operations could have for international law based on examples of state cyber operations that have occurred over the past two decades. The report then examines the main intergovernmental and academic negotiation processes that have existed and continue to exist to help determine the scope of applicability of existing international law to cyberspace, including, of course, the work of the Inter-American Juridical Committee. Finally, it offers an overview of the main specific international law issues being discussed in relation to their application to cyberspace and clarifies as far as possible the official positions adopted by the few States of the Americas that have put forward opinions on the matter to date. We hope that the report will serve as a useful tool for the many States of the Americas region that are in the process of preparing their official national positions on this important issue of the scope of application of international law to cyberspace.

2. CYBERSPACE AND CYBEROPERATIONS

The term "cyberspace" comes from the Greek *kybernetes,* which means 'the art of steering a ship' and alludes to cybernetics, the study of remote control through devices. The term was first used in 1960 in the title *Atelier Cyberspace,* used by artist Susanne Ussing and architect Carten Hoff to refer to their work of sensory installations and images. The first association of the term with the digital sphere, albeit for novelistic purposes, was in the 1980s, when the Canadian American science fiction writer William Gibson used it in his short story *Burning Chrome* and his novel *Neuromancer*. In the latter, he described it as:

> *"A consensual hallucination experienced daily by billions of legitimate operators, in all nations ... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data."*[1]

The word was taken up again with the rise of the Internet in the 1990s. The purpose of referring to "cyberspace" initially came with the concept that the Internet was a space or domain distinct from the "real world," and therefore should be a separate jurisdiction, exempt from the imposition of the might of states and their laws, and governed by the will of its users.[2] The idea generated a twofold debate: on

[1] Gibson, William. 1997. *Neuromancer*. New York, NY: Penguin Putnam.
[2] See, for example, BARLOW, J.P., *A Declaration of the Independence of Cyberspace,* proclaimed in 1996. Online: https://www.eff.org/cyberspace-independence. For an excellent account of the origin of the term see, for example:

the one hand, whether cyberspace is really a distinct domain or space, and on the other hand, by that token, whether or not it should be governed by legal norms.

In this debate, various voices have stated that the Internet and other parts that make up cyberspace are communication networks located within real space, and therefore it is not a different space: cyberspace includes both physical (hardware) and digital components.[3] Delerue, for instance, explains that cyberspace is not a fifth domain or sphere of application of law, but a medium that can be used to conduct activities in any of the four existing physical domains: land, sea, airspace, and outer space.[4] Dias and Coco, in turn, refer to cyberspace not as a virtual or separate space, but as a set of multidimensional digital technologies—or information and communication technologies (ICTs)—that are fully integrated with human activities that take place in different physical domains or spaces of the "real world."[5] The Tallinn Manual 2.0 (referred to in more detail below) defines cyberspace as "the environment formed by physical and non-physical components ... to store, modify, and exchange data using computer networks."[6]

A "cyber operation" is the use of cyber capabilities with the primary purpose of achieving its objectives in or through the use of cyberspace.[7] This term covers only acts that take place within a computer network, so that the conduct of any physical hostile act against a computer or computer network—for example, the destruction of a computer hard drive with a kinetic weapon—would not qualify as a cyber operation. Cyberoperations are an increasing part of our daily lives.

As it is not a separate field or exempt from jurisdiction, cyber operations or activities conducted through cyberspace must comply with the applicable legal rules. The law does not prohibit *per se* cybertransactions: on the contrary, they have come to facilitate our lives and interactions significantly. However, their malicious use may constitute a violation of international law, as discussed in the following section.

3. MALICIOUS CYBEROPERATIONS AND THEIR IMPLICATIONS FOR STATES

The 21st century has been the century of digitalization, which has been further accelerated by the isolation measures that accompanied the COVID-19 pandemic that has swept the world in recent years. At the same time, the growing use of ICTs and their interconnection and interdependence have also exposed the immense risks that come with their misuse, which can expose sensitive government, corporate, or private information or harm vital systems or infrastructure.

Malicious cyber operations are directed against information systems, such as databases or computer networks, with the ultimate goal of harming individuals, institutions, or companies. They can be classified in various ways and can harm software, hardware, and data, as well as natural persons (individuals) and legal entities (states, companies, and nongovernmental organizations). A single cyber operation can cause harm in several of these categories. One of the most common classifications for malicious cyber operations that harm software, hardware, and data is the so-called "CIA triad."[8] According to the latter, a malicious cyber operation can harm:

DIAS, T. & COCO, A., *Cyber due diligence in international law,* Oxford Institute for Ethics, Law and Armed Conflict, 2022, pp. 39–48.

[3] EASTERBROOK, F.H., "Cyberspace and the Law of the Horse", *University of Chicago Legal Forum* 207, 1996, p. 207.

[4] DELERUE, F., *Cyber Operations and International Law,* Cambridge University Press, 2020, pp. 11–12.

[5] DIAS, T. & COCO, A., *Cyber due diligence in international law,* Oxford Institute for Ethics, Law and Armed Conflict, 2022, pp. 47–48.

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

[7] *Ibid.*

[8] See, for example, WALKOWSKI, D., What is the CIA Triad?," 2019. Online: https://www.f5.com/labs/articles/education/what-is-the-cia-triad#:~:text=Understanding%20the%20significance%20of%20the,By%20Debbie%20Walkowski

(i) *Confidentiality,* through unauthorized access to computers, computer systems, and networks to obtain certain information;

(ii) *Integrity,* by altering, deleting, corrupting or denying access to certain data or software; or

(iii) *Availability*, by partially or totally disrupting the operation of a network or computer system.

The most common types of malicious cyber operations include:

(i) *Phishing*, which consists of sending fraudulent messages, usually via email, that appear to come from reliable and secure sources with aim of stealing highly sensitive personal data, such as login information or credit card details, among others."[9]

(ii) *Malware,* which is malicious software, including viruses and worms, that exploits vulnerabilities to breach networks and typically attacks when a user clicks on a link or email attachment, and whose impact ranges from installing malicious software to blocking access to key network components (ransomware) or stealthily obtaining information (spyware)."[10]

(iii) *SQL* (structured query language) *injection*, which occurs when a hacker inserts malicious code into a server using SQL, forcing it to reveal information that is protected or that it would not normally reveal."[11]

(iv) *Distributed Denial of Service* (DDoS) *attacks*, which saturate systems, servers, and networks with traffic in order to exhaust resources and bandwidth, rendering them unable to fulfill legitimate requests.[12]

Malicious cyber operations have, in turn, harmful effects on individuals and companies. As Dias and Coco point out, it is rare to find instances in which cyber operations that harm software, hardware, or data do not significantly impact persons, whether tangible or intangible. At a minimum, cybersecurity costs will be incurred to identify vulnerabilities and the extent of the harm and, if necessary, remedy it.[13] Harm to individuals may include damage to the environment, health, integrity, life, privacy, education or access to information and freedom of expression, among others. In the case of legal entities, including states, companies, and nongovernmental organizations, a malicious cyber operation can result in significant financial losses, considerable legal costs, and damage to their reputation and trustworthiness.

Particularly in the case of states, a malicious cyber operation can harm government systems, financial services, and essential state services such as electricity, water, food and medicine supply, medical services or transportation and security systems, among others. Such cyber operations against States may originate not only from private entities but also from other States perpetrating them directly (through their organs or agencies) or indirectly through entities or persons they hire.

Recent decades have seen numerous malicious cyber operations that have involved or significantly impacted States.[14] Attribution is a delicate issue since, to date, no State has directly acknowledged responsibility for directly or indirectly committing a malicious cyber operation. However, information available on several cyber operations that have adversely affected States in recent decades has sometimes led the affected country to presume that the operations were conducted against it by other States. As Finnemore and Hollis point out, between 2010 and 2020, an estimated 28 states—including China, Iran, the Democratic People's Republic of Korea, Russia, the United Kingdom and the United

---

[9] Iberdrola, *Ataques Cibernéticos: ¿cuáles son los principales y cómo protegerse de ellos.* Online: https://www.iberdrola.com/innovacion/ciberataques

[10] *Ibid.*

[11] *Ibid.*

[12] *Ibid.*

[13] DIAS, T. & COCO, A., *op. cit. supra* note 2, pp. 99–100.

[14] For an account of major State cyberattacks, see for example: DELERUE, F., *op. cit. supra* note 4, Appendix, pp. 499–501.

States—have been accused of conducting or supporting cyber operations with serious impacts on governments, peoples, and resources.[15] Examples of cases are examined below.

One of the first and most representative cases—due to its repercussions—was the campaign of malicious cyber operations suffered by Estonia in 2007,[16] which the country attributed to Russia. For 22 days it disabled numerous websites of Estonian organizations, including the parliament, banks, ministries, newspapers and media organizations. The cause was a disagreement with Russia over the relocation of a Soviet-era monument in the city of Tallinn.

In 2010, *Stuxnet*, a malware that some attribute to Israel and the United States, attacked the computer systems of five nuclear facilities at Natanz in Iran: the worm took control of 1,000 machines involved in the production of nuclear materials and gave commands that resulted in the centrifuges being destroyed. It is considered the first time that a cyberattack succeeded in damaging physical infrastructure.[17]

In 2015, Ukraine's power grid was disrupted by a cyberattack using the *BlackEnergy* malware, which that country attributes to Russia as part of the war that started in 2014. It was the first cyberattack against critical infrastructure to cause a blackout and the first completely remote one against an energy grid.[18] It disconnected 30 electrical substations and left some 80,000 people without electricity for six hours. It also affected several distribution companies and a total of 225,000 customers.[19]

In 2015 and 2016, a cyberattack infiltrated the U.S. Democratic National Committee's computer network, where it spied on communications, emails, and documents, and leaking them in order to interfere in the 2016 U.S. presidential election. The cyberattack was followed by a "troll" campaign on social networks to influence United States voters. The United States attributes the attack to Russian intelligence agencies.

In 2017, the *WannaCry* ransomware, attributed by some to groups linked to North Korea, affected around 230,000 computers running Microsoft Windows operating systems in more than 150 countries around the world. It is considered the largest ransomware attack in history. The most affected countries were Russia, Ukraine, India and Taiwan, as well as parts of the United Kingdom's National Health Service (NHS), Spain's Telefonica, FedEx of the United States, Germany's Deutsche Bahn and LatAm airlines, among others. It resulted in global costs of around US$7 billion. In the same year 2017, *NotPetya,* a ransomware that some attribute to Russia, hit various organizations in Ukraine, including its central bank, hospitals, airports and state-owned electric utility companies, as well as private companies, before spreading to systems in 63 other states in Europe and the United States. It caused damages totaling more than US$10 billion, making it the most devastating cyberattack in history.[20] Also in 2017, the *BadRabbit* ransomware affected media outlets in Russia and critical infrastructure organizations in the transport sector in Ukraine.

---

[15] FINNEMORE, M. and HOLLIS, D., "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity," in The European Journal of International Law, Vol. 31, No. 3, 2020, pp. 969-1003, at p. 970.

[16] See, for example, CALERO, F.J., "Heli Tiirmaa-Klaar: «Los ciberataques no caen del cielo, suceden por razones políticas»," in *ABC Internacional,* 2019. Online: https://www.abc.es/internacional/abci-heli-tiirma-klaar-ciberataques-no-caen-cielo-suceden-razones-politicas-201911050326_noticia.html

[17] See, in this regard: "El virus que tomó control de mil máquinas y les ordenó autodestruirse", en *BBC News*, October 11, 2015. Online: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

[18] See BROEDERS, D., DE BUSSER, E., CRISTIANO, F. & TROPINA, T., "Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?", *Journal of Cyber Policy,* 7:1, 2022, pp. 97–135, at p. 108.

[19] See, for example, TIDY, J., "The three Russian cyber-attacks the West most fears," BBC News, March 22, 2022. Online: https://www.bbc.com/news/technology-60841924.

[20] See, for example, BROEDERS, D., DE BUSSER, E., CRISTIANO, F. & TROPINA, T., *op. cit. supra* note 18, at p. 117; TIDY, J., *op. cit. supra* note 19.

In 2020 and 2021, the cyberattack against the United States software company *SolarWinds,* which some attribute to Russian intelligence services, spread to the company's customers, affecting the databases of more than 18,000 companies worldwide (including Microsoft, Cisco, Intel and Deloitte) and key U.S. federal government agencies (including the Departments of Homeland Security, State, Energy, and Finance and the National Nuclear Security Administration). The attack cost Solarwinds US$40 million in the first nine months of 2021, and each affected customer an average of US$12 million.

The ongoing war between Russia and Ukraine has not been without the use of cyberattacks to accompany kinetic activities.[21] Since the illegal annexation of Crimea in 2014, Ukraine has been subjected to continuous cyberattacks attributed to Russia. A day before the invasion on February 24, 2022, the *Foxblade* cyberattack was launched, which sought to wipe data from the computer networks of 19 government entities and critical infrastructure entities of the Ukrainian government. Since the invasion and as of late June 2022, Microsoft estimated that there have been cyberattacks targeting computer networks of 48 agencies and companies inside Ukraine, as well as network penetration and cyberespionage attempts on 128 organizations in 42 states allied to Ukraine.[22] The effect has been limited, as Ukraine has been greatly reinforced in its cyberdefense capabilities by various States, companies, and civil society organizations. For example, Ukrainian digital information and operations have been protected by moving them to the public cloud, stored in data centers elsewhere in Europe. Some experts do not rule out the possibility that Russia is biding its time to launch a massive cyberattack with far more destructive effects.[23]

4. THE APPLICABILITY OF INTERNATIONAL LAW TO CYBERSPACE: MULTILATERAL AND ACADEMIC PROCESSES

When inter-State cyberattacks such as those described above began, academics and governments turned their attention to whether or not international law was applicable to cyberspace and, if so, to what extent and in what respects. The issue is important since, with very few exceptions, international law has no specific rules governing cyberspace, and the main norms of international law came about long before cybertechnology was a reality, and therefore do not even envisage it. The only two existing international treaties relating to cyberspace are the Council of Europe's Budapest Convention on Cybercrime[24] and the African Union Convention on Cyber Security and Personal Data Protection,[25] which is not yet in force. Neither of them, however, specifically addresses the issue of cyber operations conducted by or against States. Developments to elucidate this issue have taken place in both academic and intergovernmental spheres.

4.1 The Tallinn Manuals

In 2009, the North Atlantic Treaty Organization's Cooperative Cyber Defence Centre of Excellence (CCDCOE), an international military organization based in Tallinn, assembled a group of independent international experts to produce a non-binding handbook on existing international law applicable to cyberwarfare. As a result of that exercise, in 2013 the group produced the *Tallinn Manual*

---

[21] See in this regard ORENSTEIN, M., "Russia's Use of Cyberattacks: Lessons from the Second Ukraine War," in *Foreign Policy Research Institute,* June 7, 2022. Online: https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/

[22] Microsoft, *Defending Ukraine: Early Lessons from the Cyber War,* June 22, 2022, pp. 2-3. Online: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK. See also Microsoft, *Special Report*: *Ukraine. An overview of Russia's cyberattack activity in Ukraine,* April 2022. Online: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[23] See European Parliament, *Russia's War on Ukraine*: *Timeline of cyber-attacks*, Briefing, June 2022, European Union. Online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

[24] Council of Europe, Budapest Convention on Cybercrime, ETS No. 185, in force since January 7, 2004.

[25] African Union Convention on Cyber Security and Personal Data Protection, adopted on June 27, 2014 (not yet in force). It has been ratified by 13 States (15 are required for its entry into force).

on the International Law Applicable to Cyber Warfare,[26] which, in addition to reaffirming that the general principles of international law applied to cyberspace, identified 95 rules and developed their respective commentaries on issues of sovereignty, state responsibility, *jus ad bellum,* international humanitarian law, and the laws of neutrality as they pertain to cyberwarfare. Following its publication, the CCDCOE convened a new group of independent international experts to conduct research and expand the coverage of the manual to also encompass international law applicable to cyber activities occurring during peacetime. As a result, 2017 saw the publication of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*,[27] which identified 154 rules governing cyber operations and developed their respective commentaries. Given recent developments in the practice and positions of States, in 2021 the CCDCOE launched Tallinn Manual 3.0, a five-year project to revise existing chapters and explore new issues of importance to States.[28]

4.2 Intergovernmental processes at the United Nations and positions of States

The information security has been a topic on the United Nations agenda since 1998, following a proposal submitted by Russia.[29] Since 2004, the United Nations General Assembly has established groups of governmental experts (GGEs) on six occasions to examine actual and potential threats in this area and recommend measures to address them. The GGEs initially adopted consensus reports in 2010,[30] 2013,[31] and 2015.[32] Since the 2013 report expressly recognized: *"International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."*[33] In addition, the 2015 report included 11 voluntary, non-binding norms on responsible behavior of States in cyberspace, with recommendations on confidence-building measures, capacity-building and cooperation.[34]

The GGE that sat between 2016 and 2017 failed to produce a consensus report due to differences that mainly revolved around how international law applied to cyberspace and which elements of international law should be considered first. The depth of those differences prevented the UN General Assembly in 2018 from adopting a consensus decision on the format to be followed for a resumption of discussions. As a result, two separate resolutions were adopted by a split vote: on the one hand, a

---

[26] SCHMITT, M. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, 2013.

[27] SCHMITT, M. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, op. cit. supra,* note 6.

[28] See, in this regard https://ccdcoe.org/research/tallinn-manual/

[29] See, in this regard https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement United Nations General Assembly, Resolution A/RES/53/70, "Developments in the field of information and telecommunications in the context of international security," 4 January 1999.

[30] Secretary-General of the United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* U.N. Doc. A/65/201 (30 July 2010). The Group met between 2009 and 2010 and was composed of experts from 15 States, including 2 from the Americas region: Brazil and the United States.

[31] Secretary-General of the United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* 19, U.N. Doc. A/68/98 (24 June 2013) ("2013 GGE Report"). The Group met between 2012 and 2013 and was composed of experts from 15 States, including 3 from the Americas region: Argentina, Canada, and the United States.

[32] Secretary-General of the United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* 10, U.N. Doc. A/70/174 (22 July 2015) ("2015 GGE Report"). The Group met between 2014 and 2015 and was composed of 20 governmental experts, including 4 from the Americas region: Brazil (chair), Colombia, the United States, and Mexico).

[33] 2013 GGE Report, *op. cit. supra* note 31, para. 19.

[34] 2015 GGE Report, *op. cit. supra* note 32.

Russian-sponsored resolution creating an Open-ended Working Group (OEWG) was adopted,[35] and on the other hand, a United States-sponsored resolution that created a new GGE.[36]

Both OEWG and GGE processes were conducted in parallel between 2019 and 2021, with very similar mandates but very different compositions. The OEWG chaired by Ambassador Jurg Lauber of Switzerland was open to the participation of all interested States and included consultations with other stakeholders (industry, civil society and academia). It adopted its final report by consensus in March 2021,[37] and also produced a Chair's Summary[38] describing some State proposals that did not elicit consensus, as well as a compendium of official state pronouncements concerning the adoption of the final report.[39] The final report reaffirmed that international law applied to ICTs but that further exchanges of ideas between States were needed, as was capacity building to develop a greater common understanding of how international law applied to the use of ICTs by States.

The GGE, for its part, was chaired by Ambassador Guilherme de Aguiar Patriota of Brazil and composed of experts from 25 States, including 4 from the Americas region: Brazil, Mexico, the United States, and Uruguay. The GGE adopted its final report, also by consensus,[40] in July 2021, in which it again reaffirmed that international law was applicable to ICTs and recognized the need for continued discussions and exchanges of views by States collectively at the United Nations on how specific rules and principles apply to the use of ICTs by States. The GGE also produced an official compendium of voluntary national contributions from state experts participating in the GGE focused specifically on the question of how international law applies to the use of ICTs.[41]

With a view to "ensuring the uninterrupted and continuous nature" of the above process mentioned above—and, at the same time, to remedy the complication of duplicate forums—in 2020 the UN General Assembly decided to establish a new OEWG on the security of and in the use of ICTs 2021–2025,[42] open to the participation of all States and with consultation meetings with other relevant stakeholders, under the chairmanship of Ambassador Burhan Gafoor of Singapore.[43] The topics for discussion under its mandate expressly include "how international law applies to the use of information and

---

[35] United Nations General Assembly, Resolution A/RES/73/27, "Developments in the field of information and telecommunications in the context of international security," 5 December 2018.

[36] United Nations General Assembly, Resolution A/RES/73/266, "Advancing responsible State behaviour in cyberspace in the context of international security," 22 December 2018.

[37] United Nations General Assembly, *Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security,* A/AC.290/202/CRP.2, 10 March 2021 ("OEWG 2021 Report").

[38] United Nations General Assembly, *Open-ended working group on developments in the field of information and telecommunications in the context of international security: Chair's Summary*, A/AC.290/2021/CRP.3, 10 March 2021.

[39] United Nations General Assembly, *Open-ended working group on developments in the field of information and telecommunications in the context of international security: Compendium of statements in explanation of position on the final report,* A/AC.290/2021/INF/2, 25 March 2021.

[40] United Nations Secretary-General*, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, U.N. Doc. A/76/135 (14 July 2021) ("2021 GGE Report").

[41] United Nations General Assembly, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266,* U.N. Doc. A/76/136 (July 13, 2021) ("GGE IL Compendium"). From the Americas region, contributions were submitted by experts from Brazil and the United States.

[42] United Nations General Assembly, resolution 75/240 "Developments in the field of information and telecommunications in the context of international security," adopted on December 31, 2020.

[43] See: https://meetings.unoda.org/meeting/oewg-ict-2021/

communication technologies by States."[44] On its website, the OEWG has also published statements of requesting States, by session and by topic, including the specific topic of how international law applies to cyberspace.[45]

Given the need to continue advancing the discussion on how international law applies to cyberspace, States have been gradually adopting and publishing official national positions on the subject. The CCDCOE, through its useful *CyberLaw Toolkit,*[46] compiles, *inter alia*, the official positions that have been published by States on the applicability of international law to cyberspace,[47] both in their complete version and classified according to the subject of international law they address. Of the 24 national positions that had been published as of July 2022,[48] only 3 were from countries in the Americas region: Brazil, Canada, and the United States.

The GGE and OEWG processes described above concern the applicability of international law to cyberspace as it relates to inter-State relations, principally. On a related but separate topic, in December 2019, the United Nations General Assembly decided to establish an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes.[49] The committee is to meet six times between 2022 and 2023 with a view to submitting a draft treaty to the General Assembly at its seventy-eighth session (September 2023-September 2024), which will address issues such as international cooperation for the prevention, investigation and prosecution of cybercrime.[50]

4.3 Other contributions

The International Committee of the Red Cross (ICRC) has produced valuable reports and opinions on the specific issue of the applicability of international humanitarian law (IHL) to cyberspace, including, among others, a general position paper on the subject in 2019[51] and an outcome report of an expert meeting in 2020 on avoiding harm to civilians from military cyber operations during armed conflict.[52] In March 2021 it also devoted an entire issue of the International Review of the Red Cross to the issue of digital technologies and war.[53] In June 2021 it launched the Global Advisory Board on digital threats during conflict, composed of 16 international experts who advise the ICRC on the main legal and policy challenges concerning protection of civilians against such threats.[54] Finally, it has initiated a series

---

[44] United Nations General Assembly, resolution 75/240 "Developments in the field of information and telecommunications in the context of international security," adopted on December 31, 2020, operative paragraph 1.

[45] See https://meetings.unoda.org/section/oewg-ict-2021_general-statements_14537_general-statements_16368/. From the Americas region, since the first two sessions held in December 2021 and March 2022, general statements from Colombia, Costa Rica, Cuba, and the United States have been published on the portal.

[46] See: https://cyberlaw.ccdcoe.org/wiki/Main_Page

[47] https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions

[48] In alphabetical order by their English names: Australia, Brazil, Canada, China, Czech Republic, Estonia, Finland, France, Germany, Iran, Israel, Italy, Japan, Kazakhstan, Kenya, Netherlands, New Zealand, Norway, Romania, Russia, Singapore, Switzerland, United Kingdom, and United States.

[49] United Nations General Assembly, resolution A/RES/74/247 "Countering the use of information and communications technologies for criminal purposes," adopted on December 27, 2019.

[50] See: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[51] ICRC, *"International humanitarian law and cyber operations during armed conflicts: ICRC Position Paper."* November 28, 2019. Online: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

[52] ICRC, "Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts," ICRC Expert Meeting 21–22 January 2020. Online: https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations

[53] International Review of the Red Cross, "Digital technologies and war," IRRC No. 913, March 2021. Online: https://international-review.icrc.org/es/revistas/irrc-no-913-las-tecnologias-digitales-y-la-guerra

[54] See: https://www.icrc.org/en/document/global-advisory-board-digital-threats

of regional state consultations on IHL and cyber operations during armed conflicts: in November 2021 it conducted consultations with Latin American States, the report on which was published recently,[55] and in December 2021 it conducted consultations with Central and Eastern European States, the report on which is forthcoming.

The ICRC has also collaborated with the CCDCOE and other participating organizations and universities to launch in 2019, on the CCDCOE web portal, the aforementioned *Cyber Law Toolkit,* an extremely useful interactive online tool for the analysis of international law and cyber operations. It includes hypothetical scenarios accompanied by legal analysis, as well as examples of real cases and a general and thematic compilation of the official positions published by States on the subject.

These global efforts are joined by the *Oxford Process on International Law Protections in Cyberspace*, launched in May 2020 by the Oxford Institute for Ethics, Law and Armed Conflict in partnership with Microsoft. Since its inception, as of the date of this report, the Oxford Process has issued five public statements, agreed upon by international legal expert groups, on international law protections against cyber operations targeting the health sector, vaccine research in the context of COVID-19, foreign electoral interference through digital means, the regulation of information operations and activities, and the regulation of ransomware operations.[56]

4.4 Regional developments in the Americas

The Organization of American States (OAS) has collaborated in training efforts and dialogue promotion among member states on the applicability of international law to cyberspace. On the one hand, the Inter-American Committee against Terrorism (CICTE) has been carrying out its Cybersecurity Program for more than 15 years, through which it assists OAS member states in the development of cybersecurity capabilities at the technical and public policy levels.[57] Among other endeavors, it assists in the development of national cybersecurity strategies, prepares regional reports and publications, and provides training to public and private officials, as well as students, on cybersecurity and cyber operations.

For its part, the Inter-American Juridical Committee (CJI) of the OAS began working on the issue in 2018, at the proposal of the then-member and rapporteur on the topic, Duncan B. Hollis (of the United States). Under the title *"Improving Transparency: International Law and State Cyber Operations,"* the initiative sought to "contribute to a broader trend in international relations seeking more transparency on how nation States understand international law's application to cyberspace,"[58] identifying areas of convergence and divergence. This, based on a questionnaire distributed in 2019 to OAS member states that contained 10 questions on specific issues of international law and their applicability to cyberspace.[59]

---

[55] ICRC and Ministry of Foreign Affairs of Mexico, "Regional Consultation of Latin American States: International Humanitarian Law and Cyber Operations During Armed Conflicts," November 9–10, 2021. Online: https://www.icrc.org/en/document/regional-state-consultations-ihl-cyber-operations

[56] Online: https://www.elac.ox.ac.uk/the-oxford-process/

[57] See: https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

[58] See Dr. Hollis' fifth report, "Improving Transparency: International Law and State Cyber Operations" CJI, 2020 ("2020 Hollis Report"), available at https://www.oas.org/en/sla/iajc/docs/themes_recently_concluded_International_law_State_cyber_operations_FINAL_REPORT.pdf

[59] The questions put to the States were: "**1.** Has your Government previously issued an official paper, speech, or similar statement summarizing how it understands international law applies to cyber operations? Please provide copies or links to any such statements. **2**. Do existing fields of international law (including the prohibition on the use of force, the right of self-defense, international humanitarian law, and human rights) apply to cyberspace? Are there areas where the novelty of cyberspace excludes the application of a particular set of international legal rights or obligations? **3.** Can a cyber operation by itself constitute a use of force? Can it constitute an armed attack that triggers a right of self-defense under Article 51 of the UN Charter? Can a cyber operation qualify as a use of force or armed attack without causing the violent effects that have been used to mark such thresholds in past kinetic conflicts? **4.** Outside of armed conflicts, when would a State be responsible for the cyber operations of a non-State

Only 9 of the 35 OAS member states responded to the questionnaire: Bolivia, Brazil, Chile, Costa Rica, Ecuador, Guatemala, Guyana, Peru, and the United States.[60] The rapporteur also held an informal discussion with legal representatives from 16 OAS member states under the Chatham House Rule. The results of the initiative were published in Rapporteur Hollis' fifth and final report in 2020 and serve as a consultation tool for States.[61] Among his conclusions, Rapporteur Hollis identified wide disparities among States in the Americas region in terms of technical capabilities (e.g., for the attribution of a cyber operation to a foreign State) and of legal experience and expertise on how international law can manifest itself in the cyber context. He also identified political challenges to greater transparency in the American States in this area, as well as internal institutional challenges within the States of the region, such as the lack of clarity in the assignment of responsibilities for cyber issues among authorities within each State or the lack of interinstitutional dialogue between the different internal authorities that could be directly or indirectly involved in cyber issues.

Further to the final recommendations of Rapporteur Hollis, the OAS General Assembly adopted a resolution reaffirming the applicability of international law in cyberspace.[62] Although the rapporteur had suggested detailed language expressly recognizing the applicability of the UN Charter, the OAS Charter, IHL, international human rights law, the duty of non-intervention, the sovereign equality, and the law of state responsibility, the consensus language adopted by the OAS General Assembly followed the trend seen in UN forums of simply restating in general terms the applicability of international law to cyberspace, as well as referring to the norms contained in the reports of the GGE. We dare assume that this more cautious approach was perhaps due to the fact that most of the States of the American region do not yet have official public positions on the applicability of specific international law issues to cyberspace and, therefore, did not yet consider themselves ready to adopt through the OAS General Assembly a detailed joint position on the issue.

Another of Rapporteur Hollis' final recommendations was that, after the expiration of his mandate at the end of 2020, the CJI retain the topic on its agenda, with the possibility of expanding its scope beyond the ten questions asked to topics such as non-intervention or international human rights law, and

---

actor? What levels of control or involvement must a State have with respect to the non-state actor's operations to trigger the international legal responsibility of that State? **5.** Are the standards of State responsibility the same or different in the context of an armed conflict as that term is defined in Articles 2 and 3 common to the 1949 Geneva Conventions? **6.** Under international humanitarian law, can a cyber operation qualify as an "attack" for the rules governing the conduct of hostilities if it does not cause death, injury or direct physical harm to the targeted computer system or the infrastructure it supports? Could a cyber operation that produces only a loss of functionality, for example, qualify as an attack? If so, in which cases? **7.** Is a cyber operation that only targets data governed by the international humanitarian law obligation to direct attacks only against military objectives and not against civilian objects? **8.** Is sovereignty a discrete rule of international law that prohibits States from engaging in specific cyber operations? If so, does that prohibition cover cyber operations that fall below the use of force threshold, and which do not otherwise violate the duty of non-intervention? **9.** Does due diligence qualify as a rule of international law that States must follow in exercising sovereignty over the information and communication technologies in their territory or under the control of their nationals? **10.** Are there other rules of international law that your government believes are important to highlight in assessing the regulation of cyber operations by States or actors for which a State is internationally responsible?"

[60] Seven of the responses were direct and substantive answers to the questions in the questionnaire, while Brazil only indicated that its position was within the framework of the GGE, which it chaired at the time, and the United States merely shared positions that it had previously made public.

[61] 2020 Hollis Report, *op. cit. supra* note 58.

[62] *OAS General Assembly*, resolution AG/RES. 2959 (L-0/20) adopted on October 21, 2020: "REAFFIRMING the applicability of international law to cyberspace and the importance of implementing voluntary, non-binding norms for responsible State behavior in cyberspace, as adopted by the United Nations in the consensus reports of the Group of Governmental Experts and Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security."

that the CJI support—in concert with other institutions, States or organizations—or undertake additional legal capacity-building efforts among OAS member states in the application of international law in the cyber context.

It was in follow-up to the latter recommendation that in 2021 the CJI decided to continue studying the topic and appointed Dr. Mariana Salazar Albornoz as rapporteur for the period 2021–2022. Based on her first report, she held an informal consultation with legal representatives of OAS member states in 2021, at which she proposed different options for continuing the work of the Rapporteurship, including the possibility of distributing a new, expanded questionnaire or focusing on technical/legal capacity building and dialogue on the topic. The vast majority of representatives indicated their preference to continue capacity building and dialogue before considering the possibility of a new questionnaire, as most States in the Americas are not yet ready to adopt official positions on the issue.

In light of the above, in her capacity as CJI rapporteur, she co-organized, together with CICTE and the OAS Department of International Law, the event *"International Law Applicable to Cyberspace*: *Dialogue with OAS Member States."* The forum was held under a hybrid format, at OAS headquarters in Washington, D.C., on June 14, 2022, with the participation of recognized international experts, to address the main specific issues of international law involved in the debate on its applicability to cyberspace. A video of the event has been posted on the OAS website to serve as a permanent consultation and support tool for States that are in the process of preparing their national positions on the issue.[63]

Additionally, in her capacity as CJI rapporteur on the subject, in concert with other organizations, she has participated in various forums that have continued discussions on the applicability of international law to cyberspace, including:

- *Within the framework of the OAS:* (i) special meeting of the Committee on Juridical and Political Affairs to reflect collectively on strengthening the accountability regime in the use of information and communication technologies (ICTs) (June 2, 2022); (ii) the webinar *International Law and State Cyber Operations,* organized by the Department of International Law (March 8, 2021); and (iii) Inter-American Defense Board seminar on *Human Rights and International Humanitarian Law for the Armed Forces of the Western Hemisphere* for 14,000 members of the armed forces in the region (March 24, 2021).
- *Organized by the ICRC*: (i) Regional Consultation of Latin American States: International Humanitarian Law and Cyber Operations During Armed Conflicts, co-organized with the Ministry of Foreign Affairs of Mexico (November 9 and 10, 2021); (ii) the global conversation *Digital Technologies and Humanitarian Action in Armed Conflict* (March 18, 2021); (iii) Regional Meeting of National Committees on IHL and Other Similar Entities of the Americas (February 4, 2021); and (iv) meetings of the ICRC Global Advisory Board on digital threats during conflict (June 9 and November 23, 2021; and June 14, 2022).
- *In academia:* Seminar *The Evolving Face of Cyber Conflict and International Law: A Futurespective,* organized by the Technology, Law and Security Program at American University, Washington College of Law (June 15 to 17, 2022).

5. SPECIFIC INTERNATIONAL LAW ISSUES APPLICABLE TO CYBERSPACE AND THE EMERGING POSITIONS OF STATES IN THE AMERICAS REGION

There are vast and varied facets to each of the international law issues that may be implicated in connection with a state cyber operation, and this section is not intended to be an exhaustive analysis of them. We will limit ourselves to mapping the main issues under debate and the positions that the States of the Americas region have begun to adopt in this regard, based on the positions that the States

[63] The video is available at:
https://www.oas.org/es/sla/ddi/Derecho_Internacional_aplicable_al_Ciber_Espacio_2022_video.asp

themselves have made public, through (i) those compiled on the CCDCOE portal (taken, in their turn, from the websites of the governments or the United Nations);[64] (ii) those published in the compendium of national positions of the 2021 GGE;[65] (iii) those that the States have asked to be published on the portal of the new OEWG for 2021–2025;[66] and (iv) the answers provided to the questionnaire put out in 2019 by the Inter-American Juridical Committee and compiled in the 2020 report of Rapporteur Hollis.[67]

From these sources, it appears that the States of the Americas that have adopted the most comprehensive official positions on most of the legal issues involved in the debate on cyberspace are Brazil, Canada, and the United States. For their part, Bolivia, Chile, Cuba, Ecuador, Guatemala, Guyana, and Peru have made clear positions on some specific issues. This section reviews the positions of those 10 countries.[68] The general statements that a number of other States have made without taking a specific position on an issue are not included in this section. It should also be noted that these sources do not contain all the oral statements made by States during the intergovernmental negotiations within the GGE and the OEWG, but only those that States themselves have decided to publish.

We will follow the general structure of the *Articles on Responsibility of States for Internationally Wrongful Acts* (which largely reflect customary international law on the subject),[69] which indicate that there is an internationally wrongful act (IWA) of a State occurs when conduct consisting of an act or omission (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State.[70]

5.1 The question of attribution

Conduct is attributable to a State when it is carried out by State organs, by persons or entities exercising elements of governmental authority, or by organs placed at the disposal of a State by another State.[71] Conduct by non-State actors is also attributable to the State when such persons are in fact acting on the instructions or under the direction or control of that State, or when they are in fact exercising powers of public authority in the absence or default of official authorities, or when it is carried out by an insurrectional or other movement that becomes the new government of the State or establishes a new State, or when the State recognizes and adopts the conduct as its own.[72] In the latter cases involving non-state actors, attribution to the State will be made after a separate assessment on a case-by-case basis.

In the cyber domain, this means that, for example, a cyber operation conducted by the armed forces or intelligence services of a State, or by a private cybersecurity company that has been contracted by the State to conduct cyberdefense on its behalf, or by a hacker group instructed by the State, will be conduct attributed to the State in question. However, in the cyberspace realm, the question of attribution is technically, legally, and politically difficult.[73]

---

[64] https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions
[65] GGE IL Compendium, *op. cit. supra* note 41.
[66] https://meetings.unoda.org/section/oewg-ict-2021_general-statements_14537/
[67] 2020 Hollis Report, *op. cit. supra* note 58.
[68] The positions provided in this section are: the positions of Brazil (2021) and the United States (2021) contained in the GGE IL Compendium, *op. cit. supra* note 41; the position of Canada (2022) published on its government website and compiled on the CCDCOE website; some positions of Bolivia, Chile, Ecuador, Guatemala, Guyana, and Peru from the 2020 Hollis Report, *op. cit. supra* note 58; and Cuba's position delivered before the new OEWG at its first session in December 2021. Online: https://documents.unoda.org/wp-content/uploads/2021/12/GTCA-Ciberseguridad-2021-2025.-Intervencion-Cuba-sobre-aplicacion-del-Derecho-Internacional.pdf
[69] *Articles on Responsibility of States for Internationally Wrongful Acts,* adopted by the United Nations International Law Commission at its fifty-third session in 2001 and annexed by the General Assembly to its resolution 56/83 of 12 December 2001, as corrected by document A/56/49(Vol. I)/Corr4.
[70] *Ibid.*, Article 2.
[71] *Ibid.*, Articles 4, 5, and 6.
[72] *Ibid.,* Articles 8, 9, 10 and 11.
[73] See, in this regard: DELERUE, F., *op. cit. supra* note 4, pp. 55–85.

Technically, to identify the person or group responsible for the malicious cyber operation, one evaluates, for example, the methods or techniques used (the so-called "tradecraft"), the physical and virtual infrastructure used (the computers from which the cyber operation was prepared, launched or transited, domain names, IP addresses, etc.) and the malware used, among other factors. This is a complex process, due to the anonymity, interconnectedness, cross-border nature, and the fact that in many cases the perpetrators of cyberattacks falsify their identities or "disguise" their methods by copying those of other groups to avoid detection.

Legally, it must be determined whether there is a link between the person or group of persons who perpetrated the cyberattack and the State, according to the attribution criteria described at the beginning of this section. Proving this link has been extremely difficult in practice. To date, no State has "self-attributed" the authorship of a cyberattack against another State. Nor has there been a judicial process before the International Court of Justice or any other international court in which a State sued another State for its alleged responsibility in a malicious cyber operation, so there has not been a legal proceeding for attribution in that regard.

So far, finger-pointing at possible state perpetrators of cyberattacks has remained in the political sphere.[74] In some instances, private companies have taken the step of daring to attribute responsibility for a cyberattack to a State. In other cases, States that have been victims of cyberattacks have been cells made political statements accusing other States of the cyberattack. Sometimes States even make joint statements. The truth is that the practice is still not uniform, and such statements vary greatly in terms of the amount of information and evidence provided, both publicly and in support of their assertions. Attribution is a sensitive issue and often requires the collaborative work of governments, private entities, and civil society. Such accusations have political consequences, such as diplomatic demarches or retaliatory measures.[75]

There is no norm of international law governing the specific standard of proof for attributing cyber operations to States. In a judicial proceeding, it will depend on the forum concerned, while, for political statements, the Tallinn Manual 2.0 indicates that States should act "reasonably" when attributing a cyber operation, considering the relevant information available and the circumstances.[76] The United States adheres to this standard of reasonableness provided for in the Tallinn Manual, and reiterates that it is not a matter envisaged in international law or required for political authority. It adds that nor is it a requirement for a State to be able to respond to a malicious cyber-operation against it with "self-help" measures such as countermeasures and reaffirms that resorting to such measures is a right of the victim State where it has information on the attribution of a cyber-operation to another State.

As regards the applicable criteria for attribution, Brazil, Canada, and the United States generally recognize that the criteria for attribution contained in the Articles on State Responsibility are customary international law. Brazil and Chile consider that, in the case of conduct by private persons or entities, it must be proven that the State had "effective control" over the cyber operation in order for it to be attributable to the State.

Finally, regarding the need to present or not to present evidence when publicly attributing cyber operations, Canada and the United States have reaffirmed that States are not required to publicly disclose the evidence on which the attribution is based. However, the United States adds that in order to facilitate an overall understanding of the emerging practice, such public attributions should, where possible, include sufficient corroborating evidence. Brazil, in turn, reiterates the importance that allocation

---

[74] For a detailed analysis of these, see: TSAGOURIAS, N. and FARRELL, M., "Cyber Attribution: Technical and Legal Approaches and Challenges," *European Journal of International Law*, Vol. 31, No. 3, 2020, pp. 941–966.

[75] For an extended analysis, see: ROGUSKI, P., "Application of International Law to Cyber Operations: A Comparative Analysis of States' views", *Policy Brief, The Hague Program for Cyber Norms, Universiteit Leiden,* 2020, https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views

[76] Tallinn Manual 2.0, *op. cit. supra* note 6*,* Chapter 4, Section 1, para. 10.

determinations be duly substantiated and justified, and that technical difficulties should not be a justification for lowering the threshold.

5.2 Breach of an international obligation

As mentioned above, the existence of an IWA requires, in addition to attribution, that the behavior be a breach of an international obligation that was binding on the State at the time the event occurred.[77] Although cyber operations between States are not prohibited *per se* by international law, there is no doubt that they may constitute a violation of international obligations. International obligations derive from the primary sources of international law, namely international treaties, customary international law, and general principles of law. Some of the main international obligations that may be violated through a cyber operation are discussed below.

5.2.1 Sovereignty

As stated in the well-known 1928 *Island of Palmas* arbitration award, *"[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.*"[78] Sovereignty is a fundamental principle of international law. In the cyber realm, the Tallinn Manual 2.0 clarifies that, in its domestic component, States have sovereign authority with respect to cyber infrastructure, persons and cyber activities located within their territory.[79]

In the cyberspace debate, the discussion revolves around the following main issues:

a) Rule or principle:

Most States that have stated their positions consider sovereignty to be an independent rule of international law whose violation engages State responsibility,[80] including, in the Americas region, Brazil, Canada, Bolivia, Guatemala, and Guyana. However, a minority, particular the United Kingdom supported by the United States,[81] consider that it is not an independent rule, but a principle guiding international relations.

[77] Articles on State Responsibility, *op. cit. supra* note 69, Article 13.
[78] Island of Palmas case, United States v. Netherlands, arbitral award, 1928.
[79] Tallinn Manual 2.0, *op. cit. supra* note 6, rule 2.
[80] This view is also supported by the Tallinn Manual 2.0.
[81] Paul C. Ney, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference,* 2 March 2020.

b) 'De minimis' or any operation:

On the premise that sovereignty is an independent rule, it must, then, be determined in which cases a cyberoperation violates the sovereignty of another State. Some consider that any penetration of a computer network located on the territory of another State violates its sovereignty. Others, by contrast, say that not all such operations constitute violations, but only those that produce more than minimal effects (the latter is the so-called *de minimis* approach).[82]

In the Americas, Canada follows the approach of the Tallinn Manual 2.0 in that it considers that cyber operations that infringe to a sufficient degree on the territorial integrity of the attacked State,[83] or that interfere with, or usurp, inherently governmental functions of the attacked State, are in violation of sovereignty. Canada emphasizes that only cyber operations that surpassed the *de minimis* or negligible effects threshold and cause significant harmful effects on the territory of another State without the consent of the other State, could amount to a violation of sovereignty. It clarifies that those that only cause minimal or negligible effects do not constitute a violation and emphasizes that States may adopt these cyber operations to defend themselves against malicious cyber actors or to defend their national security. It indicates that cyberactivity that requires rebooting or reinstalling an operating system is not likely to violate sovereignty.

In the same vein, both Canada and the United States clarify that remote cyber operations by one State involving computers or other networked devices located in the territory of another State are not *per se* in violation of sovereignty, particularly when they have no or only minimal effects. They clarify in that connection that cyber espionage is not prohibited by international law, although it may be prohibited in national laws.

Brazil would seem to tend more towards an any penetration approach, although it is not entirely clear. It mentions that interceptions of telecommunications would be considered in violation of sovereignty, and that cyber operations against computer systems located in the territory of another State or causing extraterritorial effects could also violate sovereignty.

c) The degree of infringement required

In determining what is "a sufficient degree" of breach of the integrity of the State attacked, Canada follows the approach of considering the scope, scale, impact or severity of the disruption, including the disruption of economic and social activities, essential services, inherently governmental functions, public order, or public safety. It considers that the impact or severity should be assessed in the same way and under the same criteria as for physical activities.

If the cyberoperation causes a loss of functionality of cyberinfrastructure located in the territory of another State, Canada considers that it violates sovereignty if the loss of functionality causes significant harmful effects similar to those caused by physical harm to persons or property. It cites as an example that the harm would entail repair or replacement of physical components of cyber infrastructure, or the loss of functionality of physical equipment that depends on the affected infrastructure to operate.

d) Usurping inherently governmental functions

Canada clarifies that cyber operations may violate sovereignty if they usurp such functions, regardless of whether there was physical damage, injury, or loss of functionality. For Canada, inherently governmental functions include governmental activities in the areas of health care services, administration of justice, management of elections, tax collection, national defense and the conduct of international relations, as well as the services on which it relies.

5.2.2 Non-intervention

---

[82] ROGUSKI, P., *op. cit. supra* note 76, p. 4.
[83] Tallinn Manual 2.0, *op. cit. supra* note 6, rule 4.

Non-intervention is a fundamental principle of international law and a rule of customary international law. Following the definition provided by the International Court of Justice in the *Nicaragua v. United States* case*,* non-intervention implies: (a) non-interference in matters which each State may, by the principle of State sovereignty, freely decide, including the choice of political, economic, social and cultural systems and the formulation of foreign policy; and (b) the use of methods of coercion in respect of such matters, which must be kept free.[84]

In the cyber realm, there are different positions on what constitutes coercion. On the one hand, for some, an act is coercive if it is specifically designed to compel the victim State to modify its behavior on a matter that is within its *domaine réservé* (reserved domain). For others, it is sufficient that the act effectively deprives the attacked State of its ability to control or govern matters within its *domaine réservé* (without actually seeking to compel the State to change its behavior). In the Americas, Brazil subscribes to the latter position. Canada embraces both positions and mentions the requirement that a result be imposed on the affected State and, in turn, that coercion may also occur when the affected State is deprived of the possibility to choose.

Among the examples they provide, Brazil, Canada, and the United States mention that electoral interference, if coercive, would violate the principle of non-intervention. Canada adds the example of a cyber operation that disrupts the operation of a significant gas pipeline, causing the affected State to alter its position in bilateral negotiations on an international energy agreement. The United States also added the example of a cyber operation that coercively interferes with the State's ability to protect the health of its population by, for example, conducting vaccine research or establishing cybercontrolled ventilators in its territories during a pandemic, which, it said, could be in breach of the non-intervention rule.

5.2.3 Prohibition on the use of force

Most States that expressed a position agree that a cyber operation may violate the prohibition on the use of force under Article 2(4) of the UN Charter, according to which UN Member States *"shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."* Since the notion of "force" in that prohibition refers to "armed" force,[85] the debate mainly revolves around determining when a cyber operation is considered to constitute a prohibited use of armed force under that article.

In the Americas region, Brazil, Bolivia, and Canada consider that a cyber operation violates the prohibition on the use of force if its scale and effects are comparable to those of kinetic attacks that constitute use of force under international law, based on a case-by-case assessment. The United States also recognizes that a cyber operation that results in damage similar to dropping a bomb or firing a missile would be considered a use of force.

For purposes of a case-by-case assessment, the United States believes that factors such as the nature and extent of injury or death to persons and destruction of, or damage to, property, as well as the context of the event, the actor perpetrating the action, the target and its location, the effects, and the actor's intent must be taken into account. It holds that cyber operations that cause death, injury or significant destruction, or pose an imminent threat thereof, are likely to be viewed as a use of force.

In turn, Brazil advises caution when making analogies between cyber and kinetic actions, particularly considering that, to date, no State has alleged that this prohibition has been violated to its detriment as a result of a cyberattack. It considers that in many cases it might be difficult to draw a direct analogy between the acts of aggression envisaged in UN General Assembly resolution 3314 (dating from

[84] *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States) (Merits), 1986, ICJ Rep 14, para 205.

[85] Dörr, Oliver and Randelzhofer, Albrecht, 'Article 2(4)', in Simma, Bruno et al. (eds), *The Charter of the United* Nations: *A Commentary*, Vol I (OUP 2012) 208 para. 16.

1974) and cyber operations,[86] and therefore considers it advisable to update the multilateral understanding as to what acts constitute use of force and aggression in order to include cyber attacks.

Guyana has expressed doubts that cyber-only operations can constitute a prohibited use of force under Article 2.4 of the Charter.[87]

5.2.4 Duty of due diligence

Most States that have stated positions consider that the exclusive jurisdiction that States have over cyber infrastructure located in their territories creates rights, but also obligations.[88] As indicated by the International Court of Justice in the *Corfu Channel* case, every State has an obligation not knowingly to permit its territory to be used for acts contrary to the rights of other States.[89] Following that approach, one of the voluntary standards contained in the 2015 GGE report was that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

In the cyberspace domain, there is some debate about:

a) Independent obligation or attribution criterion

In the Americas region, Chile, Ecuador, Guatemala, Guyana, and Peru seem to adhere to this position that due diligence is an obligation that applies to cyberspace. Canada refers to it as an expectation from States. The United States, for its part, considers that there is insufficient state practice and *opinio juris* to consider that due diligence is a general obligation under international law.

b) *Scope of the obligations of the State under the due diligence rule*

In the Americas, both Canada and the United States have indicated that the obligation applies when a State *becomes aware* of malicious cyber activity emanating from its territory, in which case it must adopt reasonable measures to address it. The United States restricts this obligation to cases in which the State "is notified" of the cyber operation. For its part, Canada also extends it to cases of imminent cyber operations that *would result* in significant harm to another State.

As the 2021 GGE report states, *"it is not expected that States could or should monitor all ICT activities within their territory.*"[90] This would not only be impossible but could also constitute a dangerous justification for mass surveillance systems.[91] In that regard, the United States clarifies that sovereignty over ICTs in the territory of a State should not serve as an excuse to violate human rights and other obligations under international law.

As for the scope of activities to be undertaken by the State, Canada specifies that it depends on the circumstances, including whether the State has knowledge of the act, its technical and other capabilities to detect and stop it, and the measures that would be reasonable in each case. For example, a State with limited technical capabilities would probably not be expected to respond if it did not detect malicious cyber activity emanating from or through cyber infrastructure on its territory, but once aware, that State would have to respond.

The 2021 GGE consensus report, in describing the voluntary standard of due diligence, adds that the affected State must notify the State from which the cyberattack emanated, in order to facilitate cooperation and clarification of the facts, and that the notified State must make all reasonable efforts to assist in determining whether an IWA has been committed.

5.2.5 International humanitarian law (IHL)

---

[86] United Nations General Assembly, resolution 3314 (XXIX), "Definition of Aggression," adopted on 14 December 1974.
[87] 2020 Hollis Report, *op. cit. supra* note 58, p. 37.
[88] ROGUSKI, P., *op. cit. supra* note 76, p. 11.
[89] International Court of Justice, Corfu Channel Case (United Kingdom v. Albania), Merits, 1949, ICJ Rep 4, 22.
[90] 2021 GGE Report, *op. cit. supra* note 40, para. 30(a).
[91] Delerue, F., *op. cit. supra* note 4, p. 359.

In the cyberspace realm, the 2015 GGE report recognized the applicability of the humanitarian principles of humanity, necessity, proportionality, and distinction in cyberspace. In turn, the 2021 GGE report noted:

> *"that international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognised the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict."*

a) Applicability of IHL

In the Americas region, Canada, Brazil, and the United States reaffirm that IHL applies to cyber operations in times of armed conflict. Brazil recalls the advisory opinion of the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons to indicate that excluding cyber operations from IHL would be incompatible with the intrinsically humanitarian character of the legal principles in question, which permeate the entire law of armed conflict and apply to all forms of combat and all weapons, past, present and future. Brazil clarifies that IHL is applicable to cyber operations (i) when they are used as part of an ongoing armed conflict, to contribute to conventional operations, and (ii) when the cyber operation itself crosses the threshold of violence to be classified as armed conflict.

Cuba takes the opposite position, stating that it does not consider the applicability of IHL to ICTs relevant in the context of international security, "*since this would imply tacit acceptance of the possibility of a scenario of armed conflict in this arena; it would contribute to the militarization of cyberspace and would be a first step towards equating a cyberattack with a traditional armed attack*."[92] In response to that argument, both Brazil and Canada clarify that recognizing the applicability of IHL to cyberspace is not an endorsement to militarize it nor does it legitimize illegal cyber operations, but only ensures a minimum of protection in the event of armed conflict.

b) The notion of "attack" under IHL.

While some IHL norms are applicable to any military operation, several of them are specifically applicable in the case of "attack," particularly those prohibiting attacks against civilians and civilian objects, those prohibiting indiscriminate and disproportionate attacks, and the obligation to take every precaution with a view to avoiding or minimizing incidental harm to civilians and civilian objects when an attack is carried out. Thus, in the cyberspace realm, it is crucial to determine whether a cyber operation can constitute an "attack" for IHL purposes, and under what assumptions.

Article 49 of Protocol I defines "attacks" as "acts of violence against the adversary, whether in offence or in defence." The notion of violence may refer either to the means of combat or to its effects, which means that an operation that causes violent effects may qualify as an attack even if the means used are not violent. Hence, cyber operations that are reasonably expected to cause injury or death to persons or damage or destruction of objects are considered to amount to "attacks" under IHL.[93] This position has been espoused, among others, by Canada.

The United States has said that not all cyber operations will rise to the level of an "attack" under IHL and that States must consider, among other things, whether it produces kinetic or non-kinetic effects, as well as the nature and extent of those effects and the nature of the connection, if any, between the cyber activity and the armed conflict in question. Even if it does not rise to the level of an "attack," the United States considers that the cyber operation must meet the principle of military necessity.

However, there are divergent positions on the concept of "harm" in assessing whether a cyber operation constitutes an attack. In the Americas, Chile, Peru, and the United States consider that an attack

---

[92] Position of Cuba, first session of the OEWG, December 2021, *op. cit. supra* note 68.
[93] In keeping with the analysis of the *Cyber Law Toolkit*, *op. cit. supra* note 46.

should only be considered an attack if it causes death, injury, or direct physical damage; Chile adds that actions to repair or recover the affected infrastructure or computer system would also be required. Thus, for those States mere loss of functionality of the infrastructure would be insufficient to categorize it as an attack. On the other hand, Ecuador and Guatemala consider that a cyber operation could constitute an attack without causing physical damage if it causes the loss of functionality of the target (a position shared by the ICRC). As a threshold, Ecuador considers that it should be rendered inoperable, while Bolivia refers to disabling essential services of a State such as water, electricity, telecommunications, or the financial system. Brazil merely indicates that further reflection is required on the question of the definition of cyberattack, considers civilian data to be civilian objects, and indicates in which cases a civilian acting in cyberspace can be considered as taking direct part in hostilities.

c) *Development of cyberweapons*

According to Article 36 of Protocol I to the Geneva Conventions, the development of new weapons must undergo a legal review to determine whether it can comply with humanitarian principles. This obligation applies to any weapon, including cyberweapons. For example, the development of self-propagating cyber tools that cause indiscriminate damage to civilian and military targets is prohibited.

Brazil, Canada, and the United States have recognized the applicability of this new-weapons legal review obligation to weapons that use cyber capabilities. In that regard, Canada recalls that the choice of methods and means of combat is not unlimited, and also clarifies that not all cyber capabilities and activities will constitute a weapon, means, or method of combat. Brazil clarifies that the legal review obligation applies to the development, acquisition, or adoption of such cyber capabilities.

d) Military targets and electronic data

Under the principle of distinction, parties to an armed conflict must at all times distinguish between civilian objects and military objectives and accordingly direct their operations only against military objectives.[94] Military objectives are those which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[95]

In the cyberspace realm, the debate revolves around whether data can qualify as "property," and thus be a military objective subject to attack or a civilian object protected from attack under IHL, particularly when the cyber operation does not produce physical effects.[96] For some States, such as Chile, the notion of "property" is limited to physical property that is visible and tangible in the real world, and therefore data are not assets (this is the position of the Tallinn Manual 2.0);[97] however, Chile recognizes that an attack directed exclusively against computer data could generate adverse consequences affecting the civilian population, therefore, due to its effects, the principle of distinction must be taken into account and a State should refrain from attacking data in case it could affect the civilian population, unless such data were being used for military purposes. For others, data does fall within the concept of property under IHL and, therefore, when it is civilian data, it is protected under IHL and its principle of distinction (it must not be attacked and care must be taken not to cause excessive incidental damage to it). An intermediate position has also emerged, which considers that content data (other than operational data) of a civilian nature are the only ones that are protected under IHL.

e) Scope of the principles of distinction, proportionality, and precaution

Canada expressly recognizes that cyber operations must comply with the principles of distinction, proportionality and precaution. In keeping with the principle of *distinction*, the United States holds that cyber operations during an armed conflict should be directed only at military objectives, such as

---

[94] Protocol I, Article 48.
[95] Protocol I, Article 52(2).
[96] For a detailed analysis, see Mačák, K. "Unblurring the lines: military cyber operations and international law", *Journal of Cyber Policy*, Vol. 6, 2021. Online: https://doi.org/10.1080/23738871.2021.2014919
[97] Tallinn Manual 2.0, *op. cit. supra* note 6, p. 437.

computers, other networked computing devices, or possibly specific data that, by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

On the principle of *proportionality*, the United States indicates that parties to a conflict must assess the potential effects of a cyber operation on both military and civilian infrastructure and users, including shared physical infrastructure (such as a dam or power grid) that could affect civilians, in order to assess whether the cyber operation would be expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian objects which would be excessive in relation to the concrete and direct military advantage anticipated. Aside from the potential physical damage of a cyber activity, such as death or injury resulting from effects on critical infrastructure, parties must assess the potential effects of a cyberattack on civilian objects that are not military objectives, such as private, civilian computers that have no military significance but may be connected to military targets.

Regarding the principle of *precaution* in the choice of means and methods of attack with a view to avoiding or minimizing loss of civilian life, injury to civilians, and damage to civilian objects, Brazil recognizes its applicability to cyberspace, taking into account its particularities, such as the interconnection between military and civilian networks.

f) Respect for and protection of medical units and personnel

IHL obliges parties to conflicts to respect and protect medical units, which should not be subject to attack.[98] This obligation includes not interfering with the operation of medical services. The ICRC and the Tallinn Manual 2.0 have clarified that this obligation encompasses a prohibition on deleting,[99] altering or otherwise affecting medical data, including data necessary for the proper use of medical equipment, for tracking the inventory of medical supplies, and personal medical data required for the treatment of patients. Accordingly, cyber operations during armed conflicts must also comply with this obligation.

5.2.6 International Human Rights Law (IHRL)

Due to their effects and consequences, cyber operations may also adversely affect human rights. Peru expressly recognizes the validity of various human rights in cyberspace, including "the right to privacy, freedom of information, freedom of expression, free and equal access to information, elimination of the digital divide, intellectual property rights, the free flow of information, the right to secrecy of communications, etc."[100] Canada also considers that IHRL is applicable to cyber operations, and believes that the human rights for which there are particular implications include freedom of expression and opinion, freedom of peaceful association, non-discrimination, and the right to privacy.

The United States clarifies that while the physical infrastructure supporting Internet and cyber activities is generally located in sovereign territory and is subject to the jurisdiction of the territorial State, the exercise of jurisdiction by that territorial State is not unlimited but must respect IHRL. It refers in particular to freedom of opinion and expression, which may be exercised by any means and regardless of borders.

IHRL contains obligations for the State with respect to individuals *under its jurisdiction*: this refers either to its territory or to situations in which the State exercises power or effective control, either over the territory in which a person is located, or over the individual. A State may be responsible for violations of human rights attributed to it, or for failure to take reasonable measures to protect the human rights of individuals on its territory or under its jurisdiction (for example, if it allows non-State actors to violate human rights).[101] In the case of cyber operations conducted by a State that adversely affect the

[98] I Geneva Convention, Art. 19; IV Geneva Convention, Art. 18; Additional Protocol I, Arts. 11(1) and 12.
[99] Tallinn Manual 2.0, *op. cit. supra* note 6, commentary to Rule 132.
[100] 2020 Hollis Report, *op. cit. supra* note 58, p. 32.
[101] Following the criteria of the *Cyber Law Toolkit, op. cit. supra* note 46.

rights of persons outside its jurisdiction, although the current interpretation of IHRL would appear not to allow the international responsibility of the attacking State to be invoked before an international court, there are some proposals in the academic field that seek to find a way to make that possible: Milanovic, for example, proposes a model under which States have a positive obligation to protect and ensure human rights within their jurisdiction, coupled with a negative obligation to respect human rights everywhere regardless of their jurisdiction. However, for the moment it remains an academic proposal that has yet to be accepted by courts or States.[102]

5.3 Responses available to a State that has been a victim of a malicious cyber operation

International law provides for response—or so-called *self-help*—measures that may be adopted by a State affected by the conduct of another State, namely: retaliation, countermeasures, or self-defense.

5.3.1 Retaliation

Retaliation is a legal, if unfriendly, measure taken by the victim State against the responsible State. It does not interfere with the rights of the responsible State under international law. International law permits such measures, even when the activities that provoked it do not meet the threshold of being an IWA. Thus, given the difficulty of attribution in the case of cyber operations, it has been common for States adversely impacted by cyber operations to resort to retaliation which, unlike countermeasures or self-defense, does not have as a prerequisite the determination of the existence of an IWA by the attacking State.

In the Americas region, the United States reiterates the possibility for States to adopt retaliatory measures in response to a cyber operation, citing among the examples the imposition of sanctions or the declaration of a diplomatic agent as *persona non grata*.

5.3.2 Countermeasures

Countermeasures consist of a temporary non-performance of the international obligations of the State taking the measures towards the responsible State. They are envisaged and permitted under international law as a response to the IWA of the responsible State, solely in order to "induce that State to comply with its obligations."[103] The unlawfulness of non-performance in such cases is exempted because it is in response to an IWA. Countermeasures are not unlimited but may in no case affect the prohibition of the use of force, human rights obligations, humanitarian obligations prohibiting reprisals, and other obligations under peremptory norms of general international law.[104] They must be commensurate with the injury suffered, and their adoption requires prior notification to the responsible State, except in cases of urgency where countermeasures are necessary to preserve the rights of the State.[105]

Given the difficulties in attribution and the fact that countermeasures presuppose the existence of an IWA, to date, no State has framed its response to a malicious cyber operation as a countermeasure. In the American region, the United States has clarified that countermeasures in response to cyber operations are not limited to cyber measures, but that a State may also resort to non-cyber countermeasures.

Most States in other regions that have expressed their positions say that in the cyberspace domain, in certain circumstances they may be exempt from the obligation to give prior notification of countermeasures to the responsible State, due to the covert nature of cyber intrusions and the need for secrecy and cover of countermeasures or the urgency of the action. Countries such as Estonia go further, holding that even States that have not been directly impacted may use countermeasures to support the

---

[102] See, in this regard, Milanovic, M., "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015), 56 *Harvard International Law Journal* 81, 113–118; and Delerue, *op. cit. supra* note 4, pp. 263–264.

[103] Articles on State Responsibility, *op. cit. supra* note 69, Article 49.

[104] *Ibid.*, Article 50.

[105] *Idem,* Articles 51 and 52.

State directly affected, a position that has been disputed by other States that say that only the affected State may adopt them.

5.3.3 Self-defense

Under Article 51 of the Charter of the United Nations, States have "the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security".

In the cyberspace domain, it is necessary to determine whether a cyber operation can constitute an "armed attack" for the purposes of triggering that right. In that regard, most States in other regions that have clarified their positions follow the criterion of the International Court of Justice in the *Nicaragua v. United States* case, according to which the "scale and effects" must be assessed in order to to determine whether a use of force constitutes an "armed attack": according to this, only the most serious uses of force that cause death or injury to persons or damage or destruction of property will be an armed attack and therefore trigger the right to self-defense under Article 51.[106] The United States, however, takes a different position, and considers that any unlawful use of force under Article 2(4) of the Charter constitutes an "armed attack" that triggers the right of self-defense under Article 51 of the Charter. Chile, for its part, adopts a criteria approach and considers that "cyberattacks directed against its sovereignty, its inhabitants, or its physical or information infrastructure" could qualify as armed attacks.[107] Brazil recalls that the right to self-defense is triggered by the existence of an actual or imminent armed attack, with the result that there is no right to preemptive self-defense.

Cuba, for its part, rejects the automatic application of Article 51 to cyber operations and says that it *"considers unacceptable the notion that seeks to equate a cyber attack with an armed attack in an attempt to justify the supposed applicability [...] of self-defense*".[108] Guyana considers that cyber operations alone that do not involve the use of physical weaponry cannot be considered an armed attack triggering the right to self-defense.

Both Brazil and the United States recognize that the right to self-defense must be necessary and proportional. In this regard, Canada recalls that the response to an armed cyber attack can be carried out through cyber operations, while the United States holds that there is no requirement for the State to defend itself by the same means with which it was attacked, so it can respond with cyber operations or other kinetic operations. The United States calls for States to consider passive cyber defense or active defense that does not reach the threshold of the use of force to neutralize the attack or its imminent risk before resorting to measures involving force.

Finally, Brazil considers that self-defense can only be exercised against cyber operations committed by state actors, and that it cannot be in response to non-state actors unless they are acting on behalf of or under the control of a State. The United States, by contrast, says that the right of self-defense applies when the attacker is either a state actor or a non-state actor.

6. CONCLUSION

Malicious cyber operations between States are increasingly part of our daily reality, and international law must address this global challenge. In th absence of international law norms specifically governing state cyber operations, it is essential that States continue to progres in the dialogue and examination of this issue with a view eventually to reaching agreement on how existing international law norms apply to cyberspace. The pace of progress of intergovernmental processes within the framework of the United Nations over the last two decades has shown that reaching consensus on this issue involves enormous difficulties, not only in terms of divergent legal interpretations, but also in terms of political implications and disparities in the technical capacities of States.

---

[106] *Activities... op. cit. supra* note 84, para. 191.
[107] 2020 Hollis Report, *op. cit. supra* note 58, p. 38.
[108] Position of Cuba, first session of the OEWG, December 2021, *op. cit. supra* note 68.

Academic exercises, such as the Tallinn Manuals, the efforts of the ICRC, and the Oxford process, have been extremely useful in helping to guide the understanding and positions of the few States that have already formally pronounced themselves on the matter in the framework of the UN negotiations.

In the Americas, very few States have adopted a clear position on the main issues of international law whose scope is being debated. The efforts made by the OAS through CICTE and the Inter-American Juridical Committee have made a positive contribution to deepening dialogue and making positions on the matter more transparent. It is the intention of this rapporteurship that this report, together with the dialogue and training activities that have been carried out over the past two years, will serve as a useful analytical tool for all the States in our region that are in the process of drawing up their national positions on the scope of the applicability of international law to cyberspace.