CYBERSECURITY AND THE U.N. CHARTER: A SQUARE PEG IN A ROUND HOLE

SLATE HERMAN*

Since its inception, the United Nations has struggled with balancing the interests of States acting to preserve their sovereignty. This balance was as much a problem in 1945, at the creation of the United Nations, as it is today. Now, in the age of drones, covert action, and non-state actors, the lines between the appropriate use of force and self-defense begin to blur significantly. Cyberwarfare is arriving on the scene just as the world considers ideas like digital currency, the privatization of outer space, and regulated online privacy.

For decades, the U.S. used its power to push for policies that clearly define appropriate protection of peace. The U.S. should use this power to push cyberwarfare towards the center of U.N. attention. Current standards of conflict determination within the U.N. Charter are ill-equipped to deal with the emerging challenges created by cyberwarfare. Cyber operations shake the foundation of important terms at the center of U.N. Security Council determinations, such as armed forces, use of force, and armed attack. The international community has also experienced the exploitation of non-state actors to carry out covert, state-sanctioned action.

Many of the issues pertaining to cybersecurity arise from flaws inherent to the technology itself. Solutions arising from the U.N. will not solve all cyber conflicts. Regardless, it is the job of the world's greatest forum to host the conversations surrounding these issues. Solutions to these complex problems should arise from the voices of all nations, not just those with enhanced interest in cybersecurity. Though the U.S. has significant national security interests in

*J.D. Candidate, University of Colorado Law School. This paper is dedicated to Isabelle Herman, sister, ballerina, and best friend. Though she believed my choice to go to law school made me more annoying, she supported me relentlessly into her final days. *I am who You say I am*. I am also thankful to the University of Colorado Law School and the Class of 2020 who held me up throughout my battle with leukemia, specifically: Nick Blodgett, Shelby Dolen, Morgan Hicks, Molly Jickling, Colleen McCroskey, Tyler Owen, Thomas Petrie, Andi Savage, and Bryson Seybold.

cybersecurity, U.N. resolutions addressing these issues would benefit the entire global community.

INTRODUCTION

Media often depicts hackers as hooded figures hidden in pitch black rooms.[1] Dimly illuminated by a black screen, they march their fingers across their keyboards seeking entry into restricted areas. It might shock many American citizens today to see uniformed soldiers strategizing how to take down targets halfway around the world with their hacking prowess or cyberweapons,[2] as was the case on June 20, 2019, when the Iranian Revolutionary Guard shot down a U.S. drone.[3] Less than two days later, the United States reported that it had crippled the air defenses responsible for the attack.[4] The U.S. response did not follow the

1. Selena Larson, *Why do hackers always wear hoodies? Behind the stereotype*, CNN BUS. (May 26, 2017, 10:35 AM), https://money.cnn.com/2017/05/26/technology/hacker-hoodie-stereotype-hacking/index.html [https://perma.cc/89P9-PZEZ].

2. *See* Josh Lospinoso, *Fish Out of Water: How the Military is an Impossible Place for Hackers, and What to Do About it,* WAR ON THE ROCKS (July 12, 2018), https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/ [https://perma.cc/QK5Z-UN9L].

3. Michel Moutot, *US cyber attack on Iran exploited flaw in heavily-guarded network, experts say,* TIMES OF ISR. (June 29, 2019, 6:56 AM), https://www.timesofisrael.com/us-cyber-attack-on-iran-exploited-flaw-in-heavily-guarded-network-experts-say/#gs.fzg0gg [https://perma.cc/UU7W-GRMS].

4. Zak Doffman, *U.S. Attacks Iran With Cyber Not Missiles – A Game Changer, Not a Backtrack*, FORBES (June 23, 2019, 3:33 AM), https://www.forbes.com/sites/zakdoffman/2019/06/23/u-s-attacks-iran-with-cyber-not-

typical route of a traditional weapon strike or an economic sanction. Instead, the devastating attack came in the form of malware launched from U.S. Cyber Command.[5]

The idea of U.S. military forces developing cyberweapons may sound like fanciful publicity, but the narrative takes a sinister turn when the roles reverse, and the United States becomes the target. Sony Pictures Entertainment ("Sony") suffered from a barrage of malicious cyber threats in late 2014.[6] The objective of the attack was to disrupt the release of *The Interview*, a comedy film portraying the assassination of North Korean dictator Kim Jong-un.[7] The attack began in early November 2014, with the appearance of a menacing neon skeleton representing the "Guardians of Peace" (GP), a hacking group.[8] Threats continued to mount, and in early December the GP made demands that Sony refrain from releasing *The Interview*.[9] By mid-December, Sony decided to suspend the release.[10] Though the film was eventually released, the sour taste of this attack remained in the mouth of U.S. officials who quickly rushed to pin this attack on a sovereign state.[11] Sony and the FBI sifted through mountains of code to determine a country of origin, and hopefully, an outlet for their embarrassment.[12] Though all signs pointed to North Korea, some experts were concerned about a false flag[13] attack operation attempting to frame the oft-aggressive dictator.[14] In an executive order released early January 2015, President Obama explicitly cited the Sony hack as a motive for new sanctions against North Korea.[15]

---

missiles-a-game-changer-not-a-backtrack/#7fe75fd6753f [https://perma.cc/GQG5-GPTW].

5. Moutot, *supra* note 3.

6. Stephan Haggard & Jon R. Lindsay, *North Korea and the Sony Hack: Exporting Instability Through Cyberspace*, *in* ASIAPACIFIC ISSUES, at 2 (East-West Center, Ser. No. 117, May 2015).

7. *Id.*

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.* at 2–3.

12. *Id.* at 2.

13. *See generally* Josh Fruhlinger, *What is a false flag? How state-based hackers cover their tracks*, CSO, (Jan. 9, 2020, 3:00 AM), https://www.csoonline.com/article/3512027/what-is-a-false-flag-how-state-based-hackers-cover-their-tracks.html [https://perma.cc/GGB3-NFA4] (defining a false flag cyber attack as "when a hacker or hacking group stages an attack in a way that attempts to fool their victims and the world about who's responsible or what their aims are").

14. Haggard & Lindsay, *supra* note 6, at 3.

15. *See id.*; Scott Neuman, *Obama Authorizes New Sanctions On North Korea Over Sony Hack*, NPR, (Jan. 2, 2015, 2:27 PM), https://www.npr.org/sections/thetwo-way/2015/01/02/374598365/obama-authorizes-sanctions-on-n-korea-over-sony-hack [https://perma.cc/LK2Q-H85R].

The Sony hack is representative of significant change in the U.S. attitude toward cybersecurity.[16] A country less powerful than the U.S. succeeded in threatening, and at one-point halting, free speech. North Korea was eventually named as an aggressor in the attack but hid behind a hacking group until eventually rooted out by investigators. The use of non-state actors, such as hacking groups, to carry out the bidding of nefarious governments has become increasingly common in the world of cyber operations.[17] Non-state actors often act as a smoke shield, creating significant difficulties for nations looking to resolve conflicts with seemingly oblivious states.[18]

In this note I contend that the U.N. Charter fails to adequately address non-state actors or provide effective alternatives to armed conflict. The question of how to correctly classify these actions under international law then arises. Article 51 of the U.N. Charter imbues nations with the power of self-defense against an armed attack.[19] The ancient concept of an armed attack creates significant ambiguity when applied to the revolutionary concept of cyberwarfare. The use of armed forces and other similar definitions are inadequate in their understanding of cyberoperations. The U.N. Charter also fails to prescribe appropriate responses to cyber-attacks and splits appropriate action into two categories, neither of which allow cyber operations to be classified correctly. Current international law does not adequately address the growing problem of cyberwarfare. Specifically, the blind spots created by Articles 2(4), 41, 42, and 51 of the U.N. Charter in failing to address cyber warfare, coupled with lack of responsibility for non-state actors expose the United States to significant risk.[20] The United States must be active in pushing the U.N. to consider new regulations to fix these potholes in the U.N. Charter.

Though some governmental bodies seem unwilling to join the discussion surrounding proper international cyberoperations, others leap headlong into the murky topic. The North Atlantic Treaty Organization ("NATO") has taken the largest step to adequately define cyber operations and explain how international

16. *See* Haggard & Lindsay, *supra* note 6, at 3 ("The willingness of senior US officials to confidently blame a nation state for a particular cyber attack was unprecedented.").

17. *See* Nicolò Bussolati, *The Rise of Non-State Actors in Cyberwarfare*, *in* CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 102 (Jens David Ohlin et al. eds., 2015).

18. *Id.* at 117.

19. U.N. Charter art. 51.

20. *See generally* U.N. Charter arts. 2(4), 41, 42, & 51 (addressing armed force responses to armed attacks, but never cyber attacks).

legal regimes apply to cyberweapons.[21] In 2009, the NATO Cooperative Cyber Defense Centre of Excellence embarked on a journey to produce a manual on the international law governing cyberwarfare, which became known as the *Tallinn Manual*.[22] The project collected distinguished practitioners and scholars in an attempt to project how current legal standards would govern this new form of warfare. With its primary focus on wartime action, the *Tallinn Manual* dives deeply into cyber operations involving the use of force and those that occur in the context of armed conflict.[23] In 2013, this text began serving as a resource for governments and scholars in the legal field.[24] Almost immediately after its publication, the group began work on a second edition of the *Tallinn Manual*. Released in February 2017, *Tallinn 2.0* expanded on the original version and added multiple provisions while updating the original.[25] This manual serves as a background from which I make many of my assumptions and conclusions.

The topic of cyberoperations sounds like something out of a dystopian fiction novel. This paper seeks to shine a light on these worst-case scenarios in an attempt to suggest solutions applicable to a global audience. By diving into a specific example of a cyberweapon, Stuxnet, the true capabilities and efficiency of cyberoperations are laid bare. The conversation then shifts to focus on the current issues that are caused by defects in cybersecurity. Finally, the problems and circumstances are brought up against the current solution, the U.N. Charter. At this point, the paper parses out the definitions that have kept rival nations at peace and shows how cyberwarfare may cause that structure to burst at the seams. Simply put, cyberwarfare is the use of technology to attack. Unfortunately for the U.N. and its members, solutions to this problem are anything but simple.

---

21. *See* CyberPeace Alliance, *Tallinn Manual – A Brief Review of the International Law Applicable to Cyber Operations,* MEDIUM (Dec. 6, 2019) https://medium.com/@cyberpeacealliance/tallinn-manual-a-brief-review-of-the-international-law-applicable-to-cyber-operations-5643c886d9e2 [https://perma.cc/TV9V-VMKZ]; *see generally* Stefano Mele, *Legal Considerations on Cyber-Weapons and Their Definition,* 3 J.L. & CYBER WARFARE 52, 63 (2014) (discussing the four typical elements of a cyberweapon).

22. *Id*.

23. *Id*. at 18–19.

24. *See* Michael J. Adams, *A Warning About Tallinn 2.0… Whatever It Says*, LAWFARE (Jan. 4, 2017, 8:30 AM), https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says [https://perma.cc/G7BS-L3DG] ("*The Tallinn Manual on the International Law Applicable to Cyber Warfare* is the most comprehensive and thoughtful work to date on the applicability of existing international law to cyber warfare. It is routinely referenced and relied upon by civilian and military practitioners across the globe . . .").

25. *See* CyberPeace Alliance, *supra* note 21.

I. BACKGROUND

A. Stuxnet: A New Definition of Cyberwarfare

The idea of opposing parties compromising each other's systems has been around since the dawn of the computer.[26] It only took eleven years from the introduction of the first personal computer (PC) in 1971 for the first wild[27] virus to arrive.[28] The virus, Elk Cloner, started as a prank by creator Richard Skrenta in the year 1982.[29] He altered code within games on his Apple II computer before exchanging them with his friends at the local Pittsburgh computer club.[30] Upon every fifteenth boot from an infected disk, the game would not run as intended and instead displayed a message.[31] The prank soon became tiresome, and Skrenta's friends no longer traded their disks with him.[32] Unphased, he invented a new system, one that would propagate onto computers without detection.[33] After taking two weeks to write the program, Skrenta's virus spread rampantly upon its release.[34] Unknowingly, he had just created the first computer virus. Luckily, a reboot cleaned the system, and years later, programmers reminisce upon the virus as a childish gag.[35] Though Skrenta only set out to play a prank on his friends, his actions brought core cybersecurity issues to light.

---

26. *See generally* Sean Spencer, *Timeline of Computer Viruses*, MAPCON, https://www.mapcon.com/us-en/timeline-of-computer-viruses [https://perma.cc/2Q7J-VQNT] (last visited Oct. 13, 2020) (tracing theories of self-replicating programs as far back as 1949); *see also When was the First Computer Invented?,* COMPUTER HOPE (last updated June 30, 2020), https://www.computerhope.com/issues/ch000984.htm [https://perma.cc/CMA6-3B2Q] (stating the first electric programmable computer appeared in 1943).

27. *See generally* Margaret Rouse, *In the wild*, WHATIS.COM (last updated Sept. 2005), https://searchsecurity.techtarget.com/definition/in-the-wild#:~:text=Experts%20say%20these%20wild%20viruses,even%20damaging%20a%20computer's%20BIOS [https://perma.cc/XA2Q-9DDJ]. ("[I]n order for a virus to be considered *in the wild*, 'it must be spreading as a result of normal day-to-day operations on and between the computers of unsuspecting users.'").

28. John Leyden, *The 30-year-old prank that become the first computer virus,* THE REGISTER (Dec. 14, 2012), https://www.theregister.co.uk/2012/12/14/first_virus_elk_cloner_creator_interviewed/?page=1 [https://perma.cc/J8AC-7RRS]; *see also When was the First Computer Invented?, supra* note 26; *see also* Spencer, *supra* note 26.

29. Leyden, *supra* note 28.

30. *Id.*

31. *Id.* ("Elk Cloner: The program with a personality. It will get on all your disks It will infiltrate your chips Yes it's Cloner! It will stick to you like glue It will modify ram too Send in the Cloner!").

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

Skrenta did not purchase this program online; he designed it himself.[36] This key attribute of malware creation generates issues for governments attempting to address or thwart individual threats.[37] It would be difficult or even impossible for Skrenta to build a gun or other weapon to achieve a similar destructive effect. Anyone with a computer can create malware,[38] allowing even the common user access to these powerful tools. Cyberweapons allow individual actors to have the effect of a fulltime military. These attacks raise the importance of cybersecurity from an exercise of due diligence to a major national security concern. The United States and other countries around the world struggle to use traditional avenues of peaceful resolutions to address these threats to economic stability.[39] Malware is extremely hard to track.[40] Even if the country of origin is found, hackers will often use deceptive tactics, like spoofing,[41] to make the virus look like it originated in a different location.[42] Most of these attacks come in the form of malware or phishing and caused the loss of $45 billion USD worldwide in 2018.[43] In 2010, Stuxnet changed the face of cybersecurity forever and brought to life many fears of the cyber community.

Stuxnet was a revolutionary malware that changed the concept of cyberwarfare forever.[44] The capabilities of Stuxnet transcended computer programing and set a new bar for cyber espionage and coordination.[45] It was the first instance of malware being used to

36. *Id.*

37. *See OUCH! Newsletter: Stop That Malware*, SANS (June 2018), https://www.sans.org/security-awareness-training/resources/stop-malware [https://perma.cc/A6XA-N9FZ] ("Cyber criminals are constantly developing new and more sophisticated malware that can evade detection.").

38. *Id.* ("Simply put, malware is software—a computer program—used to perform malicious actions.").

39. *See* Shannon Vavra, *U.S. Ramping Up Offensive Cyber Measure to Stop Economic Attacks,* CYBERSCOOP (June 11, 2019), https://www.cyberscoop.com/john-bolton-offensive-cybersecurity-not-limited-election-security/ [https://perma.cc/U2SA-K3F7].

40. Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011) https://www.scientificamerican.com/article/tracking-cyber-hackers/ [https://perma.cc/3LQT-GJBH].

41. *What is Spoofing?*, FORCEPOINT, https://www.forcepoint.com/cyber-edu/spoofing [https://perma.cc/357U-J95X] ("Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.").

42. *Id.*

43. *Cyber Attacks Costs $45 Billion in 2018*, SECURITY (July 10, 2019), https://www.securitymagazine.com/articles/90493-cyber-attacks-cost-45-billion-in-2018 [https://perma.cc/2AC7-GQC6].

44. Jon R. Lindsay, *Stuxnet and the Limits of Cyber Warfare*, 22 SEC. STUDIES 365, 373 (2013) ("Yet until Stuxnet there were no major cyber attacks on [industrial control systems] in real-world circumstances.").

45. *Dissecting Stuxnet*, YOUTUBE (May 8, 2012), https://www.youtube.com/watch?v=DDH4m6M-ZIU [https://perma.cc/L9RE-KJPK].

conduct physical cyberwarfare.[46] The virus gained notoriety by being the first of its kind to create physical destruction and interrupt the infrastructure of a nation.[47] Much like Skrenta's pioneer virus, Stuxnet relied upon poor security habits of its victims as well as its ability to remain undetected in order to infiltrate a system and create havoc.[48] Stuxnet was the world's first look at a complex cyberweapon.[49] Previous hacks used one of a few exploits to enter into a system and achieve the desired effect.[50] This new virus used a combination of seven different exploits to bridge the gap between its creators' fingers and the Iranian nuclear centrifuges.[51] No nation has taken official credit for the Stuxnet attack, though officials attribute the virus's formation to a cooperative effort between the United States and Israel: Operation Olympic Games.[52] To highlight the complexity of the virus, Kaspersky Lab studied Stuxnet and concluded that a team of ten people would need two or three years to complete a project of this magnitude.[53]

Underlining the difficulty of cyber defense requires a brief explanation of the virus. Stuxnet combined multiple types of malware to infiltrate a system, determine whether this system was the target, and finally to wreak havoc.[54] Essentially, the programmers instructed the virus to patrol for seven different weaknesses to ultimately reach the controller, which changed the frequency at which the centrifuges spun.[55] Scientists use these centrifuges to enrich uranium for the development of nuclear weapons and other nuclear technology.[56] This process all took place while Stuxnet disguised itself with an all-clear sign.[57] At this time,

46. Trystan Orr, *A Brief History of Cyberwarfare*, GRA QUANTUM (Nov. 1, 2018), https://graquantum.com/a-brief-history-of-cyberwarfare/ [https://perma.cc/53MK-Y2WD].

47. *Id.*

48. *Dissecting Stuxnet, supra* note 45.

49. *Id.*

50. *Id.*

51. *Id.*

52. Ellen Nakashima & Joby Warrick, *Stuxnet was Work of U.S. and Israeli Experts, Officials Say,* WASH. POST (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html [https://perma.cc/3FST-4768].

53. Josh Fruhlinger, *What is Stuxnet, Who Created it and How Does it Work?*, CSO (Aug. 22, 2017, 2:39 AM PDT), https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html [https://perma.cc/8VXC-39LC].

54. *Dissecting Stuxnet*, *supra* note 45.

55. *Id.*

56. Marshall Brain, *What's a Uranium Centrifuge?*, HOWSTUFFWORKS (last accessed on Nov. 11, 2019), https://science.howstuffworks.com/uranium-centrifuge.htm [https://perma.cc/LST5-W2A7].

57. *Dissecting Stuxnet, supra* note 45.

it is unknown exactly how the virus gained entry into the system.[58] Most likely, the chain between Stuxnet's creators and the Iranian centrifuges was completed due to the connection of a corrupted computer, controller, printer, or flash drive.[59] The virus quickly varied the speed of the centrifuges; all the while, a secondary virus presented prerecorded and inaccurate readings.[60] This rapid variation in acceleration or deceleration caused the centrifuges to burn out at a rapid pace.[61] Overall, the attack destroyed nearly 1,000 of Iran's 6,000 centrifuges.[62] As Iran begins to spin-up its nuclear program once again,[63] the Stuxnet attack will likely linger in its mind as it prepares new security protocols.

The Stuxnet virus is groundbreaking in many ways. Up until the release of Stuxnet, computer scientists had only dreamed about cyberweapons that could cause physical harm. This new technology turned theory into reality.[64] Unfortunately for the United States, Stuxnet's most groundbreaking feature exists in its reusability by both state and non-state actors.[65] With a slight adjustment, Stuxnet could be reproduced and its mayhem repeated.[66] Just a few years later, a worm nicknamed "Duqu" was discovered attempting to gather information using a Stuxnet model of penetration and verification.[67] Assuming Stuxnet can be retooled to affect U.S. systems, a malicious actor would simply need to find a vulnerability in U.S. critical infrastructure and release the virus and accompanying havoc. "All it takes is the right Google search terms to find a way into the systems of U.S. water utilities. . . ."[68] Without a complete overhaul of existing systems, Stuxnet may very well find its new home in critical U.S. infrastructure.

Due to its advanced spreading capabilities, Stuxnet could just as easily be deployed by a non-state actor and unwittingly spread

---

58. *Id.*
59. *Id.*
60. *Id.*
61. *Id.*
62. Nakashima & Warrick, *supra* note 52.
63. Patrick Wintour, *Iran Resumes Uranium Enrichment in New Step Away from Nuclear Deal,* GUARDIAN (Nov. 5, 2019), https://www.theguardian.com/world/2019/nov/05/iran-announces-injection-of-uranium-gas-into-1044-centrifuges [https://perma.cc/WYQ2-228Z].
64. Neta Alexander, *Did the Israeli-American Stuxnet Virus Launch a Cyber World War?*, HAARETZ (July 15, 2016), https://www.haaretz.com/israel-news/.premium.MAGAZINE-did-stuxnet-launch-a-cyber-world-war-1.5410099 [https://perma.cc/CSK3-BJK6].
65. David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM (Feb. 26, 2013), https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet [https://perma.cc/UXR2-AZLC].
66. *See generally* Kim Zetter, *DHS Fears a Modified Stuxnet Could Attack U.S. Infrastructure*, WIRED (July 26, 2011, 5:51 PM), https://www.wired.com/2011/07/dhs-fears-stuxnet-attacks/ [https://perma.cc/NZ4U-WASK].
67. Kushner, *supra* note 65.
68. *Id.*

by civilians. To clearly illustrate this point, Schouwenberg—one of the Kaspersky scientists who discovered Stuxnet—addressed the current debate surrounding cybersecurity.[69] "There's a lot of talk about nations trying to attack us, but we are in a situation where we are vulnerable to an army of 14-year-olds who have two weeks' training."[70] Stuxnet exposed a gaping hole in global cybersecurity, exploitable by anyone with the right toolkit.

A secondary issue arises when no sovereign nation claims responsibility for the attack.[71] Though many computer scientists and officials point to the U.S. and Israel, there is no official connection or statement from either government that directly claims ownership of this attack.[72] This attribute of cyberweapons makes it difficult to fit within current international guidelines. Cyberweapons can be deployed from anywhere while targeting any location or multiple locations simultaneously and without the constraints that many traditional weapons face.[73] Internet connectivity is an incredible asset for numerous reasons. This interconnection also eliminates many natural barriers, bringing distant quarreling nations face to face.[74]

B. The Rise of the Cyber-Headache

While cyberwarfare's emergence as a national security threat is not surprising, the rest of the U.S. economy has also felt this global shift toward cyber operations. In February 2018, the Council of Economic Advisers released a report detailing the cost of malicious cyber activity to the U.S. economy.[75] The report estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion yearly.[76]

Though this figure is substantial and should cause alarm, the economic threat is shown more effectively through trends. According to the Government Accountability Office (2017), the number of cyber incidents reported by federal agencies rose from 5,503 in FY2006 to 33,632 incidents in FY2016.[77] Thankfully, the

69. *Id.*
70. *Id.*
71. *See id.*
72. *Id.*
73. *See generally* Sue Halpern, *How Cyber Weapons are Changing the Landscape of Modern Warfare*, NEW YORKER (July 18, 2019), https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-landscape-of-modern-warfare [https://perma.cc/3AFU-2QZJ].
74. Michael Daniel, *Why is Cybersecurity So Hard?*, HARV. BUS. REV. (May 22, 2017), https://hbr.org/2017/05/why-is-cybersecurity-so-hard [https://perma.cc/9TYY-RTVS].
75. *See* COUNCIL OF ECON. ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY (Feb. 2018).
76. *Id.* at 1. *But see Cyber Attacks Costs $45 Billion in 2018*, *supra* note 43.
77. COUNCIL OF ECON. ADVISERS, *supra* note 75, at 35.

private sector's cybersecurity industry is growing as well. Morgan Stanley estimates that global IT security products and services market will grow by 18% each year between 2015 and 2020 to become a $128 billion market by 2020.[78] Cybersecurity is a rising issue for governments as well as public and private companies and individuals. Various U.S. agencies[79] are taking steps to address these issues at home, and the Department of Defense is looking to solve these problems at their source, even if that source is overseas.

The United States as well as United Nations Security Council have levied significant sanctions against North Korea as punishment for the country's continued attempts to develop a nuclear arsenal.[80] These sanctions touch all sectors of North Korea's economy and put significant strain on the country's ability to generate wealth. Unsurprisingly, nuclear weapons are expensive.[81] North Korea spent an estimated one to three billion U.S. dollars (USD) to produce the beginnings of a formidable nuclear program.[82] This spending comes within a total military budget of ten billion USD a year, equating to between a "fifth to a quarter of its gross domestic product."[83]

With sanctions coming from multiple nations and international bodies, North Korea is forced to resort to creative, and often illegal, methods of wealth-gathering. The North Korean government set its eyes on bank heists as a major target for cyber espionage.[84] In 2016, an attack on Bangladesh's central bank allowed hackers to net $81 million before bank transfers stopped.[85]

---

78. *Id.* at 34.

79. Department of Homeland Security through the Cybersecurity and Infrastructure Security Agency, the Federal Communications Commission, and the Department of Commerce through the National Telecommunication and Information Administration, and the National Institute of Standards and Technology.

80. Eleanor Albert, *What to Know About Sanctions on North Korea*, COUNCIL ON FOREIGN REL., https://www.cfr.org/backgrounder/what-know-about-sanctions-north-korea [https://perma.cc/U9TB-AAT3] (last updated July 16, 2019).

81. Stephen Schwartz, *The Cost of U.S. Nuclear Weapons*, NAT'L THREAT INITIATIVE (Oct. 1, 2008), https://www.nti.org/analysis/articles/costs-us-nuclear-weapons/ [https://perma.cc/VZ34-YGVT] ("From 1940–1996, the United States spent a minimum of $5.5 trillion on its nuclear weapons program. . . . This figure does not include $320 billion in estimated future-year costs for storing and disposing of more than five decades' worth of accumulated toxic and radioactive wastes and $20 billion for dismantling nuclear weapons systems and disposing of surplus nuclear materials. When those amounts are factored in, the total incurred costs of the U.S. nuclear weapons program exceed $5.8 trillion.").

82. *Less than one aircraft carrier? The Cost of North Korea's Nukes*, CNBC, https://www.cnbc.com/2017/07/20/less-than-one-aircraft-carrier-the-cost-of-north-koreas-nukes.html [https://perma.cc/44UM-HXPQ] (last updated July 20, 2017).

83. *Id.*

84. Evan Perez & David Shortell, *North Korean-Backed Bank Hacking on the Rise, US Officials Say*, CNN: POLITICS, https://www.cnn.com/2019/03/01/politics/north-korea-cyberattacks-cash-bank-heists/index.html [https://perma.cc/HJW5-GHTN] (last updated Mar. 1, 2019).

85. *Id.*

The attackers tricked the Federal Reserve Bank of New York to make multiple transfers from the Bangladesh bank to accounts controlled by North Korea.[86] Upon further review, forensic investigators found traces of code that was similar to code found in other North Korea malware.[87] Hackers pick targets with less advanced cyber protection in order to evade detection.

The long saga of U.S. sanctions has had a clear effect on North Korea with some unintended consequences. Instead of halting the production of a nuclear program, Kim Jong-un has resorted to cybercrime to fund his ventures.[88] Sanctions represent a peaceful alternative to military action. However, if countries like North Korea can efficiently avoid the pressures of sanctions by resorting to cybercrime, international bodies, like the U.N., will be forced to pursue other more forceful avenues of persuasion.

The U.S. military is dealing with many of the same cyber threats plaguing the U.S. economy. Development of the F-35 single-engine fighter aircraft began in 2001 and saw deliveries beginning in 2011.[89] This $400 billion program created a plane optimized to reign supreme on the modern battlefield. Within three years, China released a similar stealth fighter modeled after the F-35.[90] In 2016, U.S. officials confirmed through the testimony of a Chinese national, that malicious cyber activities compromised the blueprints for the F-35.[91] Su Bin plead guilty to stealing data, but the damage had already been done.[92] The United States spends a significant amount on its military research and development programs.[93] If these secrets are unsafe, all future investments in military technology are ripe for theft and will be available for use in building the armies of other nations.[94]

Multiple factors make cyber operations programs an efficient investment for countries looking to close a relative state power gap. Military strength acts as a marker when determining relative state power. This strength, along with various attributes such as

86. *Id.*

87. *See* Matthew Ha & David Maxwell, *Kim Jong Un's 'All-Purpose Sword'*, FOUND. FOR DEF. OF DEMOCRACIES (Oct. 3, 2018), https://www.fdd.org/analysis/2018/10/03/kim-jong-uns-all-purpose-sword/ [https://perma.cc/KN9J-WJJT] ("Subsequent investigations of the same malware samples by Kaspersky Labs, McAfee, and Recorded Future found traces of Lazarus malware tools and shared network infrastructure.").

88. Evelyn Cheng, *Five Ways North Korea Gets Money to Build Nuclear Weapons*, CNBC (Apr. 18, 2017, 10:33 AM), https://www.cnbc.com/2017/04/18/how-does-north-korea-get-money-to-build-nuclear-weapons.html [https://perma.cc/P9R3-VV3T].

89. *See* COUNCIL OF ECON. ADVISERS, *supra* note 75, at 35.

90. *Id.*

91. *Id.*

92. *Id.*

93. *See* CONG. RES. SERV., R45441, GOVERNMENT EXPENDITURES ON DEFENSE RESEARCH AND DEVELOPMENT BY THE UNITED STATES AND OTHER OECD COUNTRIES: FACT SHEET 1 (2020).

94. *See* COUNCIL OF ECON. ADVISERS, *supra* note 75, at 35.

population and gross domestic product, helps countries determine their global position relative to other nations.[95] When a country is unable to score highly in all categories, specialization can help a country create room for itself in the international conversation.[96]

Cyberspace is an area ripe for specialization. Standardization and reusability of previous malware let new countries entering cyberspace catch up quickly.[97] Standardization in the programming of malware enables programmers to navigate through code, seamlessly creating a multitude of cyberweapons.[98] Countries can then implement numerous teams to work on specific projects while skipping the early stages of development. This optimization creates a great amount of reusability in cyberweapons—one of their most efficient features. Countries can reuse their cyberweapons against similar technologies. The Stuxnet attack will likely be used again in the future to wreak havoc, but next time it may not be in the hands of the United States. As a country participates more in cyber operations, its programmers learn new techniques and become more knowledgeable in the creation of new malware.[99]

The United States is slowly beginning to move cybersecurity to the forefront of its defensive arsenal.[100] However, experts opine about weaknesses in infrastructure and the lack of current cybersecurity standards.[101] United States Cyber Command (USCYBERCOM) requested $647 million in funding for FY2018, a 16% increase in budget from 2017.[102] Congress also elevated USCYBERCOM from a sub-unified combatant command to a full unified combatant command.[103] As the United States prepares for

95. *See generally* GREGORY F. TREVERTON & SETH G. JONES, MEASURING NATIONAL POWER (2005), https://www.rand.org/content/dam/rand/pubs/conf_proceedings/2005/RAND_CF215.pdf [https://perma.cc/67S4-2KEP] (discussing the various modes of power and countries' relational strength through comparative studies of those modes).

96. ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 10 (S. M. Soares ed.) (2007) (positing the idea that specialization inherently increases the dexterity of the workman, thus allows it to be more efficient.).

97. *See* Max Smeets, *How Much Does a Cyber Weapon Cost? Nobody Knows*, COUNCIL ON FOREIGN REL. (Nov. 21, 2016), https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows [https://perma.cc/XS9M-9SRY] ("[R]eusing and building upon existing malware tools allows attackers to learn to produce cyber weapons more cost effectively.").

98. *See id.*

99. *Id.*

100. *See* Mark Pomerleau, *CYBERCOM Elevation at Heart of Budget Increase*, FIFTH DOMAIN (May 24, 2017), https://www.fifthdomain.com/home/2017/05/24/cybercom-elevation-at-heart-of-budget-increase/ [https://perma.cc/JSU2-UX3A].

101. *See generally* CYBERSPACE SOLARIUM COMMISSION, SOLARIUM COMMISSION REP. (2020), https://www.solarium.gov/report [https://perma.cc/855L-E4RP].

102. Pomerleau, *supra* note 100.

103. *Id.*; David M. Hollis, *USCYBERCOM: The Need for Combatant Command Versus a Subunified Command,* U.S. ARMY (June 29, 2010),

an all-out cyber defense strategy, it is important to review the available mechanisms for the international pursuit of peace. Unfortunately, the U.N. Charter finds itself in a similar position: woefully behind and ill-equipped.

II. PROBLEM

A. The Charter of the United Nations and the Holes Within

On October 24, 1945, the United Nations (U.N.) came into existence with the purpose of "maintaining international peace and security . . . ."[104] Its controlling document, the Charter of the United Nations ("Charter"), seeks to define the international rights of its member states and encourages nations to take diplomatic approaches whenever possible.[105] The Charter explores types of conflict, and appropriate responses should an issue arise.[106] The U.N. Security Council, established in Chapter V of the Charter, determines what measures are necessary to establish peace in conflict.[107] The Charter also strictly states in Article 51 that, "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense . . . ."[108] This charge, given to all member states of the U.N., speaks broadly to the majority of physical invasions that could arise. Unfortunately, as time marched onward, so did weapons development. Several issues are born from the terms use of force and armed force. Attempting to fit cyberwarfare into this framework will create undue tension in the new area. It is important to first define these terms before cracks appear when applied in whole to cyber operations.

1. Article 41 v. Article 42 – The Use of Armed Force

Article 39 empowers the Security Council to "determine the existence of any threat to the peace . . . and shall make recommendations . . . in accordance with Article 41 and Article 42, to maintain or restore international peace and security."[109] The

https://www.army.mil/article/41585/uscybercom_the_need_for_a_combatant_command_versus_a_subunified_command [https://perma.cc/C5VM-7GFS] (detailing the importance of USCYBERCOM's elevation to a full combatant command).

104. Karen Mingst, Cecelia M. Lynch & Jacques Fomerand, *United Nations*, https://www.britannica.com/topic/United-Nations [https://perma.cc/P63P-XJBB] (last updated Jan. 21, 2020).

105. U.N. Charter art. 1, ¶ 1.

106. *See* U.N. Charter art. 2, ¶ 4; *see also* art. 51, *supra* note 19.

107. U.N. Charter art. 23, ¶ 1; U.N. Charter art. 39.

108. Art. 51, *supra* note 19.

109. U.N. Charter art. 39.

difference between Article 41[110] and Article 42[111] turns on the use of armed force.[112] Article 41 allows the Security Council to consider measures without the use of armed force in order to pursue peaceful resolution without physical offensive action.[113] The Security Council often creates sanctions or arms embargos under Article 41 to force the peaceful resolution of conflicts.[114]

Moving from Article 41 to Article 42 shows a clear turning point in the actions approved by the Security Council. Resolutions from the council fall either under Article 41—"measure not involving the use of armed force"[115]—or Article 42—the Security Council may decide that Article 41 is inadequate and "may take such action . . . as may be necessary to maintain or restore international peace and security."[116] Article 42 operates as a "keys to the castle" approach to solving international peace issues. This approach is often used in complex hands-on operations, such as to separate warring forces;[117] to monitor and organize the electoral process;[118] and to verify the agreements between different sides of

110. U.N. Charter art. 41 "("The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.") [hereinafter Art. 41].

111. U.N. Charter 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. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations.") [hereinafter Art. 42].

112. *See* Mónica Lourdes de la Serna Galván, *Interpretation of Article 39 of the UN Charter by the Security Council. Is the Security Council a Legislator for the Entire International Community*, 11 ANUARIO MEXICANO DE DERECHO INT'L 147, 152–53 (2011) (discussing the juxtaposition between Art. 41 and Art. 42).

113. Art. 41, *supra* note 110**Error! Bookmark not defined.**.

114. *Sanctions and Other Committees*, U.N. SECURITY COUNCIL, https://www.un.org/securitycouncil/content/repertoire/sanctions-and-other-committees [https://perma.cc/3KXN-VMFN] (last visited Oct. 13, 2020) (discussing specific times the Security Council placed sections on various countries. For example, the Security Council placed sanctions places on Angolan petroleum in 1993; on the Taliban in Afghanistan in 2011; and on the Democratic People's Republic of Korea for its nuclear activity in 2006).

115. Art. 41, *supra* note 110.

116. Art. 42, *supra* note 111.

117. *Middle East-UNEF II,* UNITED NATIONS, https://peacekeeping.un.org/sites/default/files/past/unef2mandate.html [https://perma.cc/7E4L-67L4] (last visited Oct. 13, 2020) (The United Nations Emergency Force (UNEF) II was established in October 1973 to help restore pre-conflict positions after a military conflict occurred between Egyptian and Israeli forces).

118. *El Salvador-ONUSAL*, UNITED NATIONS, https://peacekeeping.un.org/sites/default/files/past/onusalmandate.html [https://perma.cc/C36D-GFAB] (last visited Oct. 13, 2020) (The United Nations Observer Mission in El Salvador (ONUSAL) was established in 1991 to enforce a cease fire agreement between the Government of El Salvador and the Frente Farabundo Martí

a civil war.[119] The available actions in Article 42 are clearly different from those in Article 41. The introduction of cyber operations into this dichotomy blurs the line between the two articles and allows for more substantial actions with less permission from the Security Council.

Cyberwarfare, in a traditional sense, would fit cleanly into Article 41 in the pursuit of peaceful goals. For example, embargos or trade sanctions could be enforced using distributed denial of service (DDOS) attacks, botnets, and ransomware to shut down the internet or shut down import and export functions in the sanctioned nation.[120] These types of actions would not be considered as involving the use of armed forces typically characterized "by [the use of] air, sea, or land forces . . . ."[121] Scientists and lawmakers have signaled that cyberwarfare attacks could rival the destructive capabilities of traditional weapons.[122] Stuxnet brought those theories to life.[123] The destroyed Iranian centrifuges clearly represent an Article 42 action. This tipping point splits cyberwarfare in half. Unfortunately, as with many systems, there is no true way to correctly and appropriately address cyberwarfare evenly or cleanly.

A counterargument to this apparent grey area is the physical implications of the Article 41 and Article 42 split. It would seem apparent that any invasion into a physical space would constitute an Article 42 action and anything that stays within cyberspace would be labeled Article 41 action. This distinction allows too much leverage to cyber operation in Article 41. The United States' response to the North Korean aggression against Sony, discussed in the introduction, highlights an issue with this argument.[124] Though not technically a sanctioned action by the U.N., the U.S.

---

para Liberación Nacional. In December 1992, ONUSAL oversaw elections in El Salvador).

119. *Guatemala-MINUGUA*, UNITED NATIONS, https://peacekeeping.un.org/sites/default/files/past/minuguamandate.html [https://perma.cc/GD2J-CNXT] (last visited Oct. 13, 2020) (The United Nations Verification Mission in Guatemala (MINUGUA) was established in 1993 to verify the implementation of an agreement between the Government of Guatemala and the Unidad Revolucionaría Nacional Guatemalteca).

120. *See, e.g.*, Nicole Perlroth & David E. Sanger, *North Korea Loses Its Link to the Internet*, N.Y. TIMES (Dec. 22, 2014), https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html [https://perma.cc/EN83-YMDN]; Mohan B Gazula, *Cyber Warfare Conflict Analysis and Case Studies*, 88–89 (MIT Management Sloan School: $(IC)^3$, Working Paper CISL# 2017-10, May 2017).

121. Art. 42, *supra* note 111.

122. *See* Todd South, *New Cyber Weapons are Here and No One is Prepared, Experts Say*, ARMYTIMES (Apr. 9, 2018), https://www.armytimes.com/news/your-army/2018/04/09/new-cyber-weapons-are-here-and-no-one-is-prepared-experts-say/ [https://perma.cc/6FWM-EY9B].

123. *See supra* I.A.

124. *See supra* Introduction.

unofficial response to North Korea's hack on Sony was to DDOS the entire country, completely blocking internet access.[125] Without deploying troops by air, land, or sea, part of an entire country's communication system was shut down.[126] Similar action, taken in pursuit of a weapons embargo, could fall under Article 41.

Without change, the current definition of armed force allows for far too much creative latitude within cyberspace. If a Stuxnet-style physical intrusion is the bare minimum for Article 42 action, the line between economic interruption and the use of armed forces begins to blur. The distinction between Article 41 and Article 42 is important when a country is looking to respond to an action or situation. However, not all cyber attacks are made in defense.

2. Article 2(4) v. Article 51 – The Force Gap

Article 2(4) of the Charter requires all members to "refrain in their international relations from the threat or use of force . . . ."[127] The exception to this rule lies in Article 51, granting member states an inherent right to self-defense if an armed attack occurs.[128] This right remains active until the Security Council can make a deliberation on whether the conflict merits an Article 41 or Article 42 response.[129]

The inquiry into the definitions of use of force in Article 2(4) and armed attack in Article 51 are relevant to the cyberwarfare debate. Commentators consider the use of force in Article 2(4) synonymous with armed or military force[130], but this is not limiting. The International Court of Justice ("ICJ") applies the prohibition in Article 2(4) "to any use of force, regardless of weapon employed."[131] This language creates a broad prohibition of force under which attacks like Stuxnet would clearly be considered a use of force. A result of this reading is that members of the U.N. would face legal action if caught using malware to cause physical harm in another sovereign nation. This begs the question, how far should this prohibition of cyberoperations extend? It is unclear if Russian meddling in the 2016 U.S. election or China's continued attack on U.S. copyright law would constitute a use of force under that standard. Article 51 rests its scale upon the infringement of

125. Perlroth & Sanger, *supra* note 120.
126. *Id.*
127. Art. 2, *supra* note 106, at ¶ 4.
128. Art. 51, *supra* note 19.
129. *Id.*
130. Nils Melzer, *Cyberwarfare and International Law*, U.N. INST. FOR DISARMAMENT RES. 1, 7 (2011), https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf [https://perma.cc/E97J-P8B5].
131. *Id.* at 7–8, 13.

sovereignty by an armed attack.[132] As discussed previously in the distinction between armed attack in Article 41 and Article 42, this higher standard of an armed attack creates an interesting split. While the use of force under Article 2(4) is broad, the definition of armed attack in Article 51 is strictly construed. This space creates a force gap, referring to the intentional space between the prohibition of Article 2(4) and the triggering of Article 51.

The force gap creates an interesting space between its prohibition on state action and the type of actions that warrant an Article 51 self-defense. The attempted hacking of the U.S. 2020 election by Iran exemplifies this gap. On Oct. 4, 2019, Iranian hackers with government backing attempted to gain access to the email accounts of various officials in the Trump campaign.[133] This action clearly satisfies Article 2(4) use of force as it threatens the "political independence" of a state.[134] However, the U.S. would be unable to act in self-defense under Article 51 as this intervention by Iran would fall short of that bar. No armed attack existed under the purview of Article 51 and thus did not necessitate a response of self-defense. This gap is important as it holds countries from intentionally escalating conflicts with a broad definition of self-defense.[135] Cybersecurity represents a threat to the force gap and will lead to an ever-dwindling space between the two articles.

As the extent of operations covered by both Article 2(4) and Article 51 expands, the gap between them begins to disappear. The variety of cyber operations pushes Article 2(4) to cover everything from unintentional expansion of targeted malware to the threat of stolen military intellectual property. The application of this article to such a wide range of conduct lessens the strength of its prohibitions. As additional countries engage in these Article 2(4) breaches, members of the United Nations will feel frustrated by the Security Council's inability to address all claims.

At the same time, cyber operations like Stuxnet have added to the numerous types of armed attacks dignifying a self-defense response. Stuxnet does not create a standard that applies to all cyberweapons. The physical destruction created by Stuxnet shows

---

132. *See supra* II.A.1 (armed attack is not directly defined by the U.N. Charter, but relies on the physical characteristics discussed under Art. 42).

133. Nicole Perlroth & David E. Sanger, *Iranian Hackers Target Trump Campaign as Threats to 2020 Mount*, N.Y. TIMES (Oct. 4, 2019), https://www.nytimes.com/2019/10/04/technology/iranian-campaign-hackers-microsoft.html [https://perma.cc/2P27-K2KV] (last updated Sept. 18, 2020) [hereinafter *Iranian*].

134. Art. 2, *supra* note 106, at ¶ 4.

135. Claus Kress, *On the Principle of Non-Use of Force in Current International Law*, JUST SECURITY (Sept. 30, 2019), https://www.justsecurity.org/66372/on-the-principle-of-non-use-of-force-in-current-international-law/ [https://perma.cc/6FKA-XHYG] ("An armed attack was, it was said verbatim, the most grave form of the use of force. This sounded as if only massive military operations may be defended against by using force.").

a clear connection between an armed attack and a cyberweapon. Does this mean that any physical destruction creates the ability to respond in self-defense?[136] If so, the flickering of the North Korean internet may have triggered an Article 51 response. If the attempted hacking of the 2020 election by Iran had caused a phone to overheat and burst into flames, would this allow the U.S. to respond in kind? This expansion of both Article 2(4) and Article 51 is not sustainable.[137] Soon, the ever-expanding and ill-defined menace that is cyberwarfare will erode the deescalating properties of the force gap.

As the lines between Article 41 and Article 42, or Article 2(4) and Article 51, begin to blur, countries looking for an opportunity to make war will seize this confusion by relying on an unjustifiably broad interpretation of these provisions. Unfortunately, other articles within the U.N. Charter create compounding complications in this area. The culmination of the cyber-headache has put a spotlight on an age-old problem: the non-state actor.

3. Non-State Actors: Cyber Guerilla Warfare

Non-State actors represent a confusing legal question even without the added ambiguity of cyber operations. In a report released in 2007, the National Intelligence Council (NIC) defines non-state actors as "non-sovereign entities that exercise significant economic, political, or social power and influence at a national, and in some cases international, level."[138] The report highlights that this definition covers a variety of groups: terrorists, international criminal organizations, multinational corporations, NGOs (non-governmental organizations), and philanthropic super-empowered individuals.[139] This group of eclectic entities cannot be managed under one banner but must be held accountable in some uniform way.

The U.S.'s interest in determining how the U.N. governs these actors is extremely varied. Growing non-state actor influence threatens the ability for Western powers to govern potentially volatile situations. Specifically identified in the NIC report are non-

136. *Id.* ("The recent discussion about whether harmful cyber operations may violate the prohibition of the use of force has largely come to the conclusion that a use of force under international law does not depend on conventional weapons being used.").

137. *Id.* ("On the horizon of the current discussion, the question has therefore arisen as to whether new vulnerabilities, especially in cyberspace, may lead to change in this long-known basic political pattern in the discussion about the prohibition of the use of force.").

138. *Nonstate Actors: Impact on International Relations and Implications for the United States*, NAT'L INTELLIGENCE COUNCIL 1, 2 (2007), https://www.dni.gov/files/documents/nonstate_actors_2007.pdf [https://perma.cc/3VFW-5JY3].

139. *Id.*

state actors that provide alternative investment opportunities, thus weakening any economic actions taken by the U.N. under Article 41.[140] As a result, this paper focuses on how this lack of regulation will affect the way non-state actors function within cyberspace.

The *Tallin Manual 2.0* highlights this problem eloquently: "whether non-[s]tate actors may initiate an armed attack as a matter of law is the subject of some controversy."[141] The term armed attack creates an important balancing test. NATO's experts in cyberlaw question whether it is legally possible for a sovereign nation to trigger Article 51 self-defense if attacked by a non-state actor.[142] This obscurity represents a significant void in existing standards and policymakers must address this gap to lift this veil. Attacks on the World Trade Center on Sept. 11, 2001, represent a large leap in the right of self-defense as applied to an attack from non-state actors. Soon after the 9/11 attacks, the Security Council adopted resolutions recognizing the U.S.'s right to self-defense against a non-state actor.[143] However, applying this decision directly to cyberwarfare remains difficult. The expert panel of the *Tallin Manual 2.0* note their split:

> [T]hese Experts would consider a devastating cyber operation undertaken by a group of terrorists from within one State against critical infrastructure located in another as an armed attack by those cyber terrorists against the latter State. A minority of the Experts did not accept this premise, suggesting that the traditional approach by which only States, or non-State actors conducting operations on behalf of States, can mount an armed attack as a matter of law.[144]

The experts suggest two possibilities: (1) right of self-defense against non-state actors exists, or (2) right of self-defense against non-state actors exists only if tied to a sovereign state.[145] Each creates substantial problems within the current regime. If rights exist against all non-state actors, many potentially innocent states will become subject to armed force. Countries without formidable cybersecurity practices will be unable to stop these actors from creating havoc originating within their borders. These attacks would subject host countries to formidable self-defense counter-measures, regardless of any attempts that nation may have taken

140. *Id.* at 4.

141. NATO COOPERATIVE CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 340 (Michael N. Schmitt ed., 2013) [hereinafter Schmitt].

142. *Id.* at 339–40.

143. S.C. Res. 1368, ¶ 3 (Sept. 12, 2001); S.C. Res. 1373, ¶ 4 (Sept. 28, 2001).

144. Schmitt, *supra* note 141, at 345.

145. *See id.* at 339–45.

to stop the attacks. Whether cyberweapon or traditional weapon, any response would damage the infrastructure and governance capabilities of the unwilling host nation.

Under the second regime, countries that suffered an attack from a cyberweapon would rush to pin the attack on a nation. Not only is this difficult due to international investigation restraints, it is nearly impossible within the structure of the internet. Following the digital trail of these attackers is nearly impossible and can take days or weeks to root out. This is an issue in both regimes, but specifically in the second, as a State looking to act would rush to a conclusion in order to appease the outrage of its people. Both regimes are unsustainable as the tide of these cyber attacks continues to mount.

This confusion within the law has created perverse incentives, as shown by Russia's new Sovereign Internet bill.[146] The new regulation would create a "Chinese-style standalone internet infrastructure" which would allow Russian authorities to more closely monitor the internet traffic traveling in and out through its country's Internet Service Providers (ISPs).[147] Now, Russia will have an increased ability to detect non-state actors attacking its network but will still likely ignore the threats to foreign entities existing within its network.[148] The incentives created by the current legal regime are as follows: intensely protect the network of your state, even if doing so fragments the global internet, and avoid investigations into non-state actors within your network for fear of potential responsibility for their actions.

While some countries shy away from pursuing the non-state actors within their networks, others pursue non-state actors as a vehicle for unsanctioned state action. In December 2018, the United States and United Kingdom (U.K.) released a joint indictment of two Chinese nationals, each part of the Advanced Persistent Threat 10 hacking group.[149] They alleged that these non-state employees were operating under the "direction and protection" of China's Ministry of State Security.[150] The target of these intrusions was the

146. Dev Kundaliya, *Russia's New Cyber Laws Will Fuel Online Crime, Claims Report,* COMPUTING (Aug. 9, 2019), https://www.computing.co.uk/ctg/news/3080270/russia-cyber-crime [https://perma.cc/9VSL-SYJG].

147. *Id.*

148. *See generally* John Lough, Orysia Lutsevych, Peter Pomerantsev, Stanislav Secrieru & Anton Shekhovtsov, *Russian Influence Abroad: Non-state Actors and Propaganda*, CHATHAM HOUSE (Oct. 24, 2014), https://www.chathamhouse.org/sites/default/files/field/field_document/20141024RussianInfluenceAbroad.pdf [https://perma.cc/4SMG-V7CB].

149. Patrick Wintour, *US and UK Accuse China of Sustained Hacking Campaign*, THE GUARDIAN (Dec. 2018), https://www.theguardian.com/world/2018/dec/20/us-and-uk-accuse-china-of-sustained-hacking-campaign [https://perma.cc/2HGM-Y5XY].

150. *Id.*

large-scale theft of intellectual property.[151] China's Foreign Ministry called the allegations "slanderous" and urged the United States to withdraw the accusation.[152] It added that it would take the measures needed to safeguard its own cybersecurity and interests.[153] This has become the two-step response to any accusation: deny knowledge of the wrongdoing and reprimand any entity pushing towards finding the culprit.[154] The international community's apathy toward non-state actors will become a thorn in the side of any action the U.N. takes. If these actors can act without accountability to U.N. policies, sovereign states will use these groups to do their bidding without recourse.

B. The Need for a New Global Cyberwarfare Framework

The combination of these regulatory gaps calls for a new agreement. Attempting to stretch current regulations to cover cyberwarfare creates issues for all nations. U.N. countries, regardless of their cyber capabilities, are subject to the now clouded Article 41 and Article 42 and the closing force-gap between Article 2(4) and Article 51. If U.N. member states find themselves victims of conduct of non-state actors, these countries would spin their wheels to find a culprit while the bad actor slithers into the shadows of cyberspace. Action must be taken to supplement or replace the current, unsustainable regime. This paper does not suggest specific action items that should be included within a new regulation. Instead, suggested here are principles and other considerations that should act as pillars for further conversation.

Principles that underline any regulation should look ahead and consider the technological changes that may take place within cyber operations. Though technologies like the Internet of Things and its various vulnerabilities are new, researchers continue to unveil statistics that continue to surprise early forecasts.[155] The conversation surrounding cyberwarfare currently exists within a small sphere of global powers. Iran, United States, China, North Korea, Israel, and Russia currently operate as the world's foremost

151. *Id.*
152. *Id.*
153. *Id.*
154. *See, e.g.*, *China Punishes NBA After Hong Kong Tweet Fallout*, CHANNEL NEWS ASIA (Oct. 8, 2019, 5:42 PM), https://www.channelnewsasia.com/news/asia/china-suspends-nba-exhibition-broadcast-hong-kong-tweet-11981134 [https://perma.cc/U9Y6-6C26] (showing the frustration of engaging in a conversation with China that is counter to PRC goals).
155. *E.g.*, U.S. DEP'T OF COMMERCE AND DEP'T OF HOMELAND SEC., BOTNET ROAT MAP STATUS UPDATE (July 28, 2020) ("Perhaps the most surprising assessment is the forecast of smaller, rather than larger, botnet").

combatants in cyberspace.[156] With three of these countries permanently on the U.N. Security Council, any determination from this body would be well-vetted from a cyber perspective.

However, as it stands, only countries with formidable capabilities are party to this conversation. Nations without advanced cyber capabilities must have a seat at the table. Without these nations' involvement, any new policy would lack the perspective of those countries who are unable to respond with cyberweapons. In the case of a cyber attack against these nations, an Article 51 self-defense would likely come from traditional weapons and not cyberweapons. Guidelines would need to be in place to facilitate an equitable response.

Any new regulation should attempt to close the gaps highlighted in this paper. The U.N. Charter, while extremely helpful in managing rising global conflicts, was seemingly not written with cyberweapons in mind. These changes would also provide an opportunity for the international community to address the issue of non-state actors. Gaining international consensus on adjustments to Article 41 and Article 42 is a daunting task. Creating a new action classification between these articles may be an easier, more-tailored, resolution. This section could focus on defining the characteristics of cyber actions and which cyberweapons qualify as armed forces.

Countries could then fully consider cyber operations as Article 41 solutions without jumping the more restrictive bar of Article 42 action. A fully robust set of cyber options would allow for Article 41 style sanctions and arms embargos to become more effective. If the U.N. were able to use cyberweapons to block access to certain websites or communications infrastructure, countries, like North Korea, would be unable to avoid these restrictions.

In addressing the diminishing force gap, the U.N. could clearly outline the rules for the protection of political independence required by Article 2(4). Two recent examples, the Russian hacking of the U.S. 2016 election[157], and the attempted hacking of the U.S. 2020 election by Iran[158], show an emboldening of interference with political sovereignty in cyberspace. The force gap is a necessary deterrent of self-defense action by sovereign nations. The U.N. should deliberate on new policies that could deter election interference in cyberspace. These changes would allow for the force

156. Bob Mason, *So Who Has the Most Advanced Cyber Warfare Technology*, FXEMPIRE, https://www.fxempire.com/education/article/so-who-has-the-most-advanced-cyber-warfare-technology-444874 [https://perma.cc/A77B-8PSB] (last visited Oct. 28, 2019).

157. *2016 Presidential Campaign Hacking Fast Facts*, CNN (Oct. 31, 2019) ,https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html [https://perma.cc/SY75-65Z4].

158. *Iranian*, *supra* note 133.

gap to remain in place and could remove some of the growing issues from both Article 2(4) and Article 51. Unfortunately, the United States will have a tough time pushing for this conversation. With a history of interference in elections,[159] it will be important for the United States to gather a coalition of like-minded nations to determine what respect for democratic elections in cyberspace must resemble.

Turning to the issue of non-state actors, the international community must clearly define which actors are subject to these standards. As previously discussed, non-state actors cover a wide variety of entities.[160] A definition for non-state actors in cyberspace should be tailored enough to cover only entities acting illegally towards specific political or monetary goals. The additions of certain buzzwords (e.g. "terrorist") would significantly damage the reputation of globally beneficial non-state actors. Many non-state actors pursue their interests in legal ways. Any regulation should catch both scenarios presented above: 1) a non-state actor acting on their own accord within a state against that state's will, and 2) a non-state actor acting on behalf of a sovereign nation. Bodies like the U.N. and NATO are responsible for calling on their member nations to root out these bad actors and avoid their use to hide non-sanctioned state actions.

C. Implications

Touching briefly on the intended consequences of new legislation is important for pushing the international community to have this conversation. While U.S. national security is the impetus behind this paper, the global community will experience enhanced security from new legislation. With the world's interconnection becoming ever stronger, sovereign nations must take responsibility for their actions on the internet. Without legislation, the internet would continue to become a more dangerous place for commerce. New legislation outlining the appropriate conduct in cyberspace would help address concerns while carrying the conversation onward.

Rules and regulations may not fix the problem, but the U.N. is responsible for hosting the discussion about the international conduct of cyber operations. The U.N. began having these conversations in several forums.[161] Even in the beginning stages, it

159. *See, e.g.*, *Iran-Contra Affair*, HISTORY (Aug. 10, 2017), https://www.history.com/topics/1980s/iran-contra-affair [https://perma.cc/D877-NAGJ].

160. *Supra* Sec. II.A.3.

161. *E.g.*, *The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased*, COUNCIL ON FOREIGN RELATIONS (Nov. 15, 2018), https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-

is clear to see the different interests of parties rising to the top. One new U.N. resolution creates an open-ended working group sponsored by Russia,[162] and the other, sponsored by the United States, creates a new Group of Government Experts to study the interplay of international law and state action in cyberspace.[163] These conversations are the first steps toward substantial action in navigating the maze of cyberspace.

CONCLUSION

This paper attempts to expose the legal confusion created by the application of the U.N. Charter to cyber operations and suggests actions to protect U.S. national security. Instead of pursuing solutions at home, it is important to take this conversation to the largest international forum: the United Nations. As the international community attempts to map the current legal structure on top of cybersecurity, certain flaws will rise above the rest. Specifically, Article 41 versus Article 42, the closing of the force gap between Article 2(4) and Article 51, and the lack of accountability for non-state actors. These three provisions muddy the waters of the U.N. Charter and will have a distinct effect on its ability to temper flaring conflicts. Well-tested standards will be tested again in the international courts and will face new scrutiny under the misunderstanding surrounding cybersecurity. If these standards continue without change, cyberweapons will thrive in an environment where confusion allows malicious actions to go unreprimanded.

---

everyone-pleased [https://perma.cc/8U4G-FQFX] (describing two resolutions adopted by the U.N. General Assembly. The first creates a working group to study and identify norms related to cyberspace. The second creates a working group to study how international law relates to cyberspace.).

162. *Developments in the Field of Information and Telecommunications and the Context of International Security*, A/C.1/73/L.27/Rev.1 (Oct. 29, 2018).

163. *Advancing Responsible State Behavior in the Context of International Security*, A/C.1/73/L.37 (Oct. 18, 2018).