STETSON BUSINESS LAW REVIEW

# APPLYING INTERNATIONAL LAW TO CROSS-BORDER CYBER ATTACKS SPONSORED BY STATE ACTORS

Saili Hernandez*

TABLE OF CONTENTS



* Associate, Hall, Booth, Smith, P.C. Stetson University College of Law, Juris Doctor (J.D.), *cum lade*, 2024. University of South Florida, Bachelor of Arts in Political Science, minor in Economics, *magma cum lade*. The author recently obtained the CIPP/US certification and hopes to apply the privacy and cybersecurity knowledge she cultivated over the years to the ever-changing challenges of data protection. The author would like to express gratitude to all Stetson Law professors, specifically Professor Mason Clark and Professor Roy Balleste, for their support and guidance navigating this field. The author also thanks her family and friends for their unwavering encouragement. This article is dedicated to Luna, Kobe, and Benji.

*"[S]upreme excellence consists in breaking the enemy's resistance without fighting."*

— Sun Tzu[1]

## *I. INTRODUCTION*

Approximately ninety-two cyberattacks will occur during the time it takes to read this article. A University of Maryland study found that, on average, there is one cyberattack every thirty-nine seconds around the world.[2] This haunting statistic puts into perspective the magnitude of international cybercrime. It explains why 156 nations, including the United States, Russia, China, and Iran, have taken measures to combat the ever-increasing problem of cybercrime.[3] What happens, however, when nations perpetuate cybercrime against other nations? These so-called cross-border, aggressive, state-sponsored cyberattacks are an increasing international problem. Since 2005, there have been at least 247 cyberattacks sponsored by China, 174 by Russia, 97 by Iran, and

1. SUN TZU ON THE ART OF WAR: THE OLDEST MILITARY TREATISE IN THE WORLD 8 (Lionel Giles trans., Allandale Online Publ'g 2000).

2. *Study: Hackers Attack Every 39 Seconds*, A. JAMES CLARK SCH. OF ENG'G (Feb. 8, 2007), https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.

3. *Cybercrime Legislation Worldwide*, UNITED NATIONS CONF. ON TRADE AND DEV., https://unctad.org/page/cybercrime-legislation-worldwide (last visited Apr. 4, 2023).

89 by North Korea.[4] These four nations account for seventy-seven percent of all suspected cyber operations sponsored by state actors.[5]

This comment examines the applicability of current international laws of war to cross-border attacks sponsored by state actors. It is apparent that the laws of the United Nations' ("UN") Charter are insufficient to address cyberattacks. The international arena must devote its efforts to working on an International Cyber Treaty ("Cyber Treaty") that addresses state-sponsored cyberattacks. The Cyber Treaty should clarify conflicting standards and fill gaps in current international law. This comment examines the feasibility of the Cyber Treaty considering the key players' conflicting interests.

Part II addresses the *jus ad bellum* principles of international law: UN Charter Articles 2(4) and 51 and their applicability to cyber-attacks. Part III examines the Russian-sponsored 2007 Estonia Distributed Denial of Service ("DDoS") Attack and its applicability to the laws of war. Part IV highlights the intersection between cybersecurity and outer space, including the increasing concern for satellite cyberattacks. Moreover, this Part discusses the differences and similarities between the legal instruments of space law and cyber law. Part V proposes an International Cyber Treaty that fills in the gaps left by applying Articles 2(4) and 51 to state-sponsored cyberattacks.

## *II. INTERNATIONAL LAW AND CYBER ATTACKS*

### A. Applicable International Law

The UN is the most influential international organization that creates and codifies international law.[6] The UN Charter contains

4. *Cyber Operations Tracker*, COUNCIL ON FOREIGN RELATIONS, https://www.cfr.org/cyber-operations/ (last visited Apr. 4, 2023).

5. *Id.*

6. *See* Edward Shils, *The Failure of the United Nations Atomic Energy Commission: An Interpretation*, 15 U. CHI. L. REV. 855 (1948) (criticizing the UN's handling of atomic energy via the Atomic Energy Commission); W. Paul Gormley, *The Unilateral Extension of Territorial Waters: The Failure of the United Nations to Protect Freedom of the Seas*, 43 U. DET. L.J. 695 (1966) (pointing out the UN's failure to reach an agreement on the international laws of the sea); Molly McGregor, *Uninformed Consent: The United Nations' Failure to Appropriately Police Clinical Trials in Developing Nations*, 31 SUFFOLK TRANSNAT'L L. REV. 103 (2007) (addressing the UN's shortfall in addressing clinical trials

many significant laws, including Article 2(4),[7] arguably one of the most important rules of modern international law.[8] Articles 2(4) and (51)[9] of the UN Charter codify the international law concept of *jus ad bellum*, which is the international law governing states going to war ("laws of war"). The Tallinn Manual on the International Law Applicable to Cyber Operations[10] ("Tallinn Manual" or "Manual") defines *jus ad bellum* as "international law governing a State's resort to force as an instrument of its national policy."[11] Plainly stated, this principle lays out the circumstances under which states could permissibly go to war. The core of *jus ad bellum* lies in the general prohibition against states using force on one another, found in Article 2(4), coupled with two exceptions in Articles 39 and 51. Working together with *jus ad bellum* is the international law principle of *jus in bello*, which governs a state's conduct once already engaged in war.[12] Applying *jus in bello* to cyberattacks is also a complex discussion topic that has earned scholars' attention. This comment, however, focuses on applying *jus ad bellum* only to cyberattacks.

### *1. Threat or Use of Force*

Article 2(4) of the UN Charter declares that:

> All members shall refrain in their international relations from the threat or use of force against the territorial integrity or

in developing nations). *But see* Julia Zorthian, *5 United Nations Achievements Worth Celebrating on U.N. Day*, TIME (Oct. 23, 2015, 6:20PM), https://time.com/4085757/united-nations-achievements/. (listing major UN accomplishments including pyramid preservation, smallpox eradication, and arms control promotion).

7. U.N. Charter art. 2, ¶ 4.

8. Anthony D'Amato, *The Meaning of Article 2(4) in the U.N. Charter* 1 (Nw. U. Sch. L. Pub. L. & Legal Theory Series Working Paper, Research Paper No. 13–30, 2013).

9. U.N. Charter art. 51.

10. The Tallinn Manual is a NATO-sponsored project comprised of an "International Group of Experts" assembled by the Cooperative Cyber Defense Center of Excellence ("CCDCOE") in Estonia. The Tallinn Manual, now in its second edition, provides rules and guidance on the application of international law to cyber operations. While the Manual is non-binding, it has become "an influential resource for legal advisers and policy experts dealing with cyber issues." *The Tallinn Manual,* CCDCOE, https://ccdcoe.org/research/tallinn-manual/ (last visited Apr. 23, 2023) [hereinafter *The Tallinn Manual*].

11. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 328-329 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

12. Noah Simmons, *A Brave New World: Applying International Law of War to Cyber-Attacks*, 4 J.L. & CYBER WARFARE 42, 49 (2014).

> political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations. [13]

The age-old question is: What did the UN mean by "force"?[14] The answer is, of course, it depends. Before diving into the different interpretations of the word "force," it is helpful to understand the historical events that led to the adoption of Article 2(4). The core of Article 2(4) traces back to the end of World War I when the League of Nations declared that "any war or threat of war" was of concern to the world.[15] The development of Article 2(4) continued with the signing of the Kellogg-Briand Pact, which condemned states resorting to war and ended in 1945 with the formal signing of the UN Charter, formally establishing the UN and articulating Article 2(4).[16] The events leading up to the formal recitation of Article 2(4) include the two World Wars, which along with the UN's aim "to save succeeding generations from the scourge of war,"[17] suggests a focus on the use of force by way of military instruments.[18] This determination also paves the way for the dominant view that Article 2(4) prohibits physical armed force only, as opposed to, for example, force as coercion.[19]

It is generally accepted and historically understood that force under Article 2(4) requires "armed force."[20] In support of this view, the UN Charter's preamble states that "armed force shall not be used, save in the common interest."[21] In addition, Article 51

13. U.N. Charter art. 2, ¶ 4.

14. Tom Ruys, *The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: are "Minimal" uses of Force Excluded From UN Charter Article 2(4)?*, 108 AM. J. INT'L L. 159, 164 n. 31 (2014).

15. Edward Gordon, *Article 2(4) in Historical Context*, 10 YALE J. INT'L L. 271, 273 (1985).

16. *Id.* at 274.

17. U.N. Charter pmbl.

18. Michael Gervais, *Cyber Attacks and the Laws of War*, 1 J.L. & CYBER WARFARE 8, 27 (2012).

19. Christopher D. DeLuca, *The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors*, 3 PACE INT'L L. REV. ONLINE COMPANION 278, 294 (2013); James A Delano. *"Force" Under Article 2(4) of the United Nations Charter: The Question of Economic and Political Coercion*, 12 VAND. J TRANSNAT'L. L. 101, 103 (1979) ("[T]he traditional view interprets article 2(4) of the United Nations Charter as referring only to military force."); *See also* Oona A. Hathaway & Rebecca Crootof, *The Law of Cyberattack*, 100 CALIF. L. REV. 817, 842 (2012).

20. Stephen Moore, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C. J. INT'L L. & COM. REGUL. 223, 236 (2013); Daniela Danca, *The Applicability of International Law to Cyber Attacks*, 2013 INT'L CONF. EDUC. & CREATIVITY FOR KNOWLEDGE-BASED SOC'Y 36, 38 (Rom.).

21. U.N. Charter pmbl.

(discussed below) references self-defense against *armed attacks*.[22] The problem with this strict interpretation is that only instances of military violence would violate Article 2(4), and states may only exercise the right of self-defense under Article 51 from armed military violence of another state.[23]

#### *2. Exceptions to Prohibition on Threat or Use of Force*

Article 2(4)'s prohibition on the use of force is subject to two exceptions: force may be allowed if the UN Security Council determines such force is needed to restore the peace[24] and if a state is acting in self-defense.[25] Article 51 codifies the latter exception providing that:

> [n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.[26]

The UN left the term "armed attack" undefined, which leads to competing interpretations of the term's intended meaning.[27] What is clear from Article 51 is that the right of self-defense is based on principles of necessity and proportionality.[28] A state's use of force under Article 2(4) might be legitimate under Article 51 only if there was an armed attack before the claim of self-defense, meaning Article 51 does not protect preemptive state attacks.[29]

### B. Applicability and Sufficiency of *Jus Ad Bellum* to Cyberattacks

Before applying Articles 2(4) and 51 to cyberattacks, it is necessary first to define a cyberattack. Starting with what a cyberattack is *not*, a cyberattack is not the same thing as

22. U.N. Charter art. 51 (emphasis added).
23. 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, 428 (2011).
24. U.N. Charter art. 39.
25. U.N. Charter art. 51.
26. *Id.*
27. *Id.*
28. Moore, *supra* note 21, at 238.
29. *Id.*

cybercrime.[30] Cybercrime, such as fraud perpetuated via a computer, is governed by national criminal law.[31] More importantly, cybercrime does not implicate Articles 2(4) and 51 because it is not *armed* conflict between states.[32] There are many definitions of "cyberattack."[33] The Tallinn Manual defines a cyberattack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[34] This definition focuses on violence against an adversary and emphasizes that the consequences, not the nature of the operation itself, must be violent to be considered an attack.[35] Additionally, the Manual's definition does not limit the definition to attacks that result in kinetic force, for instance, an aerial bombing of a cyber control building.[36]

Regarding the application of Articles 2(4) and 51, there is increasing agreement among states and scholars that these rules apply to cyberattacks.[37] States in agreement include the United States, the United Kingdom, and Estonia.[38] The Tallinn Manual

30. DeLuca, *supra* note 20, at 281.

31. *Id.*

32. *Id.*

33. Waxman, *supra* note 24, at 422 (characterizing cyberattacks as "efforts to alter, disrupt, or destroy computer systems or networks of the information or programs on them"); *Computer Security Resource Center: Cyber Attack*, NAT'L INST. STANDARDS & TECH., https://csrc.nist.gov/glossary/term/Cyber_Attack (last visited April 5, 2023) (defining cyberattack as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"); Oona A. Hathaway & Rebecca Crootof, *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 826 (2012) (defining cyberattack as "any action taken to undermine the functions of a computer network for a political or national security purpose").

34. TALLINN MANUAL 2.0, *supra* note 12, at 415.

35. *Id.*

36. *Id.*

37. Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace,* STRATEGIC STUD. Q., Fall 2012, 126, 127; Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. INT'L L.J. ONLINE 1, 2–4 (2012); Brian J. Egan, *International Law and Stability in Cyberspace,* 35 BERKELEY J. INT'L L. 169, 170–71 (2017).

38. *See* EXEC. OFF. OF THE PRESIDENT, OMB NO. 0704-0188, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2015), https://apps.dtic.mil/sti/pdfs/ADA543951.pdf (stating "[l]ong-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace"); Jeremy Wright, UK Att'y Gen., Cyber and International Law in the 21st Century, Address at Chatham House Royal Institute for International Affairs (May 23, 2018) (saying "[t]he UK has always been clear that we consider cyber space to be an integral part of the rules based international order that we are proud to promote") (transcript available in official government speech archives located at https://www.gov.uk/government/speeches/cyber-

also supports this conclusion: "[b]oth International Groups of Experts were unanimous in their estimation that existing international law applies to cyber operations."[39]

Difficulties arise when applying the laws of war to cyberattacks due to the traditional language of the Articles.[40] It is through no fault of their own, however, that the UN's founders did not foresee the current modern digital world and the possibility of cyberattacks before the signing of the UN Charter in 1945. In fact, the International Court of Justice declared that Articles 2(4) and 51 "appl[y] to any use of force, regardless of the weapons employed" in their analysis of whether the use of nuclear weapons constituted force.[41] As such, the inquiry is not whether *jus ad bellum* applies to cyberattacks but *how* to successfully apply these traditional law principles to this non-traditional weapon. The difficulty of applying Articles 2(4) and 51 to cyberattacks lies in the attacks' nature.[42] Cyberattacks are virtual, complex, anonymous, and can cause catastrophic injury to millions, potentially billions, of people, with some simple lines of code.[43] The unique features of cyberattacks pose difficulties when applying the currently accepted definitions of "force" and "armed attack," leading to the conclusion that the current laws of war may be insufficient to confront this problem.[44]

### *1. Threat or Use of Force Revisited*

Concerning force under Article 2(4), the primary consideration is whether a cyberattack rises to the level of armed force required under the traditional definition. There are six helpful factors to determine whether a cyberattack rises to the level of armed force.[45] These factors are severity, immediacy, directness, invasiveness,

---

and-international-law-in-the-21st-century); Kersti Kaljulaid, Former President of the Republic of Estonia, Remarks at the Opening of CyCon 2019 (May 29, 2019) (stating "[w]e believe and state that both the rights and obligations of international law, including those stated in the U.N. Charter, do apply to states when using IT and communication technologies").

39. TALLINN MANUAL 2.0, *supra* note 12, at 3.

40. *See* discussion *infra* Sections II.B.1, II.B.2.

41. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8).

42. Simmons, *supra* note 13, at 51.

43. *Id.*

44. *Id.* at 52.

45. 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, 914–15 (1999).

measurability, and presumptive legitimacy.[46] Using these factors, a computer network attack on an air traffic control system that results in a plane crashing would be considered armed force, allowing Article 2(4) to apply due to the severity of the attack.[47] Schmitt's framework, like the Tallinn Manual's definition of cyberattack, focuses on the *consequences* of the attack to determine if it rises to the level of armed force. On the other hand, a cyberattack on a university network designed to disrupt military research on campus would not rise to the level of armed force under these factors.[48] The low severity of the university attack, coupled with minimal consequences, fails to "resemble that characteristic of uses of armed force."[49]

### *2. Exceptions to the Prohibition on Threat or Use of Force Revisited*

Likewise, Article 51 also begs the question of whether a cyberattack rises to the level of an armed attack required for a state to enjoy the right of self-defense. Article 51 is seemingly narrower than Article 2(4), meaning that not all uses of force qualify as armed attacks.[50] There are three factors to consider whether a cyberattack constitutes an "armed attack."[51] These factors include the consequences of the attack, the state's consideration of aggressive intent, and the repetitive or isolated nature of the attack.[52] Consistent with the meaning of armed *force* under Article 2(4), the consequences of an armed *attack* must rise to a certain level in severity for a state to be justified in using self-defense.[53] Using these factors, a severe DDoS attack against the United States that cripples infrastructure would be considered armed force due to the severity.[54] In this scenario, the United States can respond with an armed force to defend itself, granted it abides by the principles of necessity and proportionality, and the attack can be attributed to a state actor.[55] A state's right to use

46. *Id.*
47. *Id.* at 916.
48. *Id.*
49. *Id.* at 917.
50. Moore, *supra* note 21, at 238.
51. Simmons, *supra* note 13, at 87–97.
52. *Id.*
53. *Id.* at 88.
54. *Id.* at 99.
55. *Id.*

armed force after a cyberattack raises the question of what type of force it may use to defend itself, which this Comment addresses in the proceeding Section.

### *3. Application of Jus Ad Bellum to Cyberattacks is Insufficient*

While it is possible to apply *jus ad bellum* to cyberattacks, the laws are insufficient to regulate cyberattacks due to the traditional interpretation of the laws. One of the most significant difficulties in applying Article 2(4) to cyberattacks is that the traditional definition of "armed force" focuses on force carried out physically and having a physical effect, such as a conventional bomb.[56] This interpretation would be too narrow for cyberattacks, considering the non-physical nature of cyberattacks. Although a cyberattack may trigger a physical reaction, much of the concern regarding cyberattacks surrounds a state's loss or destruction of data.[57] Second, even using the more expansive definitions of *force* that focus on the attack's consequences presented by Schmitt and the Tallinn Manual, the threshold for these factors is unclear. For example, the Estonia DDoS attack[58] merely caused confusion and unrest, even though the attack was on Estonia's infrastructure.[59] Under Schmitt's and the Manual's framework, would the Estonia cyberattack rise to the level of armed force, even though its consequences were minimal and trivial?[60] The answer is unclear, considering the ambiguous definitions and traditional understanding of "armed force." Even using broad interpretations of "force," many ambiguities surround applying Article 2(4) to cyberattacks.

Applying Article 51 to cyberattacks is also problematic due to the issue of attribution. Attribution is a crucial step to claims of self-defense under Article 51.[61] A state must know the perpetrator's identity to retaliate under Article 51.[62] Cyberattacks are distinguishable from conventional attacks because there are no soldiers, physical presence, or weapons to determine the

56. *Id.* at 79–80.
57. *Id.* at 80.
58. *See* discussion *infra* Section III.A.
59. DeLuca, *supra* note 20, at 298.
60. For contradicting answers to this question, see discussion *infra* Section III.A.1.
61. Moore, *supra* note 21, at 242.
62. *Id.*

attacker.[63] In fact, perpetrators of cyberattacks actively disguise their identities by altering IP addresses.[64] Even more dangerous is that a state may launch a cyberattack under the guise of originating from another state, effectively masking its identity and potentially instigating a retaliatory armed attack against the wrong state.[65] A state should not utilize Article 51's right to self-defense if it cannot determine where the cyberattack originated. However, what if a state *believes* it knows which state launched the attack? Under the current laws of war, nothing prevents a state from using the right of self-defense in this scenario.[66] It is unclear if a state would be justified in launching a retaliatory armed attack if it was mistaken as to the attacker's identity.

Along these lines of retaliation, the type of force a state may use in retaliation is also ambiguous. Using the example of the severe DDoS attack against the U.S., the question is: Provided the U.S. knows which state perpetuated the attack, could the U.S. launch its own attack against the state and cripple that state's infrastructure? The U.S. would be bound to retaliate using another "pure cyberattack" (meaning no physical effect), considering the principles of necessity and proportionality.[67] However, what if, for some reason, a "pure cyberattack" was not a viable option for the U.S.? Could the U.S. respond with physical force, or must it forego its right of self-defense? Once again, the current laws of war do not answer this question.

Another problematic element of the laws of war is that non-state actors cannot violate Article 2(4) because it applies only to state actors.[68] It is common practice for governments to contract individuals or groups of hackers to attack states.[69] If a non-state actor carries out a cyberattack, the attacked state cannot enjoy the right of self-defense under Article 51. In addition, under the current principles of *jus ad bellum*, terrorist groups like al-Qaeda may launch cyberattacks against states with (in theory) no retaliation since al-Qaeda is not a state actor. Once again, this

63. Simmons, *supra* note 13, at 100-01.
64. *Id.* at 101.
65. *Id.*
66. *Id.* at 101-03.
67. *See Id.* at 76-77.
68. *Id.* at 102-03.
69. *Id.* at 103; *See* Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L. 525, 546-48 (2012).

appears to be the wrong conclusion, especially considering the large number of non-state actors that launch cyberattacks.

## *III. CROSS-BORDER AGGRESSIVE CYBERATTACKS BETWEEN STATE ACTORS*

### A. Estonia DDoS Attack

In 2007, Estonia became the first victim of a cyberattack sponsored by a state actor.[70] The cyberattacks were in response to the Estonian government's choice to relocate a Soviet-era statue from the center of Tallinn to a military cemetery on the outskirts of Tallinn.[71] The type of attack utilized was the Distributed Denial of Service ("DDoS"), one of the most commonly used cyberattacks.[72] DDoS attacks work by overwhelming a site with fake requests to the point that the site cannot respond to all requests, and subsequently, the site crashes.[73] The DDoS attacks targeted the Estonian "government and parliamentary portals, ministries, news outlets, internet service providers, major banks, and small businesses."[74] These attacks profoundly affected Estonia's infrastructure due to the state's heavy reliance on the Internet.[75] This tiny nation, dubbed e-Estonia, is at the forefront of e-democracy[76] and is recognized as the world's most advanced digital society.[77] The sites of the two biggest Estonian banks were offline for about forty-five to ninety minutes, blocking access to simple financial tasks such as accessing or transferring money.[78] Also, the

70. *Estonian Denial of Service Incident*, COUNCIL ON FOREIGN RELATIONS (MAY 2007), https://www.cfr.org/cyber-operations/estonian-denial-service-incident.

71. Damien McGuinness, *How a Cyber Attack Transformed Estonia*, BBC (Apr. 27, 2017), https://www.bbc.com/news/39655415.

72. *Types of Cyber Attacks*, FORTINET, https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks (last visited Sep. 1, 2024).

73. *Id.*; *See also* Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602, 611-12 (2011).

74. JAMES PAMMENT, ET AL., *2007 Cyber Attacks on Estonia*, *in* HYBRID THREATS: A STRATEGIC COMMUNICATIONS PERSPECTIVE 52, 52 (2019), https://stratcomcoe.org/pdfjs/?file=/publications/download/cyber_attacks_estonia.pdf?zoom=page-fit.

75. *Id.*

76. *See Facts & Figures*, E-ESTONIA, *https://e-estonia.com/facts-and-figures/* (last visited Aug. 6, 2024) (highlighting Estonia's many electronic services such as online voting and tax submissions, e-banking and the e-residency program).

77. Susan Fourtané, *e-Estonia: The World's Most Advanced Digital Society*, INTERESTING ENG'G (Feb. 24, 2020, 12:03 PM), https://interestingengineering.com/innovation/e-estonia-the-worlds-most-advanced-digital-society.

78. Pamment, *supra* note 75, at 61.

Estonian government had to rapidly acquire alternative web hosting sites, costing approximately billions of Euros.[79]

Regarding responsibility, no concrete evidence exists attributing the cyberattack to a state. However, there is information available to suggest that Russia could have been at least indirectly responsible for the attacks.[80] Evidence of Russian responsibility included IP addresses tracing back to the computers of Russian government agencies, the Russian government's refusal to assist the Estonian government in resolving the attacks,[81] and DDoS online attack instructions written in Russian.[82] Furthermore, Russia severed commercially important railways with no prior notice for alleged repairs during the attacks.[83] While the Russian government completely denies responsibility,[84] the overwhelming evidence points to some Russian government orchestration, especially considering the funding needed for such attacks.[85] However, since no "smoking gun" proves Russian government involvement, it is difficult to attribute the attack to Russia properly. There was, however, one conviction in connection with the cyberattacks. Dmitri Galuškevitš, an Estonian student of Russian origin, was convicted for targeting a political party's website.[86] The size of the operation suggests many others were responsible for the attacks, however, due to Russia's non-cooperation, the rest remain without any repercussions.[87]

### *1. Applying Articles 2(4) and 51*

Applying the laws of war to the Estonian cyberattacks yields contradicting results, showing exactly why another solution is

79. *Id.* at 53.

80. *See* McGuinness, *supra* note 72.

81. Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, *in* PROCEEDINGS OF THE 7TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY 163, 166 (2008), https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (the Estonian government made a formal investigation request to the Russian government in May 2007 to find hackers living in Russia, a request that was never responded to despite the Mutual Legal Assistance Treaty signed by the two countries).

82. Pamment, *supra* note 75, at 53.

83. *Id.*

84. *Id.* at 58 (Sergei Ivanov, Former First Deputy Prime Minister, Vladimir Putin, President, and Sergey Viktorovich Lavrov, Foreign Minister, all claim Estonia's claim of Russian interference is a lie); *See also* Ottis, *supra* note 82, at 166.

85. *Id.* at 61.

86. Ottis, *supra* note 82, at 165.

87. *Id.* at 166.

needed. Michael Schmitt applies his "use of force" framework and concludes that the Estonian cyberattacks rose to the level of "armed force."[88] Schmitt cites the severe consequences of the attack, such as the disruption of government function and services, economic turmoil, and adverse effects on the Estonian people.[89] Likewise, Schmitt reasons the attacks were immediate, direct, invasive, and presumably illegitimate.[90] Schmitt concedes there is difficulty quantifying the consequences of the cyberattack as the only factor opposing the conclusion. Balancing all the elements, Schmitt concludes, "the incident arguably reached the use-of-force threshold."[91]

Interestingly, Reese Nguyen comes to the opposite conclusion using this same framework on the Estonian cyberattacks.[92] Nguyen claims (1) the cyberattacks were not that severe due to lack of injury and destruction; (2) the consequences were delayed; (3) the effects were not directly tied to the DDoS attacks; (4) there was minimal invasion due to the remote execution of the cyberattacks; (5) the consequences were difficult to quantify; and (6) since the attacks were legitimate because they were limited to telecommunication systems.[93] Using the same (widely accepted[94]) framework to determine whether a cyberattack amounts to the "use of force" and reaching contradictory conclusions exposes the inadequacy of applying *jus ad bellum* to cyberattacks. Notwithstanding the contradictory framework of Article 2(4), applying Article 51 to the Estonian cyberattacks would also be problematic. Since the cyberattacks were not adequately attributed to Russia, Estonia could not use the right of self-defense outlined in Article 51. Even more problematic is that the cyberattacks against Estonia were carried out by non-state actors, meaning Articles 2(4) and 51 would not apply to them.

88. Michael N. Schmitt, *Cyber Operations and the Jud Ad Bellum Revisited*, 56 VILL. L. REV. 569, 577 (2011).

89. *Id.*

90. *Id.*

91. *Id.*

92. Reese Nguyen, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1123 (2013).

93. *Id.* at 1123-24.

94. TALLINN MANUAL 2.0*, supra* note 12, at 334-36 (the Tallinn Manual uses eight almost identical factors to determine whether a cyberattack amounts to force).

### *2. NATO Article 5*

Another aspect of this cyberattack is the implication of NATO Article 5,[95] which would evoke a collective defensive response against Russia from NATO members.[96] Some experts speculate that the Russian government purposefully fell short of the threshold for invoking Article 5 due to the severe repercussions it may face from NATO's collective defense.[97] While Article 5 was not invoked in the Estonia cyberattacks, it is clear that NATO will defend its allies against a cyberattack.[98] Article 5 serves as another layer of defense for NATO countries against serious cyberattacks, a resource that should be used more often.

## B. Cyberattacks Between Russia and Ukraine

While there is a physical war between Russian and Ukraine,[99] the battle is also occurring in cyberspace. Russian cyberattacks against Ukraine began as early as 2014.[100] Three days before the referendum vote on the status of Crimea, Russia launched an eight-minute DDoS cyberattack against Ukraine to "destabilize communications and spread confusion whilst troops overran the region."[101] Also in 2014, a pro-Russian hacking group carried out cyberattacks to manipulate voting in the Ukrainian presidential election.[102] The hackers targeted the Central Election Commission in an attempt to change election results.[103] More notably, in 2015 Russia carried out another DDoS attack that affected energy

95. North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

96. Jens Stoltenberg, *NATO Will Defend Itself*, NATO, https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en (Aug. 29, 2019, 16:38) ("A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all.").

97. *See* Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, J. STRATEGIC SEC., Summer 2011, at 49, 53 ("Because of economic interdependence and the threat of nuclear escalation, Russia cannot risk attacks on NATO member states.").

98. Stoltenberg, *supra* note 97.

99. Madeline Fitzgerald & Elliot Davis Jr., *Russia Invades Ukraine: A Timeline of The Crisis,* U.S. NEWS & WORLD REP., https://www.usnews.com/news/best-countries/slideshows/a-timeline-of-the-russia-ukraine-conflict (Feb. 22, 2024, 1:44 PM).

100. Jakub Przetacznik with Simona Tarpova, *Russia's War on Ukraine: Timeline of Cyber-Attacks*, EUR. PARLIAMENTARY RSCH. SERV. 1, 1 (2022), https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549.

101. Joe Tidy, *Ukraine Cyber-Attack: Russia to Blame for Hack, says Kyiv,* BBC (Jan. 14, 2022), https://www.bbc.com/news/world-europe-59992531.

102. Przetacznik, *supra* note 101, at 3.

103. *Id.*

distribution companies and left over 230,000 Ukrainian citizens without power for one-to-six hours.[104] The infamous Russian hacking group, Sandworm, is attributed to this cyberattack.[105] The destructive attack is believed to be the first example of a power outage caused by a cyberattack.[106] The malware used in this attack is called "BlackEnergy," a malware also known to have compromised NATO, many Western European countries, and energy companies.[107]

Prior to Russia's invasion of Ukraine on February 24, 2022, cyberattacks from Russia soared in early 2022.[108] On January 14, 2022, Russian hackers brought down seventy Ukrainian government websites, including the Ministry of Foreign Affairs and the Ministry of Education.[109] Before the sites went down, a message appeared in Ukrainian, Russian, and Polish that read "Prepare for the worst" and warned Ukrainian citizens, "All your personal data has been sent to a public network. All data on your computer is destroyed and cannot be recovered."[110] Right before the invasion on February 14, 2022, a DDoS attack targeted websites of Ukraine's armed forces, public radio, and two of the biggest national banks.[111] The cyberattack brought down the banks for two hours and rendered the mobile apps and online payments inoperable.[112] Following Russia's invasion, a number of cyberattacks ensued, including the KA-SAT satellite network[113] and more cyberattacks on Ukraine's digital infrastructure blocking access to financial services and energy.[114] Another notable interruption includes a cyberattack on a Ukrainian radio station

104. *Id.*

105. Alex Hern, *Ukrainian blackout caused by hackers that attacked media company, researchers say*, THE GUARDIAN (Jan. 7, 2016, 8:20 AM), https://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company.

106. *Id.*

107. *Id.*

108. Cynthia Brumfield, *Russia-linked cyberattacks on Ukraine: A Timeline,* CSO (Aug. 24, 2022), https://www.csoonline.com/article/571865/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html.

109. *Id.*

110. *Id.*

111. Daryna Antoniuk, *DDoS attacks hit Ukrainian government websites,* THE RECORD (Feb. 14, 2022), https://therecord.media/ddos-attacks-hit-websites-of-ukraines-state-banks-defense-ministry-and-armed-forces.

112. *Id.*

113. *See* discussion *infra* Section IV.A.1.i.

114. Przetacznik, *supra* note 101, at 2.

that spread a false message that the Ukrainian President was under intensive care.[115]

While Ukraine has been successful at fighting off the bombardment of cyberattacks since the Russian invasion, experts are speculating that Russia may be holding back[116] and is set to escalate its cyberattacks against Ukraine.[117] In its February 2023 Threat Analysis Group, Google assessed Russia will "increase disruptive and destructive attacks in response to developments on the battlefield that fundamentally shift the balance . . . toward Ukraine."[118] Cyber threat group, Recorded Future, also noted in its February 2023 report that "in the near term, Russia will very likely launch a renewed offensive in Ukraine."[119]

If the prediction of increased cyberattacks is true, invoking Articles 2(4) and 51 should be considered. Applying Article 51's use of self-defense might not be problematic in this instance because the cyberattacks against Ukraine have already been attributed to Russia, and it is clear any further cyberattacks will also be attributed to the Russian government. The familiar problem would be applying Article 2(4). The definition of "armed force" is extremely limited and traditionally includes only physical force and effects. However, considering more modern interpretations of "armed force," an argument could be made that the consequences of Russia's cyberattack are not minimal. If Russia plans to ramp up its cyberwarfare, Russia may be successful at shutting down Ukraine's electric grid as it has tried in the past. As mentioned before, the ambiguity of what constitutes "armed force" makes it difficult to apply this law. However, an attack of this magnitude may be enough to trigger Article 2(4), regardless of any physical destruction.

---

115. Brumfield, *supra* note 109.

116. Natasha Ishak, *Is Russia holding back from cyberwar?,* VOX (March 19, 2022, 3:58 PM), https://www.vox.com/2022/3/19/22986316/russia-ukraine-cyber-attacks-holding-back.

117. John Sakellariadis and Maggie Miller, *Ukraine gears up for new phase of cyber war with Russia,* POLITICO (February 25, 2023, 7:00 AM), https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429.

118. Shane Huntley, *Fog of war: how the Ukraine conflict transformed the cyber threat landscape,* THREAT ANALYSIS GROUP (Feb. 16, 2023), https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

119. Insikt Group, *Themes and Failures of Russia's War Against Ukraine,* RECORDED FUTURE (Feb. 9, 2023), https://www.recordedfuture.com/themes-failures-russias-war-against-ukraine.

## C. Threats from China and Iran

### *1. China*

In its 2023 Annual Threat Assessment, U.S. Cybersecurity & Infrastructure Security Agency ("CISA") opined that "China remains the most active and persistent cyber threat to the U.S. Government, private sector, and critical infrastructure networks."[120] For decades, the People's Republic of China has engaged in malicious cyberattacks against U.S. institutions, "including healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms."[121] According to data from CrowdStrike, China was responsible for sixty-seven percent of state-sponsored cyberattacks "motivated both by intellectual property (IP) theft and intelligence gathering objectives" in 2021.[122] Compared with just seven percent for the Iranian government and one percent for the Russian government, China's stunning cyber involvement presents the biggest threat to U.S. business and government. [123]

China's malicious cyberattacks came to the forefront with Operation Aurora in January 2010.[124] Operation Aurora was a series of attacks from China that compromised many U.S. companies such as Yahoo, Adobe, Dow Chemical, and Google.[125] Google was the only company to publicly come forward and announce that the Gmail accounts of Chinese human rights activists had been compromised.[126] As a result of this attack and

120. *People's Republic of China Cyber Threat,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china (last visited Aug. 31, 2024)..

121. *China Cyber Threat Overview and Advisories*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://web.archive.org/web/20221202134121/https://www.cisa.gov/uscert/china (last visited Aug. 31, 2024).

122. CROWDSTRIKE, NOWHERE TO HIDE, 2021 THREAT HUNTING REPORT 3, 13 (2021), https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021ThreatHunting.pdf (last visited Aug. 31, 2024).

123. *Id.* at 12.

124. *Council on Foreign Relations*, *supra* note 5.

125. *Id.*

126. *Id.*

other censorship requests by the Chinese government,[127] Google ceased its operations in China.[128]

More recently, Microsoft warned that Chinese state-sponsored hackers compromised critical U.S. and Guam government infrastructures.[129] Microsoft attributes these attacks to the Chinese hacking group "Volt Typhoon," a hacking group that has been active since 2021.[130] According to Microsoft, Volt Typhoon's most recent campaign affected "communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education."[131] This hacking group works by stealing user credentials to gain access into corporate systems.[132] Microsoft contends Volt Typhoon is not interested in causing major disruption, but rather "intends to perform espionage and maintain access without being detected for as long as possible."[133]

### *2. Iran*

Also, in its 2023 Annual Threat Assessment, CISA stated, "Ahead of the U.S. election in 2024, Iran may attempt to conduct influence operations aimed at U.S. interests, including targeting U.S. elections, having demonstrated a willingness and capability to do so in the past."[134] While Iran has not carried out massive cyberattacks against the United States in recent years, its cyber history is spectacular and damaging.

---

127. *Google Co-Founder on Pulling out of China*, SPIEGEL (Mar. 3, 2010), https://www.spiegel.de/international/business/google-co-founder-on-pulling-out-of-china-it-was-a-real-step-backward-a-686269.html (Google co-founder Sergey Brin stated "[w]e got far more requests for censorship of topics and queries. Furthermore, a number of our other services like YouTube were completely blocked from the country. It was a real step backward, we felt.").

128. *Council on Foreign Relations*, *supra* note 5.

129. Microsoft Threat Intelligence, *Volt Typhoon targets US critical infrastructure with living-off-the-land techniques*, MICROSOFT (May 24, 2023), https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.*

134. Cybersecurity & Infrastructure Security Agency, *Iran Cyber Threat Overview and Advisories,* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran (last visited Aug. 31, 2024).

Iran's cyber capabilities can be traced to June 2009, following mass protests after the alleged fraudulent Iranian presidential election.[135] The mass mobilization of cyber activities became known as the Green Movement, marking one of the first known targets of Iran's operations.[136] During this era, pro-Iran hackers engaged in many malignant cyber-attacks, including defacing websites associated with pro-opposition forces, social media platforms, and Israeli businesses. [137] This era of severe and aggressive cyberattacks resulted in one of the largest security breaches in internet history. An Iranian intelligence agency hacker broke into a Dutch Security Company, called DigiNotar, and issued fraudulent encryption certificates, which allowed the Iran to spy on all Iranian Gmail users.[138] The hacker breached the company by adding a rule in a router that forced Google's traffic through another route inside the country.[139]

While most victims of Iran's cyberattacks are Iranian or surrounding countries, Iran has carried out major cyberattacks on U.S. banks.[140] In March 2016, the U.S. Department of Justice unsealed an indictment of "seven Iranian individuals who were employed by two Iran-based computer companies, ITSecTeam (ITSEC) and Mersad Company (MERSAD), that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps, on computer hacking charges related to their involvement in an extensive campaign of over 176 days of distributed denial of service (DDoS) attacks."[141] The DDoS attacks allowed the hackers access to forty-six financial institutions, including "Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T and HSBC."[142] Some days, the cyberattacks overwhelmed computer servers with as

135. Collin Anderson and Karim Sadjadpour, *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*, CARNEGIE ENDOWMENT FOR INT'L PEACE 9, 10 (2018), https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.

136. *Id.* at 11.

137. *Id.*

138. *Id.*

139. *Id.* at 60.

140. *Id.* at 6.

141. Press Release, U.S. Dep't. of Just., Office of Pub. Affairs, Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector (Mar. 24, 2016) (on file with author).

142. *The Iranian Cyber Threat*, UNITED AGAINST NUCLEAR IRAN, https://www.unitedagainstnucleariran.com/history-of-iranian-cyber-attacks-and-incidents (last visited Aug. 31, 2024).

much as 140 gigabits of data per second.[143] As such, hundreds of thousands of customers lost access to their online bank accounts, and banks paid tens of millions of dollars in remediation costs.[144]

## *IV. SPACE LAW CONSIDERATIONS*

### A. Applicability of Cybersecurity in Outer Space

While pairing cyberspace and outer space together may be unusual, the two are inextricably connected. Essential outer space services like the GPS require complex technology and software.[145] It is this very same reliance technology that exposes space objects to cyberattacks.[146]

#### *1. Satellites*

Cyberattacks against outer space satellites are of increasing concern due to the consequences such an attack would have on everyday life.[147] Satellites are used for banking, power grids, farming, military defense, television programming, weather services, and more.[148] A successful cyberattack on a satellite could threaten a country's power grid or leave millions of people without communication services.[149] Some new satellites are equipped with "thrusters" and can be steered.[150] If such a satellite was hacked, its

143. U.S. Dep't of Just., *supra* note 142.

144. *Id.*

145. *Satellite Navigation – GPS- How It Works*, FED. AVIATION ADMI., https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/gps/howitworks (last updated Jun. 24, 2024).

146. John Shin, *Why Space is the Next Frontier for Cybersecurity,* FORBES (Aug. 20, 2021, 7:45 AM), https://www.forbes.com/sites/forbestechcouncil/2021/08/20/why-space-is-the-next-frontier-for-cybersecurity/?sh=c4e54fc41b15.

147. David Livingstone and Patricia Lewis, *Space, the Final Fronter for Cybersecurity?,* THE ROYAL INSTITUTE OF INT'L AFFAIRS INT'L SECURITY DEP'T (Sept. 2016), https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

148. *What are satellites used for? (and why they matter)*, RISKWARE, https://www.riskaware.co.uk/insight/what-are-satellites-used-for-why-satellites-matter/ (last visited Aug. 31, 2024).

149. Danny Palmer, *Cybersecurity in space: The out of-this-world challenges ahead,* ZDNET (Dec. 7, 2022, 4:59 AM), https://www.zdnet.com/article/cyberspace-in-space-the-out-of-this-world-challenges-ahead/.

150. Emily Conover, *Steering Small-Sale Satellites,* AMERICAN PHYSICAL SOC'Y Vol. 24, No. 11 (Dec. 2015), https://www.aps.org/publications/apsnews/201512/satellites.cfm#:~:text=Small%20satellites%20called%20CubeSats%20can,tiny%20ion%20and%20plasma%20thrusters.

orbit, speed, and direction could all be altered.[151] Hackers could knock satellites out of their orbit, crash into other satellites, or even the International Space Station.[152]

Another challenge making cyberattacks on satellites more alarming is the rapidly growing commercial space industry.[153] NASA is no longer the only player in space. Companies like SpaceX and Blue Origin added thousands of satellites to the Earth's low orbit.[154] For example, SpaceX plans to send over 40,000 Starlink satellites into space to provide low-cost Internet to remote areas worldwide.[155] With more plans to launch satellites from SpaceX and other companies, comes more demand for building satellites cheaper and faster.[156] The rapid building of satellites is of increasing interest[157] due to the possibility of companies cutting corners to decrease costs and speed up production.[158] The commercial space industry boom has opened the door for more cyberattacks. There are more non-government space actors than ever, and the highly technical aspect of building satellites allows multiple manufacturers to be involved in a single satellite.[159] These new realities create new targets along an extensive supply chain that companies and governments are not currently equipped to handle.

151. William Akoto and The Conversation US, *Hackers Could Shut Down Satellites – Or Turn Them Into* Weapons, SCIENTIFIC AM. (Feb. 22, 2020), https://www.scientificamerican.com/article/hackers-could-shut-down-satellites-or-turn-them-into-weapons/.

152. *Id.*

153. H. Austin Simpson, *Regulating Science Fiction: The Regulatory Deficiencies in a Rapidly Growing Commercial Space Industry*, 87 J. AIR L. & COM. 759, 760 (2022).

154. *Id.* at 761*; See also* Lisa Grossman, *Half of all active satellites are now from SpaceX. Here's why that may be a problem,* SCIENCE NEWS (Mar. 3, 2023, 9:00 AM), https://www.sciencenews.org/article/satellites-spacex-problem-space-pollution (as of February 2023, the total active number of Starlink satellites - SpaceX's internet satellites - was 3,660, about half of the 7,300 operational satellites in orbit).

155. Tereza Pultarova and Elizabeth Howell, *Starlink Satellites: Everything You Need to Know About The Controversial Internet Megaconstellation,* SPACE (last updated Aug. 29, 2024), https://www.space.com/spacex-starlink-satellites.html.

156. Akoto, *supra* note 152.

157. Gen. Jay Raymond, Speech at the Air Force Association Annual Conference (Sept. 18, 2019) ("And so as we look at this new business model that's being generated by the commercial market . . . the risk calculus changes when you're producing satellites, multiple satellites a day, rather than a satellite every five or six years.").

158. Akoto, *supra* note 152.

159. *Id.*

### i. Viasat KA-SAT Satellite Cyberattack

One example of the consequences a cyberattack may have on a satellite comes via the Viasat KA-SAT case. On February 24, 2022, the day of Russia's invasion of Ukraine, a cyberattack was launched against Viasat's KA-SAT satellite broadband service.[160] The cyberattack impacted the internet access of tens of thousands of Ukrainian and EU citizens and severed the remote monitoring access of 5,800 wind turbines of a German energy company.[161] The malware used to carry out the attacks is called "AcidRain," designed to remotely "wipe modems and routers."[162] The AcidRain malware bears coding similarities with another malware previously attributed to Russia's Sandworm group.[163] This piece of evidence, along with the suspicious timing of the cyberattack, leads many to conclude Russia sponsored the cyberattack.[164] The U.S. formally attributed the satellite cyberattack to Russia in a press statement by the Secretary of State.[165] While the U.S., E.U., and other countries condemned the cyberattacks, there was no discussion of its applicability to Articles 2(4) and 51, nor NATO Article 5 repercussions.[166] Such inaction to punish Russia continues to set a dangerous precedent of allowing state-sponsored malicious cyberattacks.

---

160. *See KA-SAT Network Cyber Attack Overview*, VIASAT (Mar. 30, 2022, 4:55 AM), https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

161. *See* CyberPeace Institute, *Case Study: Viasat*, CYBER CONFLICTS (June 2022), https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

162. Juan Andres Guerrero-Saade, *AcidRain | A Modem Wiper Rains Down on Europe*, SENTINEL LABS (Mar. 31, 2022), https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

163. *Id.*

164. Ravie Lakshmanan, *E.U. Blames Russia for Cyberattack on KA-SAT Satellite Network Operated by Viasat*, THE HACKER NEWS (May 11, 2022), https://thehackernews.com/2022/05/eu-blames-russia-for-cyberattack-on-ka.html.

165. *See* Press Statement, Antony J. Blinken, Sec. of State, Attribution of Russia's Malicious Cyber Activity Against Ukraine (May 10, 2022), https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/, ("the United States is sharing publicly its assessment that Russia launched cyber attacks in late February against commercial satellite communications networks to disrupt Ukrainian command and control during the invasion.").

166. *Id.; see also* Press Release, Council of the EU, Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union (May 10, 2022), https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/ ("The European Union . . . strongly condemn[s] the malicious cyber activity conducted by the Russian Federation against Ukraine, which targeted the satellite KA-SAT network, owned by Viasat.").

### *2. W32.Gammima.AG Virus on the International Space Station*

In 2008, Windows XP laptops on the International Space Station (ISS) were infected with a virus called W32.Gammima.AG.[167] The virus was linked to Russian astronauts who carried infected USB devices on the ISS and spread the computer virus to infected computers.[168] Although the virus is considered a low-level threat, the ability of a computer to become affected in the ISS exposed the flaws of the computers at the stations and their vulnerabilities to attacks.[169] Following the vulnerability, the United Space Allowance changed the computer systems on the ISS from Windows XP to Linux for more security.[170]

## B. Differences Between the Landscape of Space Law and Cyber Law

One lesson cyberspace can learn from space comes from the 1967 Outer Space Treaty.[171] This treaty, negotiated at the height of the Cold War, codified important space principles still used today. The Outer Space Treaty declares that the exploration and use of outer space "shall be carried out for the benefit and in the interests of all countries"[172] and that outer space is free for exploration by all states.[173] However, it also limits some state activity, such as claims over outer space and celestial bodies,[174] and expressly prohibits the placement of weapons of mass destruction in outer space.[175] While the Outer Space Treaty has not escaped

167. Samuel Gibbs, *International Space Station attacked by virus epidemics,* THE GUARDIAN (Nov. 12, 2013), https://www.theguardian.com/technology/2013/nov/12/international-space-station-virus-epidemics-malware.

168. *Id.*

169. Ian O'Neill, *Computer Worm Infects International Space Station,* ASTROENGINE (Aug. 27, 2008), https://astroengine.com/2008/08/27/computer-worm-infects-international-space-station/.

170. Gibbs, *supra* note 168.

171. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter *Outer Space Treaty*].

172. *Id.* at art. I, para. 1.

173. *Id.* at art. I, para. 2.

174. *Id.* at art. II.

175. *Id.* at art IV.

criticism over the years,[176] it has significantly impacted the space field and is regarded as "the backbone for space law."[177] The Outer Space Treaty was drafted and passed when the main players, the U.S. and U.S.S.R., disagreed on space matters.[178] Yet, after recognizing the significance of outer space matters, the two countries (technically still at war) agreed on most of the treaty's provisions.[179] Putting aside state interests for the greater good is a lesson from history that should be applied in today's cyber world. An International Cyber Treaty needs to be negotiated by the key players to codify cyber rules that benefit all, much like was done in 1967 with the Outer Space Treaty.

## *V. INTERNATIONAL CYBER TREATY*

Though it may be difficult to envision a Cyber Treaty that addresses the issues outlined in this Comment, European countries agreed to a comprehensive international *cybercrime* treaty in 2001.[180] The Council of Europe Convention on Cybercrime ("Budapest Convention"), among many other things, defines criminal offenses for cybercrime and establishes domestic procedures for prosecuting computer crimes.[181] Moreover, the UN is working on another major Cybercrime Convention to deal with topics like international cooperation on cybercrime, law

176. Declan Tevyaw, *Failures and Successes of the Outer Space Treaty*, THE ALLIANCE FOR CITIZEN ENGAGEMENT (Oct. 31, 2023, 12:37 PM), https://ace-usa.org/blog/foreign-policy-region/space-oceans-and-polar-regions/failures-and-successes-of-the-outer-space-treaty/ ; *see also* Christopher D. Johnson, *Deficiencies And Pressing Issues In The Existing Legal Regime Of Outer Space: The Incompleteness Of The Legal Order For Space,* UN/Turkey/APSCO Conference on Space Law and Policy (Sept. 24, 2019) ("It is increasingly clear that the body of international space law, drafted in the 1960s and 70s . . . has a number of deficiencies in relation to existing, emerging, and proposed space activities.").

177. Loren Grush, *How An International Treaty Signed 50 Years Ago Became The Backbone For Space Law,* THE VERGE (Jan. 27, 2017, 11:14 AM), https://www.theverge.com/2017/1/27/14398492/outer-space-treaty-50-anniversary-exploration-guidelines.

178. Bureau of Arms Control Verification, and Compliance, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, U.S. DEPARTMENT OF STATE, https://2009-2017.state.gov/t/isn/5181.htm (last visited Apr. 25, 2023) ("The Western powers declined to accept the Soviet approach; the linkage, they held, would upset the military balance and weaken the security of the West.").

179. *Id.* ("After the signing of the Limited Test Ban Treaty, the Soviet Union's position changed.").

180. Council of Europe Convention on Cybercrime, Nov. 23, 2001, T.I.A.S No. 13174

181. Cong. Rsch. Serv., *Cybercrime: The Council of Europe Convention*, Doc. No. RS21208 (2006), https://www.everycrsreport.com/files/20060928_RS21208_9b5fe0ffca9f75f8fe97878249bc9df6e532364f.pdf.

enforcement's access to digital evidence, and strengthening procedural safeguards and human rights provisions.[182] There has been an international treaty on cybercrime for over twenty years, and another one is forthcoming. Why is there no international treaty on cross-border cyberattacks sponsored by state actors? The answer is embedded in politics and conflicting state interests.

### A. Defining Cyberattack

The first step to drafting a successful International Cyber Treaty will be defining a cyberattack. Without a cohesive, agreed-upon definition of cyberattack, it is challenging to differentiate cyberattacks from cybercrime and cyberespionage.[183] The definition of cyberattack should be specific and concise, leaving no room for interpretation. Making the definition of a cyberattack too broad may open the door for differing interpretations and further disagreements.[184]

While the Tallinn Manual's definition of a cyberattack is a good starting point, its effect-based approach is problematic for several reasons.[185] First, the definition focuses on the cyberattack causing injury, death, or destruction to objects. Most cyberattacks do not cause such effects but rather result in, among other things, data loss and server disruption.[186] For example, the cyberattacks against Estonia in 2007 caused financial losses and general inconvenience to the public, but there was no injury, death, or destruction to objects.[187] Another issue with the Tallinn Manual's definition of cyberattack is that it does not address the intent to cause injury, death, or destruction to objects. For instance, consider a Russian-sponsored cyberattack against Ukraine's power grid, hoping to destroy it. If, for some reason, the cyberattack is not accomplished, it would not be deemed a "cyberattack" under the Tallinn Manual. A state actor should be held accountable for failed or uncompleted cyberattacks because the state intended to cause

182. *United Nations Cybercrime Treaty,* ELEC. FRONTIER FOUND., https://www.eff.org/issues/un-cybercrime-treaty

183. Moore, *supra* note 21, at 241-42.

184. *Id.* at 242.

185. TALLINN MANUAL, *supra* note 12, at 415 ("a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.").

186. *See* Simmons, *supra* note 13, at 80; *see also* discussion *supra* Section III.A.

187. Pamment, *supra* note 75, at 11.

damage. The definition of cyberattack should include an intent element to deal with these situations. More importantly, the definition of cyberattack should be broad enough to capture the different ways a cyberattack can be carried out but also specific enough not to leave room for differing interpretations.

### B. Clear Attribution and Defense Guidelines

Attribution is deemed to be the most challenging aspect of cyberattacks.[188] The Cyber Treaty must establish elements needed to attribute a cyberattack to the wrongdoing state. Along with the elements of attribution, the Cyber Treaty should outline the evidence a state must present to prove attribution. Evidence may include IP addresses, information from political sources, similarities to malware with known actors, the temporal proximity of similar cyberattacks, and using a "honeypot" to identify actors.[189] With these guidelines in place, states should no longer be able to shift responsibility to groups or individuals hired to carry out cyberattacks.[190]

Moreover, attribution is crucial for a state's legitimate claim of self-defense.[191] Accordingly, the Cyber Treaty should outline how a state may defend itself in a cyberattack. It is important to clarify what kind of attack a state may retaliate with, whether purely cyber or a mixed attack. These guidelines should still be in accordance with the international principles of necessity and proportionality discussed previously.

### C. Inclusion of Non-State Actors

Along the same lines of attribution, the Cyber Treaty should encompass the actions of non-state actors as cyberattacks. The laws of war do not apply to non-state actors, which is problematic when states employ groups or individuals to carry out cyberattacks.[192] It is hypothesized that non-state actors could violate the laws of war if a "clear relationship" exists with a state.

---

188. *See* Simmons, *supra* note 13, at 100.
189. *See* Nguyen, *supra* note 93, at 1105.
190. *See* discussion *supra* Section III.A.
191. *See* Moore, *supra* note 21, at 242.
192. *See* discussion *supra* Section II.B.3.

[193] However, it is unclear what constitutes a clear relationship. Using the 2007 Estonia DDoS cyberattacks as an example, there is definitive proof of Russian government involvement, but is this enough to form a "clear relationship"? The Russian government certainly does not think so,[194] which is why this framework is not very useful.

Instead, the Cyber Treaty should focus on state responsibility for the actions of non-state actors. First and foremost, a cyberattack must be considered state conduct if a state sponsors a cyberattack. More importantly, states should be held responsible for the acts of non-actors, especially when states knowingly allow "its territory to be used for acts contrary to the rights of other states."[195] Such a rule would hold states like Russia responsible for the acts of Russian hackers that carry out thousands of cyberattacks.[196] This framework would also remove the ability of states to claim plausible deniability for the actions of others because any cyberattack carried out within a state's territory would be the state's responsibility. Going further, even if there is no state involvement, the state should still be held responsible for not taking the appropriate measures to stop the attacks.

### D. Possibility of an International Cyber Treaty

While the idea of a Cyber Treaty is conceptually solid, many forces make its adoption uncertain in the real world. International politics and conflicting state interests play a vital role in the making and passing of international law.[197] A viable Cyber Treaty will require states with different views on cyberattacks to come together and agree on its terms.[198] Although not all UN member

193. *See* Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 151, 157 (2010).

194. Pamment, *supra* note 75, at 8.

195. Corfu Channel (United Kingdom v. Albania), Merits, 1949 I.C.J. Rep 4, 22 (April 9, 1949); *see also* TALLINN MANUAL 2.0, *supra* note 12, at 558 ("A neutral state may not knowingly allow the exercise of belligerent rights by the parties to the conflict from the cyber infrastructure located in its territory or under its exclusive control.").

196. *See The Top 5 Russian Cyber Threat Actors to Watch,* RAPID 7 (Mar. 3, 2022), https://www.rapid7.com/blog/post/2022/03/03/the-top-5-russian-cyber-threat-actors-to-watch/.

197. Ronald J. Yalem, *Law, Organization, and Politics in the International Community*, 1957 WASH. U. L. Q. 110, 111 (1957).

198. *See* Moore, *supra* note 21, at 254.

states need to agree, a cohesive Cyber Treaty with key players as signatories will strengthen the legitimacy of the treaty.

### *1. Conflicting State Interests*

The key players in the Cyber Treaty are Russia, China, and the U.S. Each state has different cyber goals. For example, Russia focuses on cyber policies that support state sovereignty and the ability to keep citizen loyalties in check.[199] China has similar goals as Russia and emphasizes the importance of preemptive cyberattacks.[200] Meanwhile, the U.S. is focused on cooperation between international law enforcement agencies to stop cyberattacks and apprehend cybercriminals.[201] Despite multiple efforts by the Russian government[202] to reach an agreement on cyber matters with the U.S., the U.S. remains apprehensive about Russia's intentions, and with good reason.[203] Although the U.S. and Russia have not agreed on most cyber issues, in 2015, Russia and China entered into a bilateral cyber treaty that pledges neither state will launch a cyberattack against the other.[204] While this treaty only binds Russia and China, it marks a first step toward an International Cyber Treaty. I do not believe the conflicting state interests between China, Russia, and the United States will render a Cyber Treaty impossible. States should set

199. *See* Timothy L. Thomas, *Nation-State Cyber Strategies: Examples from China and Russia*, Ch. 20 *in* CYBERPOWER AND NAT'L SEC. (Franklin D. Kramer et al. ed., 2009), https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-20.pdf?ver=2017-06-16-115054-850.

200. *Id.* ("Control is a vital aspect of China's information operations theory: whoever controls the network can take preemptive actions, either in a propaganda war or in real confrontations such as computer network attacks.").

201. *See* James Carden, *Time to Pursue an International Cyber Treaty?*, THE NATION (Apr. 30, 2019), https://www.thenation.com/article/archive/international-cyber-treaty-russia-china-dnc/.

202. *See Unpacking the Competing Russian and U.S. Cyberspace Resolutions at the United Nations,* COUNCIL ON FOREIGN RELATIONS (Oct. 29, 2018, 10:00 AM), https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations.

203. *See Joint Cybersecurity Advisor: Russian-State Sponsored and Criminal Cyber Threats to Critical Infrastructure*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a (May 9, 2022) (outlining the many Russian state-sponsored cyber operations on the US, UK, Canada, Ukraine, and many others).

204. Agreement Between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in Ensuring International Information Security, China-Russ, Apr. 30, 2015, Kremlin Supp, 5770.

aside their political differences and ideology for the common good as they have done in the past.[205]

### *2. Moving Past the Politics*

Russia and the U.S. had even more significant ideological differences during the Cold War.[206] Though cyberattacks cause catastrophic effects on the economy, infrastructure, supply chains, and more,[207] the severity of the Cold War cannot be compared. The Cold War was not just a space race but also a nuclear arms race between the U.S. and Russia.[208] These two nations were actively developing weapons of mass destruction and threatening each other with nuclear attacks.[209] However, during the height of the Cold War, important agreements were reached, like the Limited Test Ban Treaty (banned nuclear tests in the atmosphere) and the Outer Space Treaty (outlawing weapons of mass destruction in outer space).[210] If the U.S. and Russia reached agreements during such tense and terrifying times, it should be possible to do the same in today's world. An International Cyber Treaty that provides rules and guidance on cyberattacks would benefit both countries and promote stability in the "fifth battlespace."[211]

## E. UN Expert Groups

In its capacity, the U.N. has attempted to address the complex issues of cyberspace and international law. The U.N. has

---

205. *See* discussion *infra* Section V.D.2.

206. *See* Joseph. S. Nye, Jr., *Rules of the Cyber Road for America and Russia,* PROJECT SYNDICATE (Mar. 5, 2019), https://www.project-syndicate.org/commentary/cyber-rules-for-america-and-russia-by-joseph-s--nye-2019-03?barrier=accesspaylog.
("But even greater ideological differences did not prevent agreements related to prudence during the Cold War"); *See also Revelations from the Russian Archives*, LIBRARY OF CONGRESS, https://www.loc.gov/exhibits/archives/sovi.html (last visited Apr. 20, 2023) ("The distinct differences in the political systems of the two countries often prevented them from reaching a mutual understanding on key policy issues and even, as in the case of the Cuban missile crisis, brought them to the brink of war.").

207. WP Creative Grp., *Cyber Threats, Real-World Consequences,* THE WASHINGTON POST (Sept. 28, 2022), https://www.washingtonpost.com/creativegroup/ibm/cyber-threats-real-world-consequences/.

208. *U.S.-Russia Nuclear Arms Control,* COUNCIL ON FOREIGN RELATIONS, https://www.cfr.org/timeline/us-russia-nuclear-arms-control (last visited Apr. 20, 2023).

209. *See generally* William J. Medland, *The Cuban Missile Crisis: Evolving Historical Perspectives*, 1990 ST. MARY'S COLL. OF MINN. (1990).

210. *United States Relations with Russia: The Cold War,* U.S. DEP'T OF STATE, https://2001-2009.state.gov/r/pa/ho/pubs/fs/85895.htm (last visited Oct. 9, 2023).

211. *See* Rex Hughes, *A Treaty for Cyberspace,* 86(2) INT'L AFFS. 523, 540 (2010).

authorized both a group of governmental experts (G.G.E)[212] and an open-ended working group (O.E.W.G)[213] on the matters of information and communication technologies. The groups of note are the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security[214] and the "Open-ended Working Group on security of and in the use of information and communications technologies."[215] These groups were mandated by the U.N., among other things, to "further develop the rules, norms and principles of responsible behaviour of States,"[216] and promote "an open, secure, stable and accessible ICT [information and communications technologies] environment."[217]

While these groups are important in developing norms and guidelines for cyber matters, the drawback of the groups is in their non-binding nature. Though some nations, namely Russia, that are part of these groups work with other experts to develop these guidelines, it is clear the rules are not being followed by the member-states. While the reports serve as important guiding principles all states should follow, the reality is they are not being properly adhered to. This is another reason why a Cyber Treaty is needed. There is only so much that non-binding norms and U.N. resolutions will do in getting states to cooperate with proper cyber behavior.

### *1. UN G.G.E.*

The above-mentioned group of experts ("Experts") on this matter consists of twenty-five members from different U.N. member countries. Some of the countries participating in this group include the United States, Estonia, China, and notably, Russia.

---

212. *Group of Governmental Experts*, UNITED NATIONS, https://disarmament.unoda.org/group-of-governmental-experts/ (last visited Sept. 11, 2023).

213. *Open-Ended Working Group on Information and Communication Technologies,* UNITED NATIONS, https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021 (last visited Sept.11, 2023).

214. *Id.*

215. *Id.*

216. *Id.*

217. Rep. of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, Forward, U.N. Doc A/76/135 (July 14, 2021) [hereinafter Advancing Responsible State Behaviour].

In its latest July 2021 Report, the Experts built on their recommendations of the 2010, 2013, and 2015 reports which laid out eleven non-binding norms of state behavior in the context of international security.[218] Some of the norms outlined include states not knowingly allowing their territory to be used for internationally wrongful acts using ICTs, states taking appropriate measures to protect their critical infrastructure from ICT threats, and states should not knowingly support activity to harm the information systems of the authorized emergency response teams.[219] These norms are further analyzed in the expert's 2021 report on this matter, including examples of "the kinds of institutional arrangements that States can put in place at the national and regional levels to support their implementation."[220] For example, regarding the norm that states should not knowingly allow their territory to be used for wrongful acts using ICTs, the experts propose that "[a] State that is aware of but lacks the capacity to address internationally wrongful acts conducted using ICTs in its territory may consider seeking assistance from other States or the private sector in a manner consistent with international and domestic law."[221] This norm is especially important in aiding developing countries that may not have adequate capacity to deal with these complex matters.

### *2. U.N. O.E.W.G.*

Another group that is currently working on cyber and information security matters is the above-stated open-ended working group ("Group").[222] This Group convened for its fifth substantive session from July 24-28, 2023. At its eightieth session, the group will submit a final report to the General Assembly.[223]

In its first annual 2022 progress report, the Group noted that cyber cooperation and assistance between states "could be strengthened to ensure the integrity of the supply chain and

218. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015).

219. *Id.*

220. Advancing Responsible State Behaviour, *supra* note 218.

221. *Id.*

222. Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/77/275 (Aug. 8, 2022).

223. *Id.*

prevent the use of harmful hidden functions."[224] Some ways to strengthen cooperation suggested by the Group include establishing policies to promote the adoption of good practices by suppliers and vendors of ICT equipment and implanting "globally interoperable common rules and standards for supply chain security."[225] Since this Group has been active for only two years and has yet to release a Final Report, there is not much substance to its released documents. In the coming years, this Group should further develop norms and rules for existing and potential cyber threats that are persuasive enough for states to follow.

## *VI. CONCLUSION*

This Comment focused on the application of the laws of war to cyberattacks. While there is no question the laws of war codified in the UN Charter apply to cyberattacks, the laws are insufficient in practice. Issues arise due to the nature of cyberattacks and the traditional definitions of "force" and "armed attack." Moreover, there is difficulty in applying Articles 2(4) and 51 to cyberattacks due to proper state attribution and the exclusion of non-state actors. These challenges can be addressed by a Cyber Treaty negotiated by the three key players: the U.S., China, and Russia. Although the cyber interests and goals of the U.S. are different from those of Russia and China, the differences should not render a Cyber Treaty impossible. Much like during the Cold War with the passing of the Outer Space Treaty, the first step is to put politics behind and realize creating a Cyber Treaty could benefit all.

224. *Id.*
225. *Id.*