INTERNATIONAL LAW STUDIES
Published Since 1895

Application of the Due Diligence Principle to Cyber Operations

Tomohiro Mikanagi

97 INT'L L. STUD. 1019 (2021)

Volume 97

2021

Published by the Stockton Center for International Law

ISSN 2375-2831

Application of the Due Diligence Principle to Cyber Operations

Tomohiro Mikanagi *

CONTENTS

* Deputy Director-General, International Legal Affairs Bureau, Ministry of Foreign Affairs of Japan. This paper is based on a presentation at the Stockton Center for International Law's three-day conference on Disruptive Technologies and International Law, December 7–9, 2020. The views expressed herein do not represent the official position of the Japanese government nor are they necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

Over the last several years governments have been attributing malicious cyber operations to certain actors, including State organs.[1] On December 19, 2017, the UK Foreign Office Minister Lord Ahmad of Wimbledon attributed the WannaCry ransomware incident to the "Lazarus Group."[2] On the same day, U.S. Homeland Security Advisor Tom Bossert briefed the press:

> After careful investigation, the United States is publicly attributing the massive WannaCry cyberattack to North Korea. . . . We're comfortable in this case, though, that it was directed by the government of North Korea. We're also comfortable in saying that there were actors on their behalf, intermediaries, carrying out this attack, and that they had carried out those types of attacks on behalf of the North Korean government in the past.[3]

On February 15, 2018, Lord Ahmad attributed the NotPetya cyber incident targeting Ukraine to the Russian government: "The UK government judges that the Russian government, specifically the Russian military, was responsible for the destructive NotPetya cyber-attack of June 2017. The attack showed a continued disregard for Ukrainian sovereignty."[4]

More recently, on July 16, 2020, the United Kingdom, the United States, and Canada jointly published an advisory that attributed cyber espionage targeting COVID-19 vaccine development to "Advanced Persistent Threats

1. Florian J. Egloff & Andreas Wenger, *Public Attribution of Cyber Incidents,* 244 CENTER FOR SECURITY STUDIES ANALYSES IN SECURITY POLICY 1 (2019).

2. Press Release, UK Foreign and Commonwealth Office, Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks (Dec. 19, 2017), https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

3. Press Briefing, White House, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (Dec. 19, 2017), https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

4. News Story, UK Foreign and Commonwealth Office, Foreign Office Minister Condemns Russia for NotPetya Attacks (Feb. 15, 2018), https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

(APT) 29."[5] The advisory stated: "The United Kingdom's National Cyber Security Centre (NCSC) and Canada's Communications Security Establishment (CSE) assess that APT29 is a cyber espionage group, almost certainly part of the Russian intelligence services. The U.S. National Security Agency (NSA) agrees with this attribution and the details provided in this report." Following the joint advisory, the UK Foreign Secretary condemned Russian intelligence services for targeting those working to combat COVID-19.[6]

These statements referred to attribution, but, except for the brief reference to sovereignty in Lord Ahmad's statement on NotPetya, they did not refer to the primary rules of international law. Article 2 of the International Law Commission's Articles on State Responsibility clarifies the two elements constituting internationally wrongful acts: "There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State."[7]

These elements present two challenges for States seeking to invoke State responsibility for cyber operations. First, it is not always clear if a particular cyber operation constitutes a breach of an international obligation to the targeted State.[8] Second, while the Articles on State Responsibility clarify the

5. UK National Cyber Security Centre, Advisory: APT29 Targets COVID-19 Vaccine Development (July 16, 2020), https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF.

6. Press Release, UK Foreign and Commonwealth Office, UK Condemns Russian Intelligence Services Over Vaccine Cyber Attacks (July 16, 2020), https://www.gov.uk/government/news/uk-condemns-russian-intelligence-services-over-vaccine-cyber-attacks.

7. International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, 56 U.N. GAOR Supp. No. 10, art. 2, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm'n 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), https://legal.un.org/ilc/texts/instruments/english/draft_articles/ 9_6_2001.pdf [hereinafter Articles on State Responsibility].

8. There is ongoing debate over the relationship between the violation of sovereignty and non-intervention. *See* Harriet Moynihan, *The Application of International Law to State Cyberattacks Sovereignty and Non-Intervention,* CHATHAM HOUSE (Dec. 2, 2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks; Przemyslaw Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, THE HAGUE PROGRAM FOR CYBER NORMS (Mar. 2020), https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views; Michael N. Schmitt, *Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention*, 96 INTERNATIONAL LAW STUDIES 554 (2020).

rules concerning attribution to States, it does not deal with the issue of proof,[9] and it is not clear to what extent the attribution has to be proven.

This article addresses the second of these two challenges. It will first reappraise the difficulty in attributing cyber operations to States in Part II. As will be discussed, States' discreet use of proxies renders the proof of attribution to States technically challenging.[10] On the other hand, the due diligence principle, if applicable, does not require attribution but can lead to the invocation of State responsibility for cyber operations emanating from the territory of other States. In the *Corfu Channel* judgment, the International Court of Justice (ICJ) recognized "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[11] This obligation originates from the concept of territorial sovereignty, which Max Huber clarified in the *Island of Palmas* case.[12] The *Corfu Channel* judgment referred to this obligation in general terms, and UN Member States have agreed that existing international law applies to cyber operations.[13] However,

9. Articles on State Responsibility, *supra* note 7, at 54, 72.

10. *See* the NATO Cooperative Cyber Defence Centre of Excellence's *International Cyber Law in Practice: Interactive Toolkit,* https://cyberlaw.ccdcoe.org/wiki/Main_Page (last visited July 22, 2021). The toolkit presents various scenarios involving non-State actors. Among the nineteen scenarios, "Scenario 14: Ransomware campaign" seems to be particularly relevant to the issues addressed in this article, and "Scenario 6: Cyber countermeasures against an enabling State" is also relevant for the analysis of the due diligence obligation. For the definition and categorization of "proxies," see Tim Maurer, "*Proxies" and Cyberspace*, 21 JOURNAL OF CONFLICT & SECURITY LAW 383 (2016). *See also* Nicholas Tsagourias & Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 EUROPEAN JOURNAL OF INTERNATIONAL LAW 941 (2020) (makes several very interesting proposals, including the revision of the legal determinants of attribution).

11. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

12. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 839 (Perm. Ct. Arb. 1928) ("Territorial sovereignty . . . involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States."). *Tallinn Manual 2.0* refers to the extension of this obligation to cases outside the territory of a State but under its control. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS r. 6, at 32–33 (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0]. This article will focus on States' obligations concerning cyber operations emanating from their territories without prejudice to the existence of such extraterritorial obligation.

13. Paragraph 19 of the 2013 UNGGE report stated: "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." 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.

UN members have not yet agreed on whether the due diligence obligation applies to cyber operations. Based on the reappraisal of the difficulty in the proof of attribution in Part II, Part III examines the application of the due diligence principle to cyber operations as an alternative path to State responsibility.

II. DIFFICULTY IN THE PROOF OF ATTRIBUTION TO STATES

Paragraph 71(g) of the 2021 Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UNGGE) states:

> [T]he Group recalls that the indication that an ICT [information and communication technology] activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself 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.[14]

Attribution statements made by government officials tend to be ambiguous about the evidence for the attribution. However, the 172-page criminal complaint affidavit from a special agent of the Federal Bureau of Investigation in the *Park Jin Hyok* case, which accuses Mr. Park of being a member of a conspiracy behind many cyber incidents, filed with a U.S. District Court in June 2018, was relatively detailed.[15] While the affidavit is not aimed at the attribution of cyber operations to North Korea, it asserted that Mr. Park and

---

A/68/98 (June 24, 2013) [hereinafter 2013 UNGGE Report]. Paragraph 24 of the 2015 UNGGE report confirmed this statement. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 24, U.N. Doc. A/70/174 (July 22, 2015); G.A. Res. 70/237 (Dec. 30, 2015) [hereinafter 2015 UNGGE Report] (the 2015 report was adopted by consensus).

14. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, ¶ 71(g) (May 28, 2021), https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf [hereinafter 2021 UNGGE Report].

15. Criminal Complaint, United States v. Park Jin Hyok, No. MJ 18-1479 (C.D. Cal. June 8, 2018), https://www.justice.gov/opa/press-release/file/1092091/download [hereinafter Affidavit].

his accomplices were working "on behalf of" the North Korean government.[16]

This affidavit explains connections among e-mail accounts, internet protocol (IP) addresses, and social networking service accounts involved in cyber operations such as the operation against Sony Pictures Entertainment in 2014, the operation against the Bangladesh Bank in 2016, and the WannaCry incident in 2017. It also explains that programs used in these operations had strong similarities, indicating a common author. The affidavit also points out connections between the addresses and accounts used in these operations and those used by the suspect, Mr. Park. For example, an e-mail account used in operations against Sony Pictures Entertainment and the Bangladesh Bank was registered by someone using an e-mail account that shared a large encrypted data box with an e-mail account used by Mr. Park.[17] According to the affidavit, many of the operations were launched from common North Korean IP addresses.[18] It argues that using a common IP address typically indicates the use of shared or common computer infrastructure or the same physical space to connect to the internet.[19] If all the evidence al-

16. *Id.* ¶ 6.

17. *Id.* ¶ 291.

18. Paragraph 28 of the affidavit explains that "North Korean IP addresses" means IP addresses registered to a company in Pyongyang and those registered to a company in China but leased or used by North Korea. Paragraph 36 says that the subjects have used North Korean IP addresses to engage in malicious and non-malicious activity. Paragraph 37 refers to eight IP addresses (#1 to #8) and says that activity originating from the North Korean IP addresses #3 and #7 has been linked to both malicious activity as well as use by subjects to access their personal accounts, including Chosun Expo accounts. It also says that activity originating from the North Korean IP addresses #4 and #8 has been linked to some of these same subjects using the IP address #7 to access the Chosun Expo accounts, including using their true names. E-mail accounts associated with Chosun Expo used by Mr. Park were accessed from the North Korean IP address #7. *Id.* ¶¶ 307, 314.c, 320, 330. The same IP address was used for malicious cyber operations. *Id.* ¶¶ 207, 209, 307, 333.

19. *Id.* ¶ 26.

leged in the affidavit is accepted, then the information technology (IT) infrastructure[20] used in the cyber operations and the perpetrators of the operations would be largely established.[21] The affidavit also refers to North Korea's relationship with the network. However, multiple layers of aliases and other intricate concealing techniques render it difficult to obtain evidence proving its connection to the actual cyber operations.

Paragraph 28(e) of the 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security refers to the use of proxies as follows: "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."[22]

A State conspiring to conduct malicious cyber operations but hoping to hide its involvement would use a person or group of persons ostensibly not working for it. "Proxy" here means a person or group of persons used by a State for hiding its involvement. The most relevant of the Articles on State Responsibility relating to attribution applicable to cyber operations using proxies seems to be Article 8, which provides: "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[23]

Article 8 refers to instruction, direction, or control. These terms are not clearly defined, but the article seems to require specificity concerning the State's influence over the conduct in question. In the 2007 *Bosnian Genocide* judgment, the ICJ said, after quoting the *Nicaragua* judgment, "It must however be shown that this 'effective control' was exercised, or that the State's instructions were given, in respect of each operation in which the alleged

20. IT infrastructure here means "All of the hardware, software, networks, facilities etc. that are required to Develop, Test, deliver, Monitor, Control or support IT services. The term IT Infrastructure includes all of the Information Technology but not the associated people, Processes and documentation." ITIL V3 Foundation Course Glossary, https://itil.it.utah.edu/downloads/ITILV3_Glossary.pdf (last visited July 22, 2021).

21. For more detailed analysis of the affidavit, see Tomohiro Mikanagi & Kubo Mačák, *Attribution of Cyber Operations: An International Law Perspective on the* Park Jin Hyok *Case,* 9 CAMBRIDGE INTERNATIONAL LAW JOURNAL 51 (2020).

22. 2015 UNGGE Report, *supra* note 13. This view is reaffirmed in paragraph 71(g) of the 2021 UNGGE Report, *supra* note 14.

23. Articles on State Responsibility, *supra* note 7, art. 8.

violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations."[24]

In rejecting the International Criminal Tribunal for the former Yugoslavia's Appeals Chamber's application of the "overall control" test, the ICJ said:

> [A] State's responsibility can be incurred for acts committed by persons or groups of persons—neither State organs nor to be equated with such organs—only if, assuming those acts to be internationally wrongful, they are attributable to it under the rule of customary international law reflected in Article 8 . . . . This is so where an organ of the State gave the instructions or provided the direction pursuant to which the perpetrators of the wrongful act acted or where it exercised effective control over the action during which the wrong was committed.[25]

The International Law Commission's commentary on Article 8 of the Articles on State Responsibility also made clear that the instructions, direction, or control must relate to the conduct that is said to have amounted to an internationally wrongful act.[26]

Evidence showing the use of various components of IT infrastructure, including IP addresses, e-mail accounts, and devices, and evidence showing similarities among programs used in cyber operations may be sufficient to prove the existence of a network comprising two elements of cyber operations: (1) the IT infrastructure and (2) the person or group of persons. However, the use of proxies hidden by aliases and intricate concealing techniques makes it difficult to collect direct evidence proving instruction, direction, or control by a State regarding specific operations. Therefore, in proving the attribution to a State, reliance on indirect and circumstantial evidence will be inevitable.

With regard to acceptable evidence for the proof of attribution, the 1949 *Corfu Channel* judgment said that, when the victim State is unable to present direct proof due to the exclusive territorial control by the respondent, such a State "should be allowed a more liberal recourse to inferences of fact and

---

24. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶ 400 (Feb. 26).

25. *Id.* ¶ 406.

26. Articles on State Responsibility, *supra* note 7, at 48.

circumstantial evidence,"[27] and that indirect and circumstantial evidence is to be accorded "special weight" when it is based on a series of facts which are linked together and lead logically to a single conclusion.[28] In addition, this judgment indicated the relationship between the gravity of charges and the standard of proof.[29] In her separate opinion in the 2003 *Oil Platforms* judgment, Judge Higgins referred to a general agreement that graver charges require a higher standard of proof.[30] This should also mean that less serious charges would require a lower standard of proof.[31]

For example, the violation of sovereignty might not be as serious as the use of force or genocide, and evidence on the attribution of cyber operations emanating from other States is difficult to obtain due to exclusive territorial control.[32] Therefore, recourse to indirect and circumstantial evidence should be allowed, and the standard of proof for violation of sovereignty should not be as high as in cases concerning the use of force or genocide.[33] However, to logically lead to a single conclusion of the existence of instruction, direction, or control by a State, it is necessary to collect and link facts showing the State's relationship with the two elements of cyber operations: (1) the IT infrastructure used in cyber operations and (2) the person or group of persons who implemented cyber operations.

The affidavit in the *Park Jin Hyok* case referred to the following evidence showing North Korea's relationship with the IT infrastructure:

- North Korean government officials had accessed some of the e-mail accounts used in hostile cyber operations.[34]

27. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 18 (Apr. 9).

28. *Id.* at 18.

29. *Id.* at 17.

30. Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 33 (Nov. 6).

31. For further analysis on the standard of proof, see Mikanagi & Mačák, *supra* note 21, at 64.

32. Respect for sovereignty is probably one of the likeliest primary rules of international law to be violated through cyber operations. *See* Schmitt, *supra* note 8.

33. Marco Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations,* 50 TEXAS INTERNATIONAL LAW JOURNAL 233, 248 (2015); Isabella Brunner et al., *Proving a State's Involvement in a Cyber-Attack: Evidentiary Standards before the ICJ,* 25 FINNISH YEARBOOK OF INTERNATIONAL LAW 101 (2015).

34. Affidavit, *supra* note 15, ¶¶ 103–10, 152–54, 276.

- Many of the operations were launched from North Korean IP addresses,[35] and due to the strict control of the access to and use of the internet in North Korea, it is likely that the North Korean government had at least known of and possibly approved these operations.[36]
- E-mail accounts associated with a company called Chosun Expo in Dalian, China, were used in cyber operations.[37] Chosun Expo was a front for the North Korean government; its employees were monitored by a political attaché from North Korea and they kept only a very small fraction of their salary, remitting the rest to the North Korean government.[38]

The affidavit referred to the following evidence showing North Korea's relationship with the person or group of persons:

- The suspect, Mr. Park, worked for Chosun Expo. Even after his return to North Korea in 2014, he used e-mail accounts associated with Chosun Expo using North Korean IP addresses.[39]
- After Sony Pictures Entertainment announced the release of a movie that was to depict a fictional North Korean leader in an unfavorable light, the North Korean government threatened retaliation in a letter sent to the U.S. National Security Council, and, following the operation against Sony Pictures Entertainment, North Korea issued a lengthy statement praising the authors, while carefully disavowing any responsibility for the operation.[40]

In more recent cases, U.S. officials accused Russia and China of involvement in malicious cyber operations. In an advisory relating to cyber operations published in August 2020, the National Security Agency referred to the use of IP addresses already associated with a Russian organization as evidence showing attribution to Russia.[41] In the indictment issued in July 2020

35. *Id.* ¶¶ 28, 36, 37, 207, 209, 307, 314.c, 320, 330, 333
36. *Id.* ¶ 272.
37. *Id.* ¶ 15.
38. *Id.* ¶¶ 269–71.
39. *Id.* ¶¶ 14, 289, 330.
40. *Id.* ¶ 84.
41. NATIONAL SECURITY AGENCY, CYBERSECURITY ADVISORY: RUSSIAN GRU 85TH GTSSS DEPLOYS PREVIOUSLY UNDISCLOSED DROVORUB MALWARE (Rev. 1.0 Aug. 2020), https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF.

in the *Li Xiaoyu and Dong Jiazhi* case, the U.S. Attorney referred to the Chinese Ministry of State Security's assistance to the suspects.[42] These kinds of evidence, if substantiated and collated, could provide indirect and circumstantial proof of the instruction, direction, or control by a State in carrying out the cyber operations.

On the other hand, the bar set by the ICJ for the proof of attribution to a State tends to be rather high. For example, in the *Oil Platforms* case, the discovery of moored mines bearing serial numbers matching other Iranian mines in the same area as the mine attack on the U.S. warship USS *Samuel B. Roberts*—in particular those found aboard an Iranian vessel boarded by U.S. forces—did not convince the ICJ that the *Roberts* struck a mine laid by Iran.[43] This evidence indicated a strong relationship between the mines laid in the area of the incident and Iran. However, it did not show the serial number of the mine that the *Roberts* actually struck. The ICJ noted that Iraq was also laying mines during the Iran-Iraq War, and the evidence shown by the United States could not logically exclude alternative interpretations not leading to Iran.

Concealing techniques employed in cyber operations are evolving daily, and it is difficult to say whether it is feasible to collect strong evidence that can logically exclude possibilities other than the instruction, direction, or control of a State.[44] The *Oil Platforms* case concerned the attribution of an armed attack which would require a relatively high standard of proof. On the other hand, non-State actors were not considered the most likely suspects in the *Oil Platforms* case, probably because they were believed to be less capable of laying mines in these areas than States. In cyber operations, it is probably more difficult to distinguish between operations by States and those by non-State actors. In this regard, it would be more difficult to exclude possibilities

42. Press Release, U.S. Department of Justice, Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research (July 21, 2020), https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

43. The ICJ said, "This evidence is highly suggestive, but not conclusive." Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 71 (Nov. 6). On the other hand, Judge Higgins, in her separate opinion, stated that this evidence is "on any test rather weighty." *Id.* at 234–35, ¶ 36 (separate opinion by Higgins, J.).

44. *See* Maurer, *supra* note 10, at 393; Russel Buchan, *Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm,* 21 JOURNAL OF CONFLICT & SECURITY LAW 429, 430–31 (2016).

other than a certain State's instruction, direction, or control in the case of cyber operations than in cases dealing with minelaying.

If a case concerning the attribution of cyber operations is brought before the ICJ, the Court can appoint experts to examine the evidence, as it did in the *Corfu Channel* case.[45] The experts' objective assessment would help evaluate the weight of evidence in eliminating possibilities other than the attribution to the accused State. However, considering the technical challenge involved in collecting evidence relating to the attribution of cyber operations to States that discreetly conduct these operations through proxies, the difficulty of attributing cyber operations to States cannot be underestimated. Therefore, as an alternative path to State responsibility, the applicability of the due diligence principle to cyber operations deserves careful but serious consideration.

III. APPLICATION OF THE DUE DILIGENCE PRINCIPLE

Tallinn Manual 2.0 supports the applicability of the due diligence principle to cyber operations.[46] In May 2020, responding to cyber incidents targeting medical facilities, more than one hundred public international lawyers, coordinated by Oxford scholars, jointly issued this statement:

> We, the undersigned public international lawyers, have watched with growing concern reports of cyber incidents targeting medical facilities around the world, many of which are directly involved in responding to the ongoing COVID-19 pandemic.
> . . .
> 2. International law prohibits cyber operations by States that have serious adverse consequences for essential medical services in other States.
> . . .
> 4. When a State is or should be aware of a cyber operation that emanates from its territory or infrastructure under its jurisdiction or control, and which will produce adverse consequences for health-care facilities abroad,

45. Brunner et al., *supra* note 33, at 103. There are also various proposals for the establishment of attribution mechanisms. *See, e.g.,* Kristen E. Eichensehr, *Symposium on Cyber Attribution: Decentralized Cyberattack Attribution,* 113 AJIL UNBOUND 213 (2019); Yuval Shany & Michael N. Schmitt, *An International Attribution Mechanism for Hostile Cyber Operations,* 96 INTERNATIONAL LAW STUDIES 196 (2020).

46. TALLINN MANUAL 2.0, *supra* note 12, rr. 6, 7, at 30–50.

> the State must take all feasible measures to prevent or stop the operation, and to mitigate any harms threatened or generated by the operation.[47]

Paragraph 2 of the statement endorsed the existence of international law prohibiting cyber operations that have serious adverse consequences for essential medical services in other States, and paragraph 4 supported the existence of legal obligations based on the due diligence principle applied to cyber operations.

As mentioned above, the *Corfu Channel* judgment referred to this principle in general terms, and UN Member States agreed that existing international law applies to cyber operations.[48] However, they have not yet agreed on whether the due diligence principle applies to cyber operations,[49] and there is a valid concern about the ambiguity of this principle. To what extent

---

47. The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector, https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea#/ (last visited July 22, 2021). In August 2020 another statement was issued focusing on cyber operations targeting vaccine research. The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research (Aug. 7, 2020), https://www.elac.ox.ac.uk/article/the-second-oxford-statement#/.

48. Paragraph 19 of the 2013 UNGGE Report stated: "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." 2013 UNGGE Report, *supra* note 13, ¶ 19. Paragraph 24 of the 2015 UNGGE Report confirmed this statement. 2015 UNGGE, *supra* note 13, ¶ 24.

49. Paragraph 13(c) of the 2015 UNGGE Report is often regarded as relevant to the due diligence obligation. It states: "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs." 2015 UNGGE Report, *supra* note 13, ¶ 13(c). The use of "should" here might indicate it is non-legally binding. However, this subparagraph cannot deny the pre-existing obligation under international law. In this regard, paragraph 25 of the final substantive report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), adopted on March 12, 2021, reads:

> States reaffirmed that norms do not replace or alter States' obligations or rights under international law, which are binding, but rather provide additional specific guidance on what constitutes responsible State behavior in the use of ICTs. Norms do not seek to limit or prohibit action that is otherwise consistent with international law.

Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 25, U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021).

do States have to monitor cyber activities in their territory? If they receive information relating to malicious cyber operations emanating from their territory, do they always have to take effective measures to stop them regardless of the credibility of the information or the seriousness of the operations? These questions are yet to be answered.

On the other hand, it is difficult to deny the existence of the obligation referred to in the *Corfu Channel* judgment, and the absence of its clearly defined outer limit cannot deny the existence of the core content. On May 28, 2021, the government of Japan submitted its "Basic Position of the Government of Japan on International Law Applicable to Cyber Operations"[50] to the UN Secretariat in response to the request of the chair of the UNGGE. The Basic Position explains Japan's position on the *Corfu Channel* due diligence obligation and refers to jurisprudence relating to various rules of international law containing the element of due diligence.[51] Such jurisprudence might not directly apply to cyber operations but assists our understanding of the nature of the due diligence obligation. The 1872 *Alabama* arbitral award pointed out that due diligence ought to be exercised by neutral governments in proportion to the risk.[52] The 2007 *Bosnian Genocide* judgment characterized the obligation to prevent genocide under the Genocide Convention as one of due diligence and found that the Federal Republic of Yugoslavia had violated the obligation by failing to use its capacity to influence the Bosnian Serb army.[53] In this judgment, the ICJ stated:

---

50. Ministry of Foreign Affairs of Japan, Basic Position of the Government of Japan on International Law Applicable to Cyber Operations, ¶ 2(4) (May 28, 2021), https://www.mofa.go.jp/files/100200935.pdf [hereinafter Basic Position].

51. *Id.*

52. Alabama claims of the United States of America against Great Britain (U.S. v. Gr. Brit.) 29 R.I.A.A. 125, 129 (Arb. Trib. 1872). The International Law Commission's commentary on Article 3 of the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities refers to the *Alabama* case saying, "The required degree of care is proportional to the degree of hazard involved. . . . The higher the degree of inadmissible harm, the greater would be the duty of care required to prevent it." International Law Commissionn, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with Commentaries*, 56 GAOR Supp. No. 10, art. 3 cmt. ¶ 18, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 Y.B. Int'l L. Comm'n 155, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf [hereinafter Draft Articles on Prevention of Transboundary Harm].

53. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶¶ 430, 438 (Feb. 26).

> 430. . . . In this area the notion of "due diligence", which calls for an assessment *in concreto*, is of critical importance. Various parameters operate when assessing whether a State has duly discharged the obligation concerned. The first, which varies greatly from one State to another, is clearly the capacity to influence effectively the action of persons likely to commit, or already committing, genocide. This capacity itself depends, among other things, on the geographical distance of the State concerned from the scene of the events, and on the strength of the political links, as well as links of all other kinds, between the authorities of that State and the main actors in the events.
>
> . . .
>
> 438. . . . Yet the Respondent has not shown that it took any initiative to prevent what happened, or any action on its part to avert the atrocities which were committed. It must therefore be concluded that the organs of the Respondent did nothing to prevent the Srebrenica massacres, claiming that they were powerless to do so, which hardly tallies with their known influence over the [Bosnian Serb army].

It seems natural that (1) the "due" diligence principle imposes an obligation proportionate to the seriousness of the risk and that (2) the capacity to influence the perpetrator of acts contrary to the rights of other States entails the obligation to use it for stopping such acts. In the absence of specific rules setting out measures to be taken by States for the prevention of hazardous activities in their territories, it is difficult to determine to what extent States shall monitor or regulate potentially hazardous activities.[54] However, when a State has the capacity to influence a person or group of persons in their territories through particular links, including financial or other assistance, and the person or group of persons is engaging in hazardous activities, the State's capacity to influence should entail an obligation to exercise that influence to stop such activities.[55]

---

54. International agreements regulating cybercrime, including the Budapest Convention on Cybercrime, can strengthen the rules on the regulation of cyber operations. *See* Convention on Cybercrime, *opened for signature* Nov. 23, 2001, T.I.A.S. No. 13,174, E.T.S. 185, 2296 U.N.T.S. 167(entered into force July 1, 2004), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

55. In the *Corfu Channel* case, Albania's particular links to the perpetrator who laid mines was not proven. On the other hand, Albania's constructive knowledge of the minelaying was proven, and the ICJ found that Albania had an obligation to notify and warn incoming vessels. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

Without prejudice to the existence of other types of obligation constituting the due diligence obligation, including the obligation to monitor or regulate,[56] if these two elements above are applied to cyber operations, the due diligence obligation seems likely to include a State's obligation to use its existing influence over the activities of a person or group of persons, when the person or the group of persons is involved in cyber operations that emanate from its territory and seriously infringe upon other States' rights and the State knows or should know of the existence of the operations.[57] In this regard, the Japanese Basic Position argues:

> [W]hen a State has received a credible notification from another State of the possibility that a person or group of persons located in its territory and receiving from it financial and other forms of support may be involved in a cyber operation that may cause serious adverse consequences, such as damage to a target State's critical infrastructure, the due diligence obligation owed by the informed State is presumed to include the obligation to exercise its capacity to influence the state supported person or group of persons so as to prevent them from implementing such cyber operations.[58]

---

56. Paragraph 17 of the International Law Commission's commentary on Article 3 of the Draft Articles on Prevention of Transboundary Harm states:

> The main elements of the obligation of due diligence involved in the duty of prevention could be thus stated: the degree of care in question is that expected of a good Government. It should possess a legal system and sufficient resources to maintain an adequate administrative apparatus to control and monitor the activities.

Draft Articles on Prevention of Transboundary Harm, *supra* note 52.

57. The *Corfu Channel* judgment clarified that the knowledge required for the application of the due diligence obligation encompasses constructive knowledge of the risk. Corfu Channel, 1949 I.C.J. at 22; *see also* TALLINN MANUAL 2.0, *supra* note 12, at 41.

58. Basic Position, *supra* note 50, ¶ 2(4).

This obligation would mean, for example, that if a State (the "territorial State"), which has influence over the activities of a person or group of persons through financial, logistical, or other links,[59] receives credible notification[60] about cyber operations emanating from its territory seriously damaging the critical infrastructure[61] of another State (the "victim State"), including information about the use of IP addresses which are allocated to the territorial State and used by the person or group of persons, and the territorial State finds out about the involvement of the person or group of persons, the territorial State must exercise its influence to stop such operations.[62] If the territorial State does not take the measures available to it to terminate the cyber operations and they continue to cause serious damage to the victim State's critical infrastructure, the territorial State would violate the due diligence obligation.

The existence of States' influence over the person or group of persons involved in cyber operations emanating from their territories might also be

59. This includes a person or group of persons under "overall control" of the State and a person or group of persons receiving financial and other support from the State, but it does not include a person or group of persons not receiving active support and purely passively harbored in the territory. *See* Tim Maurer, *supra* note 1010, at 395–97. *Tallinn Manual 2.0* provides examples of States' support to non-State actors that fall short of attribution. These include "general support for or encouragement of a non-State actor or its cyber operations," "the provision of malware," and "participation in the 'financing, organizing, training, supplying, and equipping.'" *See* TALLINN MANUAL 2.0, *supra* note 12, at 97.

60. If the territorial State has strong links with the person or group of persons involved in cyber operations, its constructive knowledge about the cyber operations might be presumed. If so, this notification would become unnecessary for the application of the due diligence obligation.

61. Paragraph 5 of the 2015 UNGGE Report said: "The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical infrastructure is both real and serious." 2015 UNGGE Report, *supra* note 13, ¶ 5. "Critical infrastructure" is not yet clearly defined but the preamble of General Assembly Resolution 58/199, titled "Creation of a global culture of cybersecurity and the protection of critical information infrastructures," refers to "critical infrastructures—such as those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health." G.A. Res. 58/199 (Dec. 23, 2003). Paragraph 18 of the final substantive report of the OEWG further clarified: "While it is each State's prerogative to determine which infrastructures it designates as critical, such infrastructure may include medical facilities, financial services, energy, water, transportation and sanitation." Final Substantive Report of the Open-Ended Working Group, *supra* note 49, ¶ 18.

62. TALLINN MANUAL 2.0, *supra* note 12, at 43–45.

concealed through aliases and other techniques. Still, it should, nevertheless, be relatively easier to prove than the States' specific instruction, direction, or control over cyber operations.

In the *Park Jin Hyok* case, according to the affidavit, the North Korean government maintained considerable influence over Chosun Expo. Mr. Park, who was accused for his role in malicious cyber operations, was allegedly using Chosun Expo's e-mail accounts from North Korea, and the same e-mail accounts were accessed from North Korean IP addresses.[63] According to the affidavit, the e-mail accounts associated with Chosun Expo and used by Mr. Park were accessed from the North Korean IP address "#7,"[64] and the same IP address was used for malicious cyber operations.[65] As mentioned above, the affidavit explains that using a common IP address typically indicates the use of shared or common computer infrastructure or the same physical space to connect to the internet.[66] Even if these pieces of evidence do not prove the specific instruction, direction, or control by the North Korean government, they seem to indicate that it was in a position to exert some influence over the network of individuals and IT infrastructure.

Similarly, the Chinese Ministry of State Security's assistance to the suspects alleged in the indictment in the *Li Xiaoyu and Dong Jiazhi* case[67] would, if supported by credible evidence, also indicate influence over the suspects. The proof of the territorial State's influence should require a lower level of specificity in its relationship to actual cyber operations than the level required for the proof of attribution under Article 8 of the Articles on State Responsibility, and, as discussed above, recourse to indirect and circumstantial evidence should be allowed for the proof of this influence by the victim State.

This is an area of international law where further clarification of customary international law through State practice and *opinio juris* is required. States should consider whether there is a legal obligation for States to take action against the activities of persons involved in cyber operations emanating from their territories that are seriously damaging other States' critical infrastructure. Taking into account the difficulty in proving specific instruction, direction, or control over cyber operations by States in accordance with the rules

63. *See supra* note 18; *see also* Affidavit, *supra* note 15, ¶¶ 307, 310, 314, 320, 330.

64. Affidavit, *supra* note 15, ¶¶ 307, 314.c, 320, 330.

65. *Id.* ¶¶ 207, 209, 307, 333.

66. *Id.* ¶ 26.

67. United States v. Li Xiaoyu & Dong Jiazhi, No. 4:20-CR-6019-SMJ (E.D. Wash. July 7, 2020), https://www.justice.gov/opa/press-release/file/1295981/download.

of attribution clarified in the Articles on State Responsibility, it seems prudent not to deny the existence of this obligation and preserve an alternative path to invoking State responsibility for cyber operations discreetly conducted through proxies.

IV. CONCLUSION

Intricate concealing techniques render it difficult to obtain direct evidence showing States' instruction, direction, or control over actual cyber operations. Therefore, recourse to indirect and circumstantial evidence should be allowed, and the standard of proof should be lowered for less serious charges. Evidence showing States' relationship with the IT infrastructure used for cyber operations and the person or group of persons involved in the operations should contribute to the proof of attribution. However, it is difficult to determine whether it is possible to obtain sufficient evidence for proving attribution to States under the existing rules of attribution.

The free flow of data should be protected in principle, and the application of international law should not cause overregulation. It is difficult to strike the right balance between freedom and regulation in cyberspace. However, cyber operations can seriously damage critical infrastructure, and the discreet use of proxies makes it difficult to attribute them to States in accordance with the existing rules of international law. For the regulation of such cyber operations, while there remains uncertainty regarding the proof of attribution, States should not deny the due diligence obligation discussed above. This obligation does not require States to extend or strengthen their influence over private individuals or entities, and, therefore, it does not give an excuse for them to take intrusive measures restricting the free flow of data and freedom of expression. It simply obliges them to use their existing influence over the activities of a person or group of persons when those persons are involved in cyber operations that seriously damage other States' critical infrastructure.

On May 13, 2021, U.S. President Biden spoke on the Colonial Pipeline incident.[68] In his remarks, President Biden referred to an "international standard" relating to the responsibility of the territorial State from which malicious cyber operations emanate. This standard can be established through conventions on cybercrime to some extent. However, even in the

68. President Joe Biden, Remarks on the Colonial Pipeline Incident (May 13, 2021), https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/.

absence of a universally accepted convention on cybercrime, if the territorial State has the capacity to influence the perpetrator, it should have a legal obligation to take measures under customary international law. The legal regulation of malicious cyber operations should be strengthened through multiple layers of obligations, consisting, *inter alia*, of attribution to States, cybercrime conventions, and the due diligence principle. These three elements are not mutually exclusive; they can supplement and reinforce each other. As an important component of this multi-layered regulation, the applicability and scope of the due diligence principle should be discussed further among States and scholars.