A Threat to Cyber Peace Everywhere: The Problem of State Responsibility for Cyber Operations Under International Law

Pedro Borges de Carvalho[1] & Sébastien Lafrance[2]

I. Introduction

The attribution of cyberattacks to states is a key element for the construction of a legal regime capable of safeguarding peace in cyberspace, thus fostering greater stability in the international order. However, the international normative framework of state responsibility under general international law is currently inadequate to effectively govern the realm of cyber operations. This paper will delve into the pitfalls of the state responsibility legal framework in relation to cyber operations. In section II, cyberspace will be analyzed as the environment in which cyber operations occur, and as a medium upon which international law and state sovereignty have incidence. Section III will then present the international customary law of state responsibility and its structural inadequacies for the governance of internationally wrongful cyber acts.

The problem of cyber operations poses two idiosyncratic challenges to international lawyers and national security analysts. First, the advent of cyber capabilities has meant that non-state actors can easily attain military and operational powers that were once held only by states.[3] As Tim Maurer noted, cyber power in the age of global connectivity is unique because it grants the operational range of an intercontinental ballistic missile at

---

[1] Associate Researcher on Law and Tech at IDTEC – Instituto de Direito e Tecnologia. LLM candidate at KU Leuven. Law graduate from PUC-Rio.

[2] Crown Counsel (Prosecutor) at the Public Prosecution Service of Canada in the Competition Law Section. Former part-time professor of law at University of Ottawa, Canada. Former clerk for the Honorable Marie Deschamps of the Supreme Court of Canada and former in-house counsel at the Law Branch of the Supreme Court of Canada. Former clerk for the Honorable Michel Robert, Chief Judge of the Quebec Court of Appeal. Public speaker in twenty countries so far. Published several book chapters and articles in seven countries so far. Hyperpolyglot. *This work was prepared separately from this author's employment responsibilities at the Public Prosecution Service of Canada. The views, opinions and conclusions expressed herein are personal to this author and should not be construed as those of the Public Prosecution Service of Canada or the Canadian federal Crown.*

[3] Thomas Payne, *Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations*, 20 Lewis & Clark L. Rev. 683, 684 (2016).

prices affordable to individuals and small groups.[4] These non-state actors are commonly employed as proxies at varying levels of control by states, which sometimes use the far-reaching extension of cyberspace to sponsor extraterritorial operations from third countries, thus aiming to further hamper any attribution efforts.[5]

In turn, the attribution of cyberattacks constitutes a second layer of complexity in that it is technically demanding, time-consuming, and restricted to countries that are technologically advanced in cyber forensics. Robust attribution of cyber operations, even when possible, cannot be offered at the speed demanded by decision makers in national security contexts, and while some countries are improving their attribution techniques, such capabilities tend to remain asymmetric across states.[6]

Since the paradigmatic cyberattacks against Estonia in 2007, the vast majority of cyber operations publicly reported have involved, either as perpetrator or victim, the United States, Russia, and China.[7] The short recent history of formal attributions of cyber operations to states confirms this assertion and seems to reflect the asymmetric nature of cyber forensics and cyber defence capabilities throughout the international society.

On 19th July 2021, an unprecedented coalition including the United States, the U.K., the EU and all NATO members formally accused the Chinese government of being responsible for the major 2021 global hack on Microsoft email software, attributing the cyber operation to China's Ministry of State Security, which would allegedly have acted in association with criminal contract hackers.[8]

---

[4] Tim Maurer, Cyber Mercenaries: The State, Hackers and Power 26 (2018).

[5] *Id*., at 27.

[6] Maurer, *supra* note 4, at 24.

[7] Luke Chircop, *A Due Diligence Standard of Attribution in Cyberspace*, 67 International and Comparative Law Quarterly 643, 667 (2018).

[8] Eric Tucker, *Microsoft Exchange hack caused by China, US and allies say*, Associated Press (Jul. 19, 2021), https://apnews.com/article/microsoft-exchange-hack-biden-china-d533f5361cbc3374fdea58d3fb059f35. Zolan Kanno-Youngs & David E. Sanger, *U.S. Accuses China of Hacking Microsoft*, The New York Times (Jul. 19, 2021), https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html.

Few months before, in April 2021, the United States attributed the groundbreaking SolarWinds cyber espionage campaign to the Russian Foreign Intelligence Service and responded with severe sanctions.[9]

In 2020, during the first months of the COVID-19 pandemic, cyberattacks of alleged Chinese origin targeted hospitals and healthcare organizations in several Western countries,[10] as well as multiple European and U.S. supercomputers conducting research on the novel coronavirus, which had to be temporarily shut down.[11] The European Union also accused Russia and China of engaging in a deliberate disinformation campaign on the coronavirus in social networks,[12] which was intended to aggravate the health crisis in European countries by weakening confidence in public health systems.[13]

Moreover, over several years, cyber campaigns of economic espionage and intellectual property theft systematically conducted by Chinese hackers against U.S., European, and Japanese companies have resulted in hundreds of billions of dollars in losses, in what has become known as the "greatest transfer of wealth in history."[14] Five officials from Unit 61398 of the Chinese People's Liberation Army, the Chinese Army's specialized cyber

---

[9] The White House, *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government*, The White House Statements and Releases (Apr. 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

[10] Samuel Stolton, *Von der Leyen: Chinese cyberattacks on EU hospitals 'can't be tolerated'*, Euractive (Jun. 23, 2020), https://www.euractiv.com/section/digital/news/von-der-leyen-chinese-cyberattacks-on-eu-hospitals-cant-be-tolerated/. Anthony Galloway, *Coronavirus cyber attackers going after hospitals*, The Sydney Herald (May 20, 2020), https://www.smh.com.au/politics/federal/coronavirus-cyber-attackers-going-after-hospitals-20200520-p54uq3.html.

[11] Supercomputers in Germany, Switzerland, Scotland, and the United States were compromised by Chinese actors, whose goal appeared to be to steal intellectual property and public health data associated with the development of a COVID-19 vaccine, or simply to stall research in those countries. William Turton, *Hackers Target European Supercomputers Researching Covid-19*, Bloomberg (May 15, 2020), https://www.bloomberg.com/news/articles/2020-05-15/hackers-target-european-supercomputers-researching-covid-19. David E. Sanger & Nicole Perlroth, *U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks*, The New York Times (May 10, 2020), https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html.

[12] European Commission, *Coronavirus: EU strengthens action to tackle disinformation*, European Commission Press Corner (Jun. 10, 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006.

[13] Michael Peel & Sam Fleming, *EU warns of pro-Kremlin disinformation campaign on coronavirus,* Financial Times (Mar. 17, 2020), https://www.ft.com/content/d65736da-684e-11ea-800d-da70cff6e4d3.

[14] Adam Segal, The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age 8 (2d ed. 2017).

unit,[15] have been convicted in a grand jury in Pennsylvania for conspiring to hack American companies from the energy and mining sectors, and selling their trade secrets to Chinese companies between 2006 and 2014.[16]

The other rare instances in which the U.S. has attributed a cyber operation to a state include the campaign of interference in the 2016 U.S. elections, to Russia, and the 2014 Sony hack, to North Korea.[17]

For all the pressure the West's adversaries have exerted over it on the cyber front, some say it was the U.S. that was primarily at fault for sparking the arms race in cyberspace.[18] With Israel's help, the National Security Agency (NSA) has developed the "world's first cyber-weapon": the worm malware named "Stuxnet."[19] Stuxnet was a worm ("a self-replicating stand-alone malicious program")[20] capable of generating kinetic effects resulting in physical destruction.[21] Then-President Obama secretly authorized its further development and employment to fulfill its original purpose: to delay Iran's nuclear program.[22] Stuxnet infected the computer systems of the country's main uranium enrichment plant in Natanz. The malware was capable of accelerating the enrichment

[15]Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 87 (2d ed. 2017).

[16] Robert Chesney, *DOJ's Summary of the Charges in the Chinese Economic Espionage Case*, Lawfare (May 19, 2014), https://www.lawfareblog.com/dojs-summary-charges-chineseeconomic-cyberespionage-case.

[17] William Banks, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, 95 Texas L. Rev. 1487, 1492 (2017).

[18] Neta Alexander, *Did the Israeli-American Stuxnet Virus Launch a Cyber World War?*, Haaretz (Jul. 15, 2016), https://www.haaretz.com/israel-news/.premium.MAGAZINE-did-stuxnet-launch-a-cyber-world-war-1.5410099.

[19] Ellen Nakashima & Joby Warrick, *Stuxnet was work of U.S. and Israeli experts, officials say*, The Washington Post (Jun. 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[20] Yaroslav Radziwill, Cyber-Attacks and the Exploitable Imperfections of International Law xvii (2015).

[21]Marin Ivezic, *Stuxnet: the father of cyber-kinetic weapons*, CSO (Jan. 22, 2018), https://www.csoonline.com/article/3250248/stuxnet-the-father-of-cyber-kinetic-weapons.html.

[22] Nakashima & Warrick., *supra* note 5.

centrifuges above the safe speed and then directing them to abruptly slow down, causing the engines to be destroyed.[23]

For Adam Segal, the news about the Stuxnet attack on Iran's nuclear program marked 2012 as "Year Zero" in the new "hacked world order," just as 1947 represented the beginning of the Cold War. In this geopolitical order, states have launched a global competition for primacy over cyberspace.[24] The growing share of people (2.7 billion, 40% of the world's population)[25] and things (with the expansion of the Internet of Things)[26] connected to the Internet can only increase the risks implied by cyber operations. In fact, according to the World Economic Forum's latest global risks report, cybersecurity failure and IT infrastructure breakdown are among the top 10 global threats in terms of likelihood and impact.[27] The urgency of the cyberthreat stems from the perceived vulnerability of critical infrastructure,[28] and of as many other targets as can be accessed through cyberspace.

In response to high-profile cyber operations, authorities seek to reaffirm the application to cyberspace of the principle of sovereignty and public international law as a whole.[29] However, even if the content of primary norms of public international law in cyberspace were comprehensively agreed upon by states, the attribution problem would still be a consistent impediment to state accountability for internationally wrongful cyber acts.

Under general international law, the Law of State Responsibility is essentially a system of secondary norms — the general conditions under international law for a state to be

---

[23] Segal, *supra* note 14, at 2.

[24] *Id*., at 2.

[25] *Id*.

[26] Maurer, *supra* note 4, at 27.

[27] World Economic Forum, *The Global Risks Report 2021*, World Economic Forum Reports (Jan. 19, 2021), https://www.weforum.org/reports/the-global-risks-report-2021.

[28] World Economic Forum, *Wild Wide Web: Consequences of Digital Fragmentation*, World Economic Forum Reports (Jan. 15, 2020). https://reports.weforum.org/global-risks-report-2020/wild-wide-web/?doing_wp_cron=1594525606.2813379764556884765625.

[29] See, for instance: Dapo Akande, Duncan Hollis, Harold Hongju Koh & James O'Brien, *Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector,* EJIL:Talk! (May 21, 2020), https://www.ejiltalk.org/oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-health-care-sector/.

held responsible for internationally wrongful acts, and the consequences of such responsibility — as opposed to primary norms — the substantive norms (whether customary or conventional) that establish the content of a given state's international obligations.[30]

The Law of State Responsibility has been the object of progressive development and codification efforts by the UN International Law Commission (ILC), culminating in the 2001 Draft Articles on Responsibility of States for Internationally Wrongful Acts. Under this instrument, an "internationally wrongful act" is defined as a commission or omission of conduct that (i) constitutes a violation of an international obligation of the state and (ii) is attributable to the state under international law.[31] Respectively, the first element is analyzed under primary norms of international law and the second element under secondary norms.

This paper is structured with a focus on secondary norms of state responsibility for cyber operations and is not concerned with the substantive content of international obligations in cyberspace. It will attempt to demonstrate how cyber operations are particularly difficult to attribute to sponsoring states under the already extremely stringent rule of attribution enshrined in Article 8 of the Draft Articles, and argue it is dysfunctional in governing the realm of cyberspace.

II. The Cyberspace

II. 1. Cyberspace and Cyber Operations

The term "cyberspace" was coined by writer William Gibson, who first employed it in his science fiction story "Burning Chrome," published in 1982. Gibson created the word by observing computer users and videogame players that appeared to him to have developed "a belief that there is some kind of actual space behind the screen, some place that you cannot see but you know is there."[32]

---

[30] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (2001), general commentary (1).

[31] *Id.,* Art. 2.

[32] Sue Barnes, *Cyberspace: Creating paradoxes for the ecology of self*, *In*: Lance Strate et al (eds.), Communication and Cyberspace 195 (1996). *Apud*: Nicholas Tsagourias, *The Legal Status of Cyberspace, In*: Nicholas Tsagourias &, Russell Buchan Cheltenham (eds.), Research Handbook on International Law and Cyberspace 22 (2015).

Striving for a working legal definition, Kriangsak Kittichaisaree defines Cyberspace as "the man-made environment or space where electronic communication over interconnected networks of information and communications infrastructure, including the Internet, telecommunications networks, and computer systems, occurs."[33]

More recently, the 2020 Oslo Manual on Select Topics of the Law of Armed Conflict, when defining cyber operations as "operations that employ capabilities aimed at achieving objectives in or through cyberspace" in its Rule 20, incidentally defined Cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[34]

The question of whether and how international law governs cyberspace, as has been the case with other frontiers in human history such as outer space and the deep seabed,[35] has been the object of much debate.

II.2 Public International Law in the Cyberspace

In the absence of international treaties regulating cyber operations, two bodies of experts have played a leading role in clarifying the international law applicable to cyberspace. The instruments developed by these groups are central to the study of public international law in cyberspace, which is why this section focuses primarily on them.

II.2.1 The United Nations Group of Governmental Experts (GGE) on Advancing responsible State behavior in cyberspace in the context of international security

The Group of Governmental Experts was originally established in 2020 by the UN General Assembly, which requested the Secretary-General to establish a group of experts with a mandate to produce reports on international concepts for strengthening the security

[33] Kriangsak Kittichaisaree, Public International Law of the Cyberspace 2 (2017).

[34] Y. Dinstein & A. W. Dahl, Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary 19 (2020).

[35] Scott J. Shackelford, *The Future of Frontiers*, 23 Lewis & Clark L. Rev. 1331-1384 (2020).

of global information and telecommunications systems.[36] The GGE consists of a select number of experts appointed on a geographically equitable basis and adopts reports only by consensus.

The first group of experts did not achieve consensus, but a second group was convened in 2009. This group, benefiting from the awareness of the risk of interstate conflict raised by the 2007 Russian cyberattacks on Estonia and the Russian cyber-operations campaign against Georgia during the 2008 armed conflict, successfully submitted a first report with preliminary findings, noting that states were developing ICTs as instruments of war and intelligence for political purposes.[37] The 2010 report also pointed to the risks of instability entailed by the uncertainty about the parameters of attribution in cyberspace, as well as a lack of common understanding about rules of conduct.[38]

In its 2013 and 2015 reports the Group affirmed the applicability of existing general international law to the activities of states in cyberspace, in particular the UN Charter in its entirety, offering basic non-binding normative guidance for state behavior in cyberspace.[39]

After a failed attempt at reaching a consensus report in 2017,[40] the GGE successfully submitted a consensus report at the end of its 2019/2021 session, which built upon the rules set forth by the previous reports. Notably for the purposes of this piece, at paragraph 71(g), it reads: [41]

---

[36]United Nations General Assembly, A/Res.56/19 (2020), https://www.un.org/ga/search/viewm_doc.asp?symbol=A/RES/56/19(2020).

[37] Anders Henriksen, The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace, 5 Journal of Cybersecurity 1, 2 (2019).

[38] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Consensus Report A/Res/65/2001 (2010).

[39] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Consensus Report A/Res/70/174 (2015).

[40] Henriksen, *supra* note 37, at 3.

[41] Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (Advance Copy),* United Nations (May 28, 2021), https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

> "The Group reaffirms that States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. It also reaffirms that States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts. At the same time, the Group recalls that the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient to attribute the activity to that State; and notes that accusations of organizing and implementing wrongful acts brought against States should be substantiated. The invocation of the responsibility of a State for an internationally wrongful act involves complex technical, legal and political considerations."

Although the consensus reports of the Group of Governmental Experts are an evident source of ***opinio juris*** indicative of international customary law on the basic issue of applicability of the UN Charter to cyberspace, the only persuasive and comprehensive instrument to which one can currently turn for a detailed attempt at codifying the international law applicable to cyber operations is the Tallinn Manual 2.0.

II.2.2 The Tallinn International Group of Experts

The Tallinn Manual on the International Law Applicable to Cyber Warfare was published in 2013, after 4 years of work by an international group of independent experts convened at the invitation of the NATO Cooperative Cyber Defense Center of Excellence (NATO CCD COE). A new international group of experts reconvened to update the Manual, also including rules applicable in peacetime. The result was the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

The Tallinn Manual 2.0 is aimed primarily at state legal advisors. The Manual seeks to codify, in an objective manner, existing international law (***lex lata***) from the point of view of the International Group of Experts, as reviewed by individuals in relevant government positions. The positions of NATO or the states or organizations that any of the members or observers of the International Group of Experts are affiliated with should not be

understood as reflected in the Manual, which expresses only the individual positions of the Experts.[42]

Therefore, strictly speaking, the Manual would fit into the roster of sources of public international law under Article 38 of the Statute of the International Court of Justice as "teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law," [43] and cannot *per se* be taken as a source of *opinio juris*. However, being on par with other eminent manuals of war such as the 1880 Oxford Manual on the Laws of War on Land and the 1994 San Remo Manual on the International Law Applicable to Armed Conflicts at Sea, one can expect considerable deference to the Tallinn Manual 2.0. In times of normative paucity, this type of non-binding instrument can guide state practice toward the development of international custom, or even influence the drafting of an international treaty on the subject along its lines.[44]

II.3 Sovereignty in Cyberspace

It is well established that the Sovereignty Principle applies to cyberspace. More specifically, states may exercise sovereignty over cyber infrastructure located in their territories and over activities related to them.[45] This is a consensus under state practice, as codified by the Tallinn Manual and the United Nations GGE.[46]

It is important to discern that sovereignty over cyber infrastructure does not imply sovereignty over cyberspace itself.[47] The Tallinn Manual expresses the position that no

[42] Schmitt, *supra* note 15, at 2-3.

[43] International Court of Justice, Statute of the International Court of Justice Art. 38(d) (1945).

[44] Geoffrey S. Corn et al, The Law of Armed Conflict: An Operational Approach 59 (2012).

[45] Schmitt, *supra* note 15, at 11-12, 18-19.

[46] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Consensus Report A/68/98 (2013), para. 20; Consensus Report A/Res/70/174 (2015), para. 27.

[47] Radziwill, *supra* note 20, at 101.

state can claim sovereignty over cyberspace per se, as a substantial part of the infrastructure that underpins cyberspace is in the sovereign territory of other states.[48]

But what about exercising sovereignty over only a specific part of cyberspace? On this point states differ. The concept of cyberspace freedom advocated by the United States characterizes cyberspace as a global common in its integrity and repudiates the creation of isolated alternatives to the internet.[49] In contrast, there are countries that seek to create a national intranet entirely detached from the World Wide web and under complete state control.[50] Such is the case with Iran's National Informational Network, dubbed the "Halal Internet,"[51] and North Korea's infamous Kwang Myong Network.[52]

III. State Responsibility for Internationally Wrongful Cyber Acts

III.1 The Tallinn International Group of Experts' position: applying the ILC Articles on State Responsibility rules of attribution to cyberspace

The International Group of Experts established that the customary law of state responsibility, consisting of secondary rules of international law, undeniably extends to cyber operations.[53] Accordingly, the Group drew extensively on the ILC Articles in drafting the Tallinn Manual's rules on international state responsibility,[54] essentially translating them to the cyberspace context.

It will be examined how the cyber environment challenges the effectiveness of the traditional modes of attribution enshrined in the Articles.

---

[48] Schmitt, *supra* note 15, at 13.

[49] Radziwill, supra note 20, at 94.

[50] *Id.* at 105.

[51] Jon Gambrell, *Iran deploys 'halal' internet in latest bid to rein in citizens' web freedoms*, Independent (Jan. 29, 2018), https://www.independent.co.uk/news/world/middle-east/iran-halal-internet-national-information-network-web-freedoms-citizens-access-social-media-telegram-a8182841.html.

[52] Martyn Williams, *A peek inside North Korea's intranet*, North Korea Tech (Jul. 6, 2015), https://www.northkoreatech.org/2015/07/06/a-peek-inside-north-koreas-intranet/.

[53] Schmitt, *supra* note 15, at 80.

[54] *Id*., at 79.

III.2 The shortcomings of the ILC Draft Articles for attribution in cyberspace

While the attribution standards of the International Law Commission's Articles on State Responsibility reflect the general normative framework on state responsibility, they are clearly insufficient to address the inherent problems of cyber operations.[55] The International Group of Experts notes in the Tallinn Manual much of the practical challenges of conforming the Articles to cyberspace, without, however, suggesting structural changes in order to adapt the applicable attribution rules.[56]

This section aims to present the landscape of unique challenges that the disruptive nature of cyberspace and its unique architecture pose to traditional rules of attribution.

III.2.1 An Introduction to the Structural Peculiarities of Cyberspace

Beyond the monitor separating the realm of the physical from the virtual, operations occur in unique — sometimes tortuous, confusing — ways, and rules of the traditional legal order need to adapt accordingly in order to regulate them.

This world of numbers and codes is a prolific realm for technically savvy actors, where anonymity is easily attainable, and cybernetic games of mirrors and smokescreens are recurring. Attribution in cyberspace is, and will remain for the foreseeable future, a huge technical problem.[57] In essence, this is due to the obsolescence of the cyberspace infrastructure, whose architecture dating back to 1982 was designed for a small number of trusted researchers, not for the number of 2 billion users currently active on the Internet.[58] Consequently, the volume of cyberthreats today far exceeds the cybersecurity that its Internet Protocol (IP) and Transmission Control Protocol (TCP) foundation was designed to support.[59]

---

[55] Payne, *supra* note 3, at 715.

[56] Schmitt, *supra* note 15, at 87-94.

[57] S.J. Shackelford & R.B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 Georgetown Journal of International Law 971, 983-984 (2011).

[58] Shackelford & Andres, supra note 57, at 982.

[59] *Id*.

Tracing the perpetrator of a cyberattack involves two levels of technical hurdles: identifying the computer (or computers) from which the operation was launched and identifying the person who operated the computer.[60]

In cyber forensics, the primary method for identifying the computer of origin of a given threat is to verify its unique IP number. However, hackers have a myriad of techniques to hinder the operation of IP number locator programs.[61]

For example, operators sometimes employ IP Spoofers, programs that forge an IP address to hide the identity of the offenders, impersonate a trusted host, or create the illusion that the cyberattack was launched from a different location.[62] In this way, spoofing allows hackers to act under the guise of a specific state or organization, deliberately promoting the misattribution of their crime to the one whose IP they have spoofed.

Moreover, even without utilizing IP spoofing, malicious operators can use simple means to deceive victims as to their real identity, even if temporarily, by posing as other organizations: these are "false flag" operations. In April 2015, a few months after the terrorist attacks on Charlie Hebdo, a "false flagging" tactic was employed in an international cyber operation against the French broadcaster TV5 Monde. Hackers identifying themselves as the "Islamic State Cyber Caliphate" posted ISIS jihadist propaganda on TV5's Twitter and Facebook accounts, and knocked all 12 of its channels offline for more than eight hours.[63] The attack consisted of a sophisticated process of system corruption that narrowly failed to permanently destroy the station's entire IT infrastructure.[64] Despite the attempt to impersonate ISIS members, French authorities determined two months later that the attack had in fact been carried out by Russian hackers, and technical forensics attributed the operation with "medium confidence" to the

---

[60] Chircop, *supra* note 7, at 646.

[61] Shackelford & Andres, *supra* note 57, at 982.

[62] Radziwill, *supra* note 20, at 327.

[63] Segal, *supra* note 14, at 14.

[64] Gordon Corera, *How France's TV5 was almost destroyed by Russian hackers*, BBC News (Oct. 10, 2016), https://www.bbc.com/news/technology-37590375.

GRU (the military intelligence service of the Russian Federation).[65] It is speculated that this was a test of new types of cyberattacks by Russia.[66]

The modern hacker's arsenal is vast. Using certain Trojan malware, hackers can infect other computers and launch cyberattacks from a network of "zombie botnets," such as large spam campaigns with spambots, or distributed denial-of-service (DDoS) attacks. DDoS attacks are ordinarily launched to prevent legitimate users from accessing a particular system, but more complex DDoS can coopt huge networks of zombie botnets (potentially millions of computers) to attack servers from multiple locations and in multiple ways.[67]

As an illustration of this type of threat, the International Group of Experts cites an operation attributed to North Korea in 2013 in which thousands of South Korean servers and computers in the financial and media sectors were shut down. This attack came from IT infrastructure located in several countries, none of which appear to have been involved in the operation.[68]

In the Tallinn Manual this incident is evoked to suggest the inadequacy of the territoriality of coopted private cyberinfrastructure as a criterion for attribution to a state.[69] This observation is based on the impossibility, as a rule, to identify with sufficient certainty the individual who used the machine in the cyberattack only according to the location of the computer. This challenge is known as the "human machine gap."[70]

Therefore, as far as evidentiary matters are concerned, even the identification of a particular computer particularly indicative of state involvement is insufficient for conclusive attribution if the identification of its user in the instance of the cyberattack in question is also absent.

---

[65] Maurer, *supra* note 4, at 24.

[66] Segal, supra note 14, at 14.

[67] Radziwill, *supra* note 20, at 328.

[68] Schmitt, *supra* note 15, at 91.

[69] *Id*.

[70] R. Geiβ & H. Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention*, *In*: Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace 625 (2013). *Apud*: Luke Chircop, *A Due Diligence Standard of Attribution in Cyberspace*, 67 International and Comparative Law Quarterly 643, 646 (2018).

Finally, cyber forensics aside, attribution in cyberspace faces yet another layer of legal complexities: the level of sufficient certainty under the applicable normative parameter. But this difficulty is not unique to the cyber realm — any effort of state accountability for the conduct of non-state actors will find a barrier in the rigid criteria of customary international law. However, the distinctive challenges of attribution in cyberspace, concerning the identification of the computers of origin of an operation and the individuals responsible, considerably magnify the limitations of the existing international legal framework.[71]

III.2.2 Proxies in Cyberspace

To develop effective norms for the governance of cyberspace, it is necessary to address international accountability for the operations of non-state actors, a characteristic problem in the cyber context.[72]

The category of "non-state actors" refers to both individuals and groups (whether or not hierarchical, organized, or having legal personality under domestic law), and in the realm of cyberspace includes independent hacker groups, criminal organizations perpetrating cybercrimes, corporations, insurgent groups, and cyber terrorists.[73]

In effect, the absence of an adequate normative framework for holding these actors accountable poses a danger to international peace and security to the extent that, in addition to the threat of sophisticated independent hackers, states can cooperate to varying degrees with non-state actors, and thereby evade accountability or lawful retaliation for unlawful cyber campaigns with extraterritorial effects.[74]

Therefore, among the modes of attribution under customary international law, we will restrict ourselves to those most commonly invoked to address this type of threat, in order to demonstrate the incipiency of even the (hypothetically) most useful legal instruments under the law of international responsibility.

---

[71] Chircop, *supra* note 7, at 647.

[72] *Id.*

[73] Schmitt, *supra* note 15, at 95.

[74] Banks, *supra* note 17, at 12.

In its rules 15 to 18, the Tallinn Manual transposes to the cyber context articles 4 to 11 of the ILC's Articles on State Responsibility. Of these, most relevant for the purposes of this paper is Article 8, on the attribution of wrongful acts perpetrated by non-state actors following the instructions of a state, or under state direction or control. Article 8 has been referred to by the International Court of Justice as reflective of customary international law.[75]

Article 8 establishes two modes of attribution. The first deals with private entities that commit internationally wrongful acts on the *instructions* of the state.[76] Cases of this kind typically involve the recruitment of private actors ("volunteers," "patriots") by state agencies to act as auxiliaries, while outside the official government structure.[77] The second is the *direction and control* mode. Under this mode, the conduct of a non-state actor that has been specifically directed by a state shall be attributable to the latter.[78]

The applicable *effective control* test under article 8 is considerably stringent, and has not ever been met in the cases involving paramilitary groups before the International Court of Justice.[79] For the actions of a non-state actor to be attributed to a state under the effective control test, the Court requires that effective control be demonstrated in "each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the people or groups of people having committed the violations."[80] The Court has also noted that this is the applicable test regardless of the nature of the wrongful act, unless in the presence of a "clearly expressed *lex specialis*."[81]

---

[75] Application of the Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. (February 26) (Merits, Judgment), paras. 398, 406.

[76] International Law Commission, *supra* note 30, Art. 8, commentary (1).

[77] *Id*., commentary (2).

[78] *Id*., commentary (3).

[79] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 65 (June 27) (Merits, Judgment); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 226 (Dec. 19) (Merits, Judgment); Application of the Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. 215 (February 26)(Merits, Judgment).

[80] Application of the Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. (February 26) (Merits, Judgment), para. 400.

[81] *Id*., para. 401.

In order to answer whether this attribution criterion is adequate to address international illicit conduct in cyberspace, one must first understand the phenomenon of "patriotic hackers." Operating similarly to other hackers, this category is characterized by acting with political objectives, either on behalf of a state interest or as a response to an offense to the nation,[82] whose operations entail questions of state responsibility to the extent that there is confluence between state interests and the targets of such patriotic hacker groups, as well as evidence of coordinated or subordinated action.[83]

In 2007, Estonia faced violent protests and looting by its ethnically Russian population, allegedly orchestrated by the Russian Federation over the removal of a Soviet monument from downtown Tallinn.[84] In Moscow, the Estonian embassy was attacked by pro-Kremlin youth groups.[85] In tandem with the clashes, during three weeks, Estonian government, corporate and bank websites were targeted by distributed denial of service (DDoS) attacks conducted through botnets, being defaced to display Russian political propaganda, and resulting in losses of 750 million euros.[86] At the time, instructions on how, when and against which targets to launch such attacks were disseminated on several Russian language websites.[87] Estonia made formal requests to Russia to help it contain the cyberattacks, and then to investigate their authorship, both of which were denied. Two years later, a pro-Kremlin youth group called Nashi, instrumental in pro-Putin propaganda campaigns, claimed to have orchestrated the cyberattacks.[88]

Would it be possible to attribute Nashi's operations against Estonian cyberspace to the Russian Federation under Article 8? Nashi was created by the Kremlin to contain potential anti-government youth movements in Russia. It has considerable ties to the Russian

---

[82] Payne, *supra* note 3, at 706.

[83] *Id.,* at 707.

[84] Trevor McDougal, *Establishing Russia's Responsibility for Cyber-Crime Based on its Hacker Culture*, 11 Brigham Young University International Law & Management Review 55, 61 (2015).

[85] Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Cooperative Cyber Defence Centre of Excellence (2008), https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[86] McDougal, *supra* note 84, at 61.

[87] Ottis, *supra* note 85.

[88] McDougal, *supra* note 83, at 62.

government in financial, political, and leadership terms. However, existing evidence of government support does not imply effective state control, as Nashi appears to retain a significant margin of autonomy.[89] Therefore, it has been concluded that the factual link between Nashi and the Russian Federation is comparable to that between the Nicaraguan Contras and the United States: a non-state group largely funded and supported by the state, but not strictly controlled by it insofar as that, in retaining some operational autonomy, they cannot be found to be under "effective control."[90] Thus, in accordance with the International Court of Justice's jurisprudence, the cyberattacks orchestrated by Nashi in 2007 would most likely not be successfully attributed to Russia under the effective control test, despite its evident and substantial involvement in the operations.

Such incidents demonstrate how even in cases of strong indicia of state involvement, unlawful cyber activities sponsored by states are largely found on the margin of any applicable international law, due to the unrealistically high evidentiary threshold the general law of state responsibility demands for any wrongful act, including, currently, cyber operations. In this sense, the law seems blind to the strategic use of proxies by states in illicit cyber operations, which, even more than conventional military operations, offer further technological means for obscuring the identity of perpetrators and associated entities, such as sponsoring states themselves.

IV. Conclusion

The International Group of Experts suggests contextual analysis of the concrete case as the best tool for accurate attribution of cyber operations under the Articles of the International Law Commission. In this sense, indicia contrary to state involvement in a given hack would be a friendly relationship between the countries involved, as well as the existence of a history of cooptation of state computers by non-state actors (supported by reliable intelligence or a repeated pattern).[91]

---

[89] Payne, *supra* note 3, at 707.

[90] *Id.*

[91] Schmitt, *supra* note 15, at 92.

However, these interpretative guidelines may not be enough to ensure swift attribution in all circumstances, potentially making it impossible for the target state to employ countermeasures in response to unlawful cyber operations.[92]

This paper has thus joined other authorities in pointing to the rigidity and inadequacy of Article 8 under the law of state responsibility in the context of cyber operations and suggests that a *lex specialis* for attribution is warranted. That it *can* emerge under the general law of state responsibility is well known,[93] as this is provided for by ILC's Draft Article 55, which establishes that the "articles do not apply where and to the extent that the conditions for the existence of an internationally wrongful act or the content or implementation of the international responsibility of a State are governed by special rules of international law."[94]

However, the prospect of a special rule of attribution that is more favorable for holding states accountable for fostering threats against international cyber peace arising seems improbable, as several states seem to find that it is in their best strategic interest to keep pursuing "irresponsible behavior" in cyberspace against their geopolitical adversaries.

[92] Chircop, *supra* note 7, at 645.

[93] *Id.,* at 660.

[94] International Law Commission, *supra* note 30, Art. 55.