IS THE CURRENT INTERNATIONAL LAW A GOOD FIT FOR CYBERSECURITY? A U.N. CHARTER-BASED ANALYSIS

YUAN FANG*

I. INTRODUCTION

The 21st century has witnessed the rapid emergence of cyber technologies worldwide. The Internet has dramatically gone beyond the physical boundary of each state, making cybersecurity a challenge facing the international community as a whole.[1] Among the various international systems, international law plays a significant role and functions irreplaceably in addressing these challenges.[2] However, it remains a question whether the regulatory framework of current international law is well equipped for the challenges deriving from cyberspace. As a response to this question, this article will particularly look to the law of war, which inquires about the legitimacy of the acts conducted under Jus in Bello (known as "international humanitarian law" or "law of armed conflict"), and Jus ad Bellum (known as "use of force"). Generally, Jus in Bello governs the conduct of warring parties, whereas Jus ad Bellum formulates the conditions for war.[3] While there has been a relative abundance of scholarship exploring the applicability of Jus in Bello in the cyber sphere,[4] less attention has been paid to the cyber implications of Jus ad Bellum.[5]

---

1 *See* Matthias C. Kettemann, *Ensuring Cybersecurity through International Law*, 69 REVISTA ESPAÑOLA DE DERECHO INTERNACIONAL 281, 283–84 (2017) (stating that cybersecurity lies in the common interest of all states).

2 *See id.* at 284–88 (noting that cybersecurity is intermingled with both international treaty law and customary international law by virtue of the interconnectivity between international law and the Internet).

3 For a detailed description of the relationship between Jus in Bello and Jus ad Bellum, see, *e.g.*, Jenny Martinez & Antoine Bouvier, *Assessing the Relationship Between Jus in Bello and Jus ad Bellum: An "Orthodox" View*, 100 AM. SOC'Y INT'L L. PROC. 109 (2006); Julie Mertus, *The Danger of Conflating Jus ad Bellum and Jus in Bello*, 100 AM. SOC'Y INT'L L. PROC. 114 (2006). In addition to Jus in Bello and Jus ad Bellum, an increasing number of scholars recognize the notion of "Jus post Bellum," which looks at the international justice in the post-war era. *See, e.g.*, Carsten Stahn, *'Jus ad bellum', 'jus in bello'…'jus post bellum'?—Rethinking the Conception of the Law of Armed Force*, 17 EUR. J. INT'L L. 921 (2007).

4 *See, e.g.*, Terry D. Gill, *International Humanitarian Law Applied to Cyber-Warfare: Precautions, Proportionality and the Notion of "Attack" under the Humanitarian Law of Armed Conflict*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 366 (Nicholas Tsagourias & Russell Buchan eds., 2015); Elizabeth Mavropoulou, *Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks*, 4 J.L. & CYBER WARFARE 23 (2015); Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 LOY. L.A. INT'L & COMP. L. REV. 303 (2010).

5 *See, e.g.*, Oona A. Hathaway & Rebecca Crootof, *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 841–49 (2012); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421 (2011); Danial B. Silver, *Computer Network Attack as a Use of*

Accordingly, this article will particularly focus on the interactions between cyber technology and Jus ad Bellum, primarily the "use of force" under the Charter of the United Nations (hereinafter "the U.N. Charter").

The U.N. Charter prohibits the illegal use of force, but recognizes two circumstances where the use of force is permissible.[6] In terms of the illegitimate use of force, Art. 2(4) of the U.N. Charter stipulates that the threat or use of force is unjustifiable if it is "against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[7] On the contrary, U.N. Charter Art. 51 and Art. 42 provide two justifications for the use of force. Specifically, Art. 51 recognizes the Member State's "inherent right of individual or collective self-defense,"[8] and Art. 42 legitimizes the use of force that adheres to the Security Council's authorization.[9] For this article, the following discussions will focus on two main issues: first, the controversies that arise from the scope of "use of force" under Art. 2(4) when it is applied within the cyber realm; second, the requirement of attribution under Art. 51 and its intersection with cyberspace. Instead of judging if specific acts conducted in cyberspace might fit into the U.N. Charter, the inquiry of this article is broader and more structural: are the current rules and interpretations of the U.N. Charter sufficient for making that determination?

Force Under Article 2(4) of the United Nations Charter, 76 INT'L L. STUD. 73 (2002); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

6 Matthew C. Waxman, *Regulating Resort to Force: Form and Substance of the UN Charter Regime*, 24 EUR. J. INT'L L. 151, 155 (2013).

7 U.N. Charter art. 2, ¶ 4. All acts falling within the scope of Art. 2(4) of the U.N. Charter may serve as a basis for finding a crime of aggression at the International Criminal Court (ICC), so long as they are a "manifest" violation of the Charter. *See generally* Sean D. Murphy, *The Crime of Aggression at the ICC*, *in* THE OXFORD HANDBOOK OF THE USE OF FORCE IN INTERNATIONAL LAW (Marc Weller ed., 2015). The 2010 Kampala Conference had discussions about the determination of whether the violation of Art. 2(4) is "manifest." The current test used to measure the gravity of armed force is a four-factor test proposed by the Office of the Prosecutor (OTP) of the ICC, which comprehensively looks to the scale, nature, manner of the commission, and impact of the use of force. INT'L CRIM. CT. OFF. OF THE PROSECUTOR, REPORT ON PRELIMINARY EXAMINATION ACTIVITIES 2019, (Dec. 5, 2019), https://www.icc-cpi.int/itemsDocuments/191205-rep-otp-PE.pdf.

8 U.N. Charter art. 51.

9 *Id*. art. 42 ("Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security.").

II. ON THE SCOPE OF "USE OF FORCE" UNDER ART. 2(4)

A. The Scope of "Use of Force" in the Traditional Setting

The answer to what the "use of force" under U.N. Charter Art. 2(4) exactly means first lies in the case law. Several monumental cases in the history of international law have shaped our current understanding of Art. 2(4) "use of force." In the case of *Nicaragua*,[10] the International Court of Justice (hereinafter "the I.C.J.") defined the "use of force" under Art. 2(4) as "the most grave forms of the use of force (those constituting an armed attack)," which are distinguishable from "other less grave forms."[11] To determine if certain acts fall within the definition of "use of force" under Art. 2(4), the I.C.J. looked to the "scale and effects" of the force used.[12] In applying the test, the I.C.J. stated that an armed attack can be neither "a mere frontier incident" nor merely "assistance to rebels in the form of the provision of weapons or logistical or other support" in light of its scale and effects.[13] Subsequent to *Nicaragua*, the *Oil Platforms* case[14] added to the interpretation of the "scale and effects" test. In its *Oil Platforms* judgment, the I.C.J. suggested that the cumulative nature of a series of forcible actions could possibly turn them into an "armed attack."[15] Additionally, the "scale and effects" test is further clarified by several other I.C.J. judgments, like *Armed Activities* and *Eritrea-Ethiopia Claims Commission*.[16] In spite of the increasing clarity, the "scale and effects" test is still frequently criticized for its uncertainty and ambiguity. As pointed out by some scholars, the "scale

10 In *Nicaragua*, the Nicaraguan government contested the legitimacy of U.S. support for rebels attacking the Nicaraguan government, "as well as such U.S. acts as laying mines in Nicaraguan" territory "and attacking Nicaraguan ports and oil installations." In its judgment, the ICJ concluded that the behavior of the U.S. constitutes an illegal use of force against Nicaragua. MARK WESTON JANIS, JOHN E. NOYES & LEILA NADYA SADAT, INTERNATIONAL LAW: CASES AND COMMENTARY 790–92 (6th ed., 2020).

11 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 191 (June 27).

12 *Id.* ¶ 195.

13 *Id.*

14 In *Oil Platforms*, Iran claimed that the U.S. "had breached the 'freedom of commerce' provision in the 1955 Treaty of Amity, Economic Relations and Consular Rights between the two countries by taking military action against Iranian offshore oil platforms in 1987 and 1988." The ICJ rejected the claim, "finding that the U.S actions against the oil platforms did not disrupt commerce between the territories of Iran and the United States." William H. Taft, IV, *Self-Defense and the Oil Platforms Decision*, 29 YALE J. INT'L L. 295, 295 (2004).

15 Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 64 (Nov. 6) ("Even taken cumulatively . . . these incidents do not seem to the Court to constitute an armed attack on the United States . . . as a 'most grave' form of the use of force. . . .").

16 For a description of the cases, see Abdulqawi A. Yusuf, *The Notion of "Armed Attack" in the Nicaragua Judgment and Its Influence on Subsequent Case Law*, 25 LEIDEN J. INT'L L. 461, 468–70 (2012).

and effects" test neither "clearly elaborate[s] on the required scale and effects necessary to reach the threshold of armed attack," nor "provide[s] guidance on what type of response might be appropriate for acts that fall below the threshold."[17] As a consequence, the scope of "use of force" under Art. 2(4) is potentially overbroad, "rang[ing] from a fairly restricted use of force, such as a border raid causing limited loss or damage, to a full-scale invasion of [the] territory."[18]

While the case law does not provide a clear answer regarding the scope of "use of force" under Art. 2(4), we are likely to gain a better understanding of it through the distinction between military coercion and economic/political coercion. Conventionally, Art. 2(4) of the U.N. Charter solely prohibits "military coercion."[19] For example, U.N. General Assembly Resolution 3314 formulated seven acts that fall within Art. 2(4), all of which are characterized by using or threatening to use armed force.[20] By contrast, the U.N. rejected the proposal of "economic coercion" in 1945,[21] and the proposal of "political coercion" in 1970,[22] explicitly excluding them from the scope of "use of force" under U.N. Charter Art. 2(4).

B. The Scope of "Use of Force" in the Cyber Context

This article will explore the scope of Art. 2(4) "use of force" in the cyber context, primarily within the framework of the Tallinn Manual on International Law Applicable to Cyber Warfare (hereinafter "the Tallinn Manual"), since it covers a much broader set of "views and expertise than is gathered in any other single source."[23] Organized and coordinated by the North Atlantic Treaty Organization (NATO), the Tallinn Manual 1.0 was

17 *Id.* at 465.

18 David Kretzmer, *The Inherent Right to Self-Defense and Proportionality in Jus Ad Bellum*, 24 EUR. J. INT'L L. 235, 243 (2013).

19 *See* Hathaway & Crootof, *supra* note 5, at 845 (citing Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1041 (2007)).

20 G.A. Res. 3314 (XXIX), Definition of Aggression, at 142 (Dec. 14, 1974).

21 TALLINN MANUAL ON THE INTERNATIONAL HUMANITARIAN LAW APPLICABLE TO CYBER WARFARE 46 n.11 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL 1.0].

22 *Id.* at 46 n.12.

23 Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. 735, 740 (2017). Regardless of the Tallinn Manuals' tremendous influence, the attitudes toward the Tallinn Manuals among different people are highly divergent. Some scholars think positively about the Tallinn Manual, noting that it provides a "unique and comprehensive statement on the international law applicable to cyber operations." *Id.* The opponents criticize that the Tallinn Manual adds to the existing ambiguity rather than clarifying it. *See generally* Lianne J.M. Boer, *Restating the Law as It Is: On the Tallinn Manual and the Use of Force in Cyberspace*, 5 AMSTERDAM L.F. 4 (2013) (considering the four possible ways of viewing the criteria of the Tallinn Manual and finding that the results are dissatisfactory).

released in 2013,[24] and the Tallinn Manual 2.0 was subsequently published in 2017.[25] Despite the fact that the means used for attacks have been diversified in cyberspace as compared to the traditional setting, the Tallinn Manuals' interpretation with respect to the "use of force" under U.N. Charter Art. 2(4) is generally pursuant to the existing rules. In terms of the "scale and effects" test in case law, both the Tallinn Manual 1.0 and 2.0 recognize that the focus on scale and effects is an "equally useful approach" in light of cyber operations.[26] With regard to the distinction between military coercion and economic/political coercion, the Tallinn Manual 1.0 proposes that cyber operations that involve, or are otherwise analogous to, economically or politically coercive activities are definitely not prohibited uses of force with respect to the definition of use of force.[27] The Tallinn Manual 2.0 omitted this expression, keeping silent on whether economic or political coercion may fit into the Art. 2(4) "use of force" in cyberspace.[28]

C. The Gaps between the Current Framework and the Demands of Cyberspace

Although no consensus has been reached with regard to the exact meaning of "scale and effects," some criteria have been provided for the determination of whether the threshold of "armed attack" is met. These criteria comprehensively look to the severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy of the use of force in question.[29] Following these criteria, earlier researchers believed that cyber-attacks in the form of economic or political coercion are unlikely to be grave enough to constitute an "armed attack."[30] However, the research completed more recently indicates there is a possibility that certain economic or political coercion in cyberspace may satisfy the requirements for Art. 2(4) of the U.N. Charter in accordance with these criteria.[31]

---

24 TALLINN MANUAL 1.0, *supra* note 21.

25 TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schnitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

26 TALLINN MANUAL 1.0, *supra* note 21, at 45–46; TALLINN MANUAL 2.0, *supra* note 25, at 331.

27 *See* TALLINN MANUAL 1.0, *supra* note 21, at 46.

28 TALLINN MANUAL 2.0, *supra* note 25, at 331.

29 *See* Schmitt, *supra* note 5, at 914–15.

30 See *id.* at 914 ("Economic and political coercion can be delimited from the use of armed force by reference to [the] criteria.").

31 *See* Silver, *supra* note 5, at 89 ("[E]xamination of the criteria suggests that virtually any event of [cyber-attack] can be argued to fall on the armed force side of the line, except perhaps as regards the criterion of severity.").

Given that different attacks may have totally different means and consequences, whether a cyber-attack may fall within U.N. Charter Art. 2(4) should be analyzed case by case.[32] After a review of a series of scenarios relating to economic or political coercion in cyberspace, the conclusion of this article is different from the previous views that economic or political coercion within the cyber sphere is either very unlikely or very likely to fall within Art. 2(4). The real problem here is that the advancement of cyber technology has made cyber-attacks in the form of economic or political coercion tremendously different from these coercions in their traditional sense, whereas the existing rules and their interpretations fail to reflect this significant shift. This failure weakens our capacity to decide if a cyber-attack might fall within Art. 2(4).

With regard to economic coercion, one of the most extreme hypotheticals is a cyber-attack on a major international stock exchange that causes the market to crash.[33] Similar to traditional economic coercion, even a cyber-attack as severe as this may still fail to meet the threshold for severity, since mere financial loss is unlikely to constitute damage for this purpose.[34] However, because of the efficiency of electronic transmission, the connection between a cyber-attack on the stock exchange and the occurrence of the negative consequences would be more immediate than usual. This challenges the conventional understanding that the linkage between the initial acts and their effects tends to be indirect in an instance of economic coercion.[35] Another example of economic coercion in cyberspace is the WannaCry "ransomware" attack, which happened in May 2017. Within four days, the malware spread quickly and reached more than 230,000 computers in more than 150 countries around the world.[36] The incident resulted in great financial losses to both individuals and companies: the ransomware encrypted data on infected machines, locking victims out of their files unless they paid $300 in Bitcoin;[37] a number of global companies, including Spain's Telefonica, France's Renault, and FedEx, were seriously impacted by the attack.[38] Economic coercion resembling this last example alone will possibly not be considered as an Art. 2(4) "use of

32 *See* WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 120–21 (1999).

33 JEREMY A. RABKIN & JOHN YOO, STRIKING POWER: HOW CYBER, ROBOTS, AND SPACE WEAPONS CHANGE THE RULES FOR WAR 179 (2017).

34 *See* TALLINN MANUAL 2.0, *supra* note 25, at 343.

35 *See id.* at 331.

36 Kristen Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 537 (2020).

37 *Massive Ransomware Infection Hits Computers in 99 Countries*, BBC NEWS (May 13, 2017), https://www.bbc.com/news/technology-39901382.

38 *Id.*

force" in terms of severity. Nevertheless, given the precision and accuracy of its cyber-attack, the WannaCry ransomware is potentially able to bring extremely severe consequences to the specific targets. For instance, the ransomware shut down computers in more than eighty national health service organizations in England, "resulting in almost 20,000 cancelled appointments, 600 GP surgeries having to return to pen and paper, and five hospitals simply diverting ambulances, unable to handle any more emergency cases."[39] Assuming the shut-down of the health service centers caused physical injury or death in addition to merely economic damages, it is not unlikely that it would be regarded as an attack under the U.N. Charter Art. 2(4).

Concerning political coercion, cyber propaganda aiming at election intervention, terrorism, racial discrimination, or other political goals has become reality.[40] Compared to the traditional form, the political coercion in the context of cyberspace triggers more concerns about whether it is likely to be seen as a "use of force" in the sense of Art. 2(4), given that the trend of "weaponization" of the Internet and social media has become increasingly obvious in recent years.[41] It remains to be seen what are the specific difficulties encountering the existing rules and interpretations of the U.N. Charter Art. 2(4) as applied to the political coercion in cyberspace.

III. ON THE REQUIREMENT OF ATTRIBUTION UNDER ART. 51

A. The Requirement for Attribution in the Traditional Context

Art. 51 of the U.N. Charter prominently raises two requirements for the attribution of the use of force falling within Art. 2(4) in order for the exercise of self-defense. First, Art. 51 demands the attributed attack to impose an "imminent threat" to the attacked state. The "imminent threat" requirement derives from the *Caroline* incident in 1837,[42] where two core principles of

39 Alex Hern, *WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in* 2017, GUARDIAN (Dec. 30, 2017, 3:00 AM), https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

40 *See, e.g.*, Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30 (2018); Ariel Victoria Lieberman, *Terrorism, the Internet, and Propaganda: A Deadly Combination*, 9 J. NAT'L SEC. L. & POL'Y 95 (2017); Gail Mason & Natalie Czapski, *Regulating Cyber-Racism*, 41 MELB. U. L. REV. 284 (2017).

41 *See generally* P.W. SINGER & EMERSON T. ROOKING, LIKEWAR: THE WEAPONIZATION OF SOCIAL MEDIA (2018).

42 *See* Ashley S. Deeks, *Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483, 502 (2012). In *Caroline*, the Canadian rebels used the U.S. territory

legal international self-defense, necessity and proportionality, were proposed.[43] In terms of necessity, the *Caroline* demands that self-defense is justified only if the danger is "instant, overwhelming, leaving no choice of means, and no moment for deliberation."[44] In other words, the attacks to be attributed to must be still in progress.[45] The principle of necessity was widely used in international disputes after the *Caroline* event and rapidly came to represent the customary international law of self-defense. Art. 51 of the U.N. Charter incorporated it as one of the pillars of the right of self-defense.[46] In recent years, some states (especially the U.S.) advocated for the concept of "preemptive self-defense" for the interpretation of the U.N. Charter Art. 51, seeking a conceptual expansion of the "imminent threat" to encompass non-imminent threats.[47] However, it has been an unsuccessful attempt to change the international custom thus far, and the "imminent threat" standard is still good law.[48]

Art. 51 then requires the attack to be attributed to a "state actor." "State actor" is traditionally understood as the individuals, groups, or organizations related to state government. However, an increasing number of scholars argue that this narrow interpretation imposes a constraint on the exercise of the right of self-defense by states.[49] With the rise of international terrorism, states like the U.S. suggest the adoption of the "unwilling or unable" test, which advocates for the legitimacy of self-defense when the territorial state is unwilling or unable to address the terroristic threat.[50] In applying the "unwilling or unable" inquiry, "state actor" is likely to range

as a staging ground from which to attack British forces in Canada. The rebels used a steamer called the *Caroline* to transport themselves from the U.S. side of the Niagara River to the Canadian side. British troops set fire to and destroyed the *Caroline*, prompting a strong objection from the U.S. and a series of diplomatic exchanges setting forth each state's position.

43 *See* Matthew Allen Fitzgerald, *Seizing Weapons of Mass Destruction from Foreign-Flagged Ships on the High Seas under Article 51 of the UN Charter*, 49 VA. J. INT'L L. 473, 479 (2009).

44 *See* LORI F. DAMROSCH, LOUIS HENKIN, RICHARD CRAWFORD PUGH, OSCAR SCHACHTER & HANS SMIT, INTERNATIONAL LAW: CASES AND MATERIALS 923 (2001) (citing the Letter from Mr. Webster to Lord Ashburton, August 6, 1842).

45 *See* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 1420 (Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus & Nikolai Wessendorf eds., 3d ed. 2012) ("[T]he [cyber] attack must not be over but still ongoing.").

46 *See* Fitzgerald, *supra* note 43, at 480.

47 *See* Waxman, *supra* note 5, at 434–36.

48 *See id.* at 458–59 (noting the difficulty of reaching interpretive agreement between different countries by virtue of the divergence on national strategies).

49 *See, e.g.*, Elizabeth Wilmhurst, *The Chatham House Principles of International Law of the Use of Force in Self-Defense*, 55 INT'L & COMPAR. L.Q. 963, 969 (2006) ("There is no reason to limit a State's right to protect itself from an attack by another State . . . . The source of the attack, whether a State or a non-state actor, is irrelevant to the existence of the right.").

50 *See generally* Deeks, *supra* note 42 (providing a sustained descriptive and normative analysis of the "unwilling or unable" test).

from the most typical actors to the non-state actors including but not limited to terrorist groups. Despite this, the narrower interpretation of the "state actor" currently is still good law.[51]

B. The Attribution Requirements within the Cyber Sphere

The Tallinn Manual 1.0 and 2.0 are inclined to broaden the interpretations of both the "imminent threat" and the "state actor" underlying the U.N. Charter Art. 51. In terms of "imminent threat," the majority of Tallinn experts are supportive of the notion of "anticipatory self-defense," which is similar to the aforementioned "preemptive self-defense."[52] By doing so, the Tallinn Manuals encourage the inclusion of at least some of the non-imminent threats as to the interpretation of the "imminent threat" within Art. 51. With regard to "state actor," "the majority concluded that self-defense against a cyber armed attack is permissible when . . . the territorial State is unable (e.g., because it lacks the expertise or technology) or unwilling to take effective actions to repress the relevant elements of the cyber armed attack."[53] Accordingly, the Tallinn Manuals are open to the possibility that under certain circumstances the attribution to non-state actors might be sufficient to reach the threshold of Art. 51. While the expert opinions are academically authoritative, they are neither legally binding, nor a reflection of the official position of any state.[54] Therefore, the Tallinn Manuals do not change the default that the Art. 51 attribution rules set for the traditional context are to be equally applied to cyberspace.

C. The Gaps between the Existing Mechanism and the Needs of Cyberspace

Attribution is extremely difficult in the sphere of cyberspace in comparison with the traditional context, partially as a result of the unique design of the Internet.[55] Cyber-attack is typically featured by its rapidity, secrecy, and complexity, which will possibly erode the applicability of the attribution rules under the U.N. Charter Art. 51. However, the existing rules

---

51 *See id.* at 546 ("[T]he 'unwilling or unable' test . . . currently lacks sufficient content to serve as a restrictive international norm.").

52 *See* TALLINN MANUAL 2.0, *supra* note 25, at 351.

53 *See id.* at 347.

54 Kristen E. Eichensehr, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 108 AM. J. INT'L L. 585 (2014).

55 *See* Herbert Lin, *Attribution of Malicious Cyber Incidents: From Soup to Nuts*, 70 COLUM. J. INT'L AFFS. 75, 100 (2016); *cf.* Eichensehr, *supra* note 36, at 520 (noting that the technical difficulty of cyber attribution is just the precursor to the more complicated legal and policy questions). *But cf.* RABKIN & YOO, *supra* note 33, at 171 (brushing off the attribution problem in the cyber realm as a minor issue).

and interpretations in regard to Art. 51 fail to promptly respond to the rapid evolvement of cyber technologies, impairing our ability to determine if certain attribution to cyber-attack meets the requirement of Art. 51.

First, the "imminent threat" requirement is hard to be reached in the cyber context for both the rapidity and secrecy of cyber-attack. According to a recent investigation of thousands of data breaches, the time from the first action in an event chain to the initial compromise of an asset is most often measured in seconds or minutes.[56] The rapidity of cyber-attacks leaves basically no time for the attacked state to determine the source, possibly leading to the failure of attribution.[57] Despite the fact that the cyber operation is conducted in a short period of time, the time needed for discovering the attack is dramatically longer, usually taking "weeks or months."[58] The secrecy of a cyber operation results in further obstacles for satisfying the "imminent threat" requirement.

Second, the requirement for "state actor" is also difficult to meet, given the complexity of the actors involved in the cyber-attack. There are generally three types of actors amid attribution, namely the machine (the IP address leveraged to conduct the attack), the perpetrator (the human intruder perpetrating the attack), and the adversary (the state as the ultimately responsible party).[59] The relationship between the various actors is hugely complicated in reality. As a result, "knowing the machine responsible does not necessarily provide the identity of the perpetrator, and knowing the identity of the perpetrator does not necessarily reveal the party that is ultimately responsible."[60] The complexity of the actors within the cyber operation makes any attribution to "state actor" hardly possible.

CONCLUSION

This article eventually reaches a conclusion that the current international law may not be a good fit for cybersecurity in light of the U.N. Charter. Given the ambiguity and uncertainty of the existing rules and interpretations, as well as the novel demands of cyber technologies, the U.N. Charter is not well equipped for addressing issues arising from the cyber realm. Regarding the scope of "use of force" under the U.N. Charter Art.

56*See* Verizon, *2018 Data Breach Investigations Report (Exclusive Summary)* (2018), https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.

57 *See* RABKIN & YOO, *supra* note 33, at 178.

58 *See* Verizon, *supra* note 56.

59 *See* Lin, *supra* note 53, at 80–89.

60 *See id*. at 89.

2(4), the "scale and effects" test and the distinction between military and economic or political coercion that currently applied in the traditional context, are inadequate in response to the efficiency and precision of cyber-attacks. As to the requirement for attribution under the U.N. Charter Art. 51, the limitations like "imminent threat" and "state actor" that contemporarily applied for non-cyber attribution, are unable to effectively react to the rapidity and secrecy of cyber-attacks, as well as the complexity of the actors engaged in the cyber operation.

With all the dissatisfactions, the next issue to be addressed is how to bridge the gaps between the U.N. Charter and cyberspace. To acquire the flexibility required for adapting the U.N. Charter to the cyber era's new demands, we are supposed to situate the U.N. Charter in a broader picture. The U.N. Charter is essentially a reflection of the intersection between the two main themes throughout the development of international law, respectively the protection of human rights, and the defense of national sovereignty. Through a deeper understanding of their relationship, we are likely to find the path forward to make the U.N. Charter a better fit for cybersecurity.