Brooklyn Journal of International Law

Volume 38 | Issue 2 Article 8

2013

Granting an Automatic Authorization for Military Response: Protecting National Critical Infrastructure from Cyberattack

Gabriel K. Park

GRANTING AN AUTOMATIC AUTHORIZATION FOR MILITARY RESPONSE: PROTECTING NATIONAL CRITICAL INFRASTRUCTURE FROM CYBERATTACK

INTRODUCTION

The Internet enables people to easily communicate across the world and freely share files, photos, and videos without geographical limitation. It has undoubtedly become essential to all modern countries in the world; it is at the cornerstone of and controls commerce, government activities, energy production and distribution, water treatment, mass transit, and emergency services.[1] However, the Internet's connectedness and openness have also allowed anyone to anonymously launch cyberattacks and inflict damage upon another country without physical limitation.[2] From hundreds of miles away and using only a laptop computer,[3] states and non-state actors[4] alike can attack another nation's critical infrastructure[5]—including sys-

---

1. *See* ANDRE COLARIK, CYBER TERRORISM: POLITICAL AND ECONOMIC IMPLICATIONS vii–xii (2006).

2. *See* THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT, NATIONAL SECURITY LAW IN CYBERSPACE 21–22 (2000).

3. *See* Lieutenant Commander Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 2 (2009).

4. In this Note, unless specified otherwise, "state" refers to a nation. A non-state actor refers to an individual or an entity that is not affiliated or under the control of a nation's government.

5. Critical infrastructure are those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, [and] national public health or safety." 42 U.S.C. § 5195c(e); Major Sean Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J. L. & TECH. 404, 406 (2007) ("Critical infrastructure includes the following sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, and postal and shipping."); *National Strategy for Homeland Security*, OFFICE OF HOMELAND SECURITY 29–30 (2002), *available at* http://www.ncs.gov/library/policy_docs/nat_strat_hls.pdf [hereinafter *National Strategy*].

tems that are vital to national security such as sectors controlling energy, transportation, food, public health, and chemical industry[6]—instantaneously causing disastrous effect to the targeted nation and its citizens.[7]

In recent years, several episodes have scratched at the surface of such disastrous possibilities. In 2007, the Russian government allegedly launched a series of cyberattacks[8] on Estonia, which essentially paralyzed the entire country; the attacks affected Estonia's commercial banks, media outlets, and government websites.[9] In 2009, Georgia also came under cyberattack, resulting in the shutdown of Georgia's government and commercial websites.[10] Just a year later, in 2010, a sophisticated virus known as Stuxnet infiltrated and significantly impaired an Iranian uranium enrichment plant by sabotaging the plant's centrifuges.[11] Stuxnet had the capacity to attack computer networks that controlled "oil pipelines, electronic utilities, nuclear facilities, and other industrial sites."[12] The most significant, and alarming, aspect of the Stuxnet episode is that the initial attacker spread the virus information across the world, and its secrets are now available to anyone who seeks

---

6. *See* Condron, *supra* note 5, at 406; *National Strategy*, *supra* note 5 at 29–30.

7. *See* Sklerov, *supra* note 3, at 18–20.

8. In this Note, "cyberattack" refers to "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them." 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, 422 (2011).

9. *See* Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia*, N.Y. TIMES (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html?scp=1&sq=estonia,%20russians&st=Search; *see also* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=5.

10. Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 46 (2009).

11. David E. Sanger, *Iran Fights Malware Attacking Computers*, N.Y. TIMES (Sept. 25, 2010), http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html?scp=8&sq=stuxnet&st=cse [hereinafter *Iran Fights Malware*].

12. *Id.*

them. As a result, anyone can download Stuxnet, redesign the code, and launch it to against a new target.[13]

The United States is especially vulnerable to cyberattack, partly due to the fact that its information and electronic networks of military, public, and private sectors are interconnected.[14] Moreover, some of the United States' adversaries already possess the ability to directly attack one of the United States' critical infrastructure sectors via cyberattack, and America may not be prepared for such attack.[15] On May 12, 2011, two years after President Obama released *Cyberspace Policy Review*, a comprehensive review of the federal government's efforts and strategy in protecting the nation's information and communication infrastructure, [16] the Obama Administration unveiled a *Cybersecurity Legislative Proposal,* a non-binding set of regulations the Obama Administration composed in order to improve the security of the nation's network and infrastructure,[17] and submitted it to Capitol Hill.[18] One of the purposes of

---

13. John Markoff, *A Silent Attack, but Not a Subtle One*, N.Y. Times (Sept. 26, 2010), http://www.nytimes.com/2010/09/27/technology/27virus.html?scp=5&sq=stuxnet&st=cse [hereinafter *A Silent Attack*].

14. *See* RICHARD A. CLARKE & ROBER K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 226–27 (2010).

15. *60 Minutes: Former Chief of National Intelligence Says U.S. Unprepared for Cyber Attack* (CBS television broadcast Nov. 8, 2009) (Transcript available at http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml) (In a 2009 interview with *60 Minutes*, Admiral Mike McConnell, former Director of National Intelligence, opined that the United States' adversaries have the capability to bring down a power grid via cyberattack, and stated that "[the] United States is not prepared for such an attack.").

16. White House, *Cyberpolicy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, (May 2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf ("But with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights. The government has a responsibility to address these strategic vulnerabilities to ensure that the United States and its citizens, together with the larger community of nations, can realize the full potential of the information technology revolution.").

17. *Cybersecurity Proposal,* WHITE HOUSE, (May 12, 2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf [hereinafter *Cybersecurity Proposal*].

the *Proposal* was to "protect our national security by addressing threats to our power grids, water systems, and other critical infrastructure."[19]

In order to address the growing threat of cyberattacks, there have been efforts to create international agreements to regulate cyberspace, to analogize the issue of cyberattacks to current international law, and even to ban cyber weapons.[20] However, these efforts have not been successful and are not adequate to address the danger of cyberattacks on national critical infrastructure.[21] Scholars argue that any international treaty regarding cyberspace will be insufficient and nearly impossible to enforce,[22] and it is unclear whether the current international legal regime can govern cyberattacks.[23] Making matters more difficult, and the current international efforts even less adequate, is the attribution problem;[24] due to the anonymity aspect

18. Howard A. Schmidt, *The Administration Unveils Its Cybersecurity Legislative Proposal*, THE WHITE HOUSE BLOG (Sept. 20, 2011, 2:00 PM), http://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal.

19. *Id*.

20. *See* Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185, 2296 U.N.T.S. 123 (In 2001, the Council of Europe drafted and adopted Convention on Cybercrime, the first international treaty seeking to address crimes in cyberspace) [hereinafter Convention on Cybercrime]; *see also* Todd Leaven & Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny*, 12 N.C. J.L. & TECH. ON. 1, 15–22 (2010) (describing the debate over establishment of international agreement regarding cyberattacks); *see also* Waxman, *supra* note 8, at 426 (examining the challenge of addressing cyberattacks by using Articles 2(4) and 51 of the United Nations Charter).

21. *See* Duncan B. Hollis, *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 391 (2011); *see also* Leaven & Dodge, *supra* note 20, at 19–20; Scott J. Shackelford, *Article: From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKLEY J. INT'L L. 192, 216–18 (2009);

22. *See* Leaven & Dodge, *supra* note 20, at 23–24; *see also* Hollis, *supra* note 21, at 392–93.

23. *See* Waxman, *supra* note 8, at 427 (stating that Charter Article 2(4)'s prohibition of use of force is difficult to interpret); *see also* Hollis, *supra* note 21, at 393 ("First, states must not launch (or threaten) a cyberattack that qualifies as a use of force . . . . This prohibition is vague in its particulars.").

24. Attribution refers to the ability to trace back to the original machine, actor, or entity that initiated the cyberattack. David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 531, 531–32 (2011).

of the basic architectural structure of the Internet, it is difficult to pinpoint the original initiator of a cyberattack.[25]

Although international treaties regulating cyberspace may be ineffective, to most effectively protect national critical infrastructure against cyberattacks, an international agreement is needed that will authorize a nation that has been cyberattacked to respond with military action. Part I of this Note provides a background to explain the immediacy and the potential disastrous effect of a cyberattack to a country's critical infrastructure. Part II discusses the attribution problem of cyberspace and its effect on regulation of cyberattacks. Part III explains possible response measures under the current international law, argues the inadequacy of current international law, and explores the difficulty of establishing a future, hypothetical international legal regime regarding cyberattacks on critical infrastructure. Finally, Part IV proposes an international agreement that will grant automatic authority for a nation to respond with a military action against a state[26] that has launched a cyberattack upon the nation's critical infrastructure, and explains how the proposed agreement will also minimize the attribution problem. Furthermore, Part IV elucidates the need for such agreement, its effectiveness, and nations' incentives to join the proposed international agreement.

I. BACKGROUND: IMMEDIACY AND THE POTENTIALLY DISASTROUS EFFECTS OF A CYBERATTACK ON NATIONAL CRITICAL INFRASTRUCTURE

A. Types, Purposes, and Impacts of a Cyberattack

A foreign state or a non-state actor can use different types of cyberattacks against another nation to achieve different purposes. There are largely three categories of cyberattacks: Internet-delivered malicious software,[27] denial-of-service ("DOS")

---

25. For a detailed explanation, *see id.* at 542–44; *see also* Hollis, *supra* note 21, at 397–98.

26. The proposed international agreement will grant an injured state authority to respond with military action against any state that has launched a cyberattack on its critical infrastructure, or against a state from which a non-state entity has launched a cyberattack, regardless of whether the government authorized the attack.

27. Sklerov, *supra* note 3, at 13–14. For further information, *see* Major John S. Fredland, *Building a Better Cybersecurity Act: Empowering the Exec-*

attacks,[28] and "unauthorized remote intrusion into computer systems by individuals."[29] The Internet-delivered malicious software, more commonly known as "malware," affects computer systems by infecting e-mails, exploiting vulnerable engines, and visiting infected websites.[30] The denial-of-service attack targets a computer system, and overwhelms it with information until it seizes and can no longer function.[31] The most severe form of DOS attack is a distributed-denial-of-service ("DDoS") attack because, in addition to shutting down computer systems, it can make the system more vulnerable to other forms of attacks by affecting the system's defenses.[32] The individual remote intrusion involves unauthorized access to a computer system by an attack,[33] which enables the attacker to harm the system in any number of ways.[34]

A state or a non-state actor can use these different types of cyberattacks to perform a variety of tasks: from stealing someone's identity to illegally extracting classified data.[35] A cyberattack that extracts confidential information can result in loss of millions of dollars. For example, in 2007, the Federal Bureau of Investigation estimated that cyberattacks caused an average financial loss of $167,713 per attack and "over $400 billion in damages in the United States."[36] Not long after, during a 2009 speech, President Obama stated that in 2008 alone cyber criminals stole intellectual property worth up to one trillion dollars from businesses around the world.[37] More recently, in 2010, Google, and more than thirty other U.S. companies, suffered

---

utive Branch Against Cybersecurity Emergencies, 206 MIL. L. REV. 1, 10–13 (2010).

28. Sklerov, *supra* note 3, at 13–14; *see also* Fredland, *supra* note 27, at 10.

29. *Id.*

30. RICK LEHTINEN ET AL., COMPUTER SECURITY BASICS 3–21 (2d ed. 2006).

31. *Id*. at 81.

32. COLARIK, *supra* note 1, at 103.

33. *Id*. at 94.

34. *See id*. at 84.

35. *See* Clark & Landau, *supra* note 24, at 536–42.

36. Sklerov, *supra* note 3, at 18 n.95 (citing CLAY WILSON, CONG. RESEARCH SERV., RL32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 27–29 (2008)).

37. Barack Obama, President of the United States of America, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009) (transcript available at http://www.whitehouse.gov/the_press_office/remarks-by-the-president-on-securing-our-nations-cyber-infrastructure).

cyberattacks that illegally downloaded intellectual property data from the companies' computer networks.[38]

In addition to attacking individuals or private companies, cyberattack's severity can elevate to the matter of national security. A cyberattack can "pry into a state's public, sensitive and classified computers . . . to manipulate data; to deceive decision makers; to influence public opinion; and even to cause physical destruction from remote locations abroad."[39] As noted above, Georgia and Estonia experienced firsthand the effect that a cyberattack can have on their national security, and the United States has also suffered national security breaches from cyberattacks. For instance, in 2008, there was a breach in the U.S. military computer network when an unknown person inserted a flash drive to a military laptop; the malware inside the flash drive stole a great amount of classified information.[40] On July 4, 2009, a DDoS attack affected a number of U.S. and South Korean government websites.[41] Specifically, the attacks shut down the U.S. Secret Service website, including its Treasury and Transportation Departments pages,[42] and South Korea's Blue House,[43] Defense Ministry, and National Assembly websites.[44] Cyberattacks such as these, attempting to steal classified national security information and to shut down government websites, still continue and are not likely to stop anytime soon.[45]

---

38. John Markoff et al., *In Digital Combat, U.S. Finds No Easy Deterrent*, N.Y. TIMES (Jan. 26, 2010), http://www.nytimes.com/2010/01/26/world/26cyber.html?scp=1&sq=in%20digital%20combat,%20u.s.%20finds%20no%20easy%20deterrent&st=cse.

39. Sklerov, *supra* note 3, at 17–18 (quoting WINGFIELD, *supra* note 2, at 21–22).

40. Waxman, *supra* note 8, at 444.

41. Choe Sang-Hun & John Markoff, *Cyberattacks Jam Government and Commercial Websites in U.S. and South Korea*, N.Y. TIMES (July 9, 2009), http://www.nytimes.com/2009/07/09/technology/09cyber.html?scp=1&sq=cyberattacks%20jam&st=cse.

42. *Id.*

43. Blue House is South Korea's equivalent of the White House.

44. Sang-Hun & Markoff, *supra* note 41.

45. General Keith Alexander, the Director of National Security Agency, stated that, in 2010 the Department of Defense alone was subject to "hundreds and thousands" of cyberattack attempts everyday. Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*, 2 HARV. NAT'L SEC. J. 591, 592 (2011).

B. Potential Impact of a Cyberattack on National Critical Infrastructure

Although cyberattacks can have a variety of negative impacts on national security, scholars believe that the most dangerous attacks are those against a nation's critical infrastructure.[46] A direct cyberattack to a nation's critical infrastructure will "likely result in significant loss of life, as well as economic and social degradation."[47] Citizens' confidence in their government will decline dramatically, and the rise in the level of fear among citizens will "impact the basic social fabric."[48] According to Richard Clarke, the former Chair of the President's Critical Infrastructure Protection Board, a successful cyberattack on vulnerabilities in the U.S. critical infrastructure will likely be disastrous: "Transportation systems could grind to halt. Electronic power and natural gas system[s] could malfunction. Manufacturing could freeze. 911 Emergency call centers could jam. Stock, bond, futures, and banking transactions could be jumbled . . . our forces [will be] at great risk by having their logistics system fail."[49] As Clarke has eluded, the days when a cyberattack could result in the mere theft of documents seem to be over.

C. Emergence of Stuxnet and Future Cyberattack on Critical Infrastructure

The danger of a cyberattack on national critical infrastructure increases as the complexity and sophistication of cyberattacks advance. Cybersecurity experts and analysts widely be-

---

46. Sklerov, *supra* note 3, at 18 n.95; *see* Timothy Shimeall et al., *Countering Cyber War*, 49 NATO REV. 16, 17–18 (Winter 2001/2002), *available at* http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf; *see also*, Rebecca C. E. McFadyen, *Protecting the Nation's Cyber Infrastructure: Is the Department of Homeland Security Our Nation's Savior or the Albatross Around Our Neck?*, 5 I/S: J.L. & POL'Y FOR INFO. SOC'Y 319, 342 (2009).

47. Shimeall, *supra* note 46, at 17.

48. *Id*. at 18 (describing the likely results of a cyberattack on different pillars of a nation's critical infrastructure).

49. *Cyber Security: The Challenges Facing Our Nation in Critical Infrastructure Protection: Hearing Before Subcomm. on Tech., Info. Policy, Intergovernmental Relations and the Census of the Comm. on Gov't Reform H.R.*, 108th Cong. 13 (2003) (statement of Richard Clark, Special Advisor, United States National Security Council).

lieve that Stuxnet[50] was responsible for destroying one-fifth of Iran's nuclear centrifuges in 2010.[51] When Stuxnet first surfaced in 2009, experts described it as "the most sophisticated cyberweapon ever developed."[52] The Stuxnet malware that attacked the Iranian nuclear facilities appears to have included two major components: the first component was designed to spin Iran's nuclear centrifuges wildly out of control, and the second component "secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart."[53] The program was successful, and the engineers and officials of the Iranian nuclear facilities did not notice that Stuxnet was sabotaging their nuclear facilities.[54]

What separates Stuxnet from previous viruses and malwares used for cyberattack is that it had the ability to "jump from

---

50. Cybersecurity experts widely believe that Israel and the United States were behind the development, testing, and eventual launch of Stuxnet in order to disrupt Iran's nuclear program development. *See Iran Fights Malware*, *supra* note 11; *see also Times Topics: Stuxnet*, N.Y. TIMES (Jan. 15, 2011), http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html?inline=nyt-classifier [hereinafter *Stuxnet*]. *But see* John Markoff, *A Code of Chaos*, N.Y. TIMES (Oct. 2, 2010), http://www.nytimes.com/2010/10/03/weekinreview/03markoff.html?scp=6&sq=stuxnet&st=cse (noting that it is unlikely that Israeli and U.S. governments left such blatant clues, and the real authorship of Stuxnet is not likely to be discovered) [hereinafter *A Code of Chaos*]. However, according to an article in the *New York Times* in June 2012, Stuxnet was developed by the United States and Israel to "slow the progress of Iran's nuclear efforts. David E. Sanger, *Obama Order Sped up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?hp [hereinafter *Cyberattacks Against Iran*].

51. *Times Topics: Iran's Nuclear Program (Nuclear Talks 2012)*, N.Y. TIMES (Oct. 21, 2012), http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html?scp=3&sq=stuxnet,%20iran&st=cse [hereinafter *Iran's Nuclear Program*].

52. William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

53. *Stuxnet*, *supra* note 50.

54. *Id.*

Windows-based computers to a specialized system used for controlling industrial equipment, like electric power grids, manufacturing plants, gas pipelines, dams and power plants."[55] Previously, and in contrast, most types of cyberattacks focused on extracting privileged information from websites and corporate or military networks.[56] Whoever created Stuxnet intended the virus to go after industrial systems and specifically attack a country's critical infrastructure.[57]

Though the Iranian episode has passed, Stuxnet is still capable of wreaking havoc. Although Stuxnet is a technological wonder and a proof of advancement in computer technology, it is a weapon that poses significant danger to many nations' critical infrastructure. As mentioned earlier, the most frightening part of Stuxnet is that the creator of Stuxnet spread the malware throughout the world.[58] The Stuxnet code has appeared in many countries, including China, India, Indonesia, and Iran,[59] and it continues to spread at an alarming rate.[60] Melissa Hathaway, a former U.S. National Cybersecurity Coordinator, stated that "[p]roliferation is a real problem, and no country is prepared to deal with it."[61] Another problem with Stuxnet is that it is "highly visible," meaning any government or cybersecurity companies can dissect and examine the Stuxnet code.[62] This is dangerous because there is always a possibility of an attacker creating different versions Stuxnet and launching new assaults.[63] In fact, in October 2011, a new Stuxnet-like virus

---

55. *A Code of Chaos*, *supra* note 50.

56. *Id*.

57. *See A Silent Attack*, *supra* note 13; *see also* William J. Broad & David E. Sanger, *Worm Was Perfect for Sabotaging Centrifuges*, N.Y. TIMES (Nov. 18, 2012), http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html?pagewanted=all (In the case of Iranian nuclear facilities, experts determined that Stuxnet "had been precisely calibrated in a way that would send nuclear centrifuges wildly out of control.").

58. *A Silent Attack*, *supra* note 13 (exploring different theories on the reason behind the widespread of Stuxnet). It seems that an element of the Stuxnet program was released accidentally. *See Cyberattacks Against Iran*, *supra* note 50.

59. *A Code of Chaos*, *supra* note 50.

60. *A Silent Attack*, *supra* note 13.

61. *Id*.

62. *Id*.

63. *Stuxnet*, *supra* note 50.

called "Duqu" emerged, equally capable of threatening the security of a country's critical infrastructure.[64]

Creating a virus or program that is as advanced and complex as Stuxnet is not easy or cheap. Some have speculated that the cost of creating Stuxnet was approximately $1 million and that the virus was "sophisticated enough to have required backing of one or more nation states."[65] In fact, an article from the *New York Times* highlighted the difficulty that the United States had in developing what later became known as Stuxnet until there was a breakthrough aided by the Israeli government.[66] This demonstrates that it is unlikely that non-state entities, individuals, or less developed countries with limited technology and resources have the ability to create a type of cyberattack that is equally or more sophisticated and destructive than Stuxnet.

Due to the emergence of Stuxnet, the world is now aware of a type of cyberattack that can directly target a nation's critical infrastructure and bring about devastating effect. If there is a successful cyberattack on a country's oil pipelines, nuclear plants, stock market, or water plants, it can have a devastating effect on the country's entire population. Thus, it is imperative that the international community quickly creates a method to effectively address and prevent such a cyberattack on national critical infrastructure.

II. THE ATTRIBUTION PROBLEM

The attribution problem is the source of much of the challenges of regulating cyberspace.[67] Simply put, cyberspace provides a platform where one can engage in activity anonymously.[68] Anonymity can create problems even at the most basic lev-

---

64. John Markoff, *New Malicious Program by Creators of Stuxnet Is Suspected*, N.Y. TIMES (Oct. 18, 2011), http://www.nytimes.com/2011/10/19/technology/stuxnet-computer-worms-creators-may-be-active-again.html [hereinafter *New Stuxnet*].

65. Ben Flanagan, *Former CIA Chief Speaks out on Iran Stuxnet Attack*, NAT'L (Dec. 15, 2011), http://www.thenational.ae/thenationalconversation/industry-insights/technology/former-cia-chief-speaks-out-on-iran-stuxnet-attack (noting that it cost approximately $1 million to create the Stuxnet virus).

66. *See Cyberattacks Against Iran*, *supra* note 50.

67. For an in-depth discussion of attribution issues, see Clark & Landau, *supra* note 24, at 531.

68. Hollis, *supra* note 21, at 397.

el of the Internet use. For example, the anonymous aspect of the Internet has enabled schoolchildren to engage in cyberbullying, a label for online activities of teasing, harassing, or abusing others.[69] When dealing with normal Internet uses, government agencies and police can often track down the person who posted such comments through an Internet Protocol ("IP") address with the assistance of an Internet Service Provider.[70]

However, IP address tracing has many flaws.[71] An IP address may be a corporate account that actually holds numerous internal accounts or may lead to a physical location that provides free access to the general public, such as a coffee shop.[72] Even when an IP address leads to the original machine that initiated a cyberattack, it may be a computer corrupted with a virus. Using a virus in this way, an attacker can launch a cyberattack remotely from the corrupted computer, thereby concealing his actual identity.[73] In fact, many computers in the United States are infected with viruses without the knowledge of the owners or users, and an attacker can use these computers to remotely launch attacks on other computers or networks.[74] Additionally, a skilled hacker can leave "false flag," making an innocent entity seem responsible for a cyberattack.[75]

Even if some attacks are traceable, it takes much effort, expertise, and expense to track them.[76] When a government agency or a security firm is successful in determining the origi-

---

69. *See* Times Topics: *Cyberbullying*, N.Y. TIMES (Nov. 26, 2011), http://topics.nytimes.com/top/reference/timestopics/subjects/c/cyberbullying/index.html?scp=1&sq=cyber%20bullying&st=cse ("Its amorphous nature and the rapidly changing technological landscape have made it difficult for schools and even the courts to address the cyberbullying.").

70. Clark & Landau, *supra* note 24, at 545. If the Internet Service Provider ("ISP") keeps a good record of IP addresses that it assigns, then it can trace which computer had an IP address that it assigned. However, since ISPs regularly clear their IP address logs, a request to track the source must happen quickly. Hollis, *supra* note 21, at 398–99.

71. *Id.*

72. *Id.*

73. *Id.* at 378.

74. Fredland, *supra* note 27, at 11 (citing Jack Goldsmith, *Can We Stop the Global Cyber Arms Race?*, WASH. POST (Feb. 1, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/01/31/AR2010013101834.html); Hollis, *supra* note 22, at 378.

75. Hollis, *supra* note 21, at 397.

76. *See id.* at 398–400; Condron, *supra* note 5, at 418.

nal machine that initiated the attack, it still must identify the *person* who launched it.[77] Yet even if the computer user whose activity sparked the cyberattack can be identified, the question of who was actually behind the attack remains.[78] An individual, terrorist group, or even a nation state, could have launched the cyberattack;[79] merely identifying the individual person who used the machine that initiated the attack may not necessarily unveil the actual entity behind the cyberattack.[80] Pinpointing the actual entity that originated the cyberattack is important because the responsive action that a government can take will differ based the nature of that identity.[81]

It is virtually impossible to track down the original entity behind a sophisticated cyberattack.[82] Cybersecurity experts claim that they will never know who was behind the creation of Stuxnet and its launch on the Iranian nuclear facility.[83] This poses a problem in regulating cyberspace because without a system that can catch and prosecute the perpetrator, it will be difficult to deter cyberattack attempts.[84] Effective deterrence comes from catching the perpetrator and rendering an appropriate punishment,[85] but if one can remain anonymous and untraceable throughout a cyberattack, then there is no reason for that entity to stop launching cyberattacks.[86] Thus, the attribution problem becomes the main issue of any international agreement attempt to regulate cyberattacks. Unless the basic

77. *See* Clark & Landau, *supra* note 24, at 542–43, 547.

78. Condron, *supra* note 5, at 417.

79. *Id*. at 404; Shackelford, *supra* note 21, at 199–200.

80. *See* Toby L. Friesen, *Resolving Tomorrow's Conflicts Today: How New Developments Within the U.N. Security Council Can Be Used to Combat Cyberwarfare*, 58 NAVAL L. REV. 89, 105 (2009); *see also* Hollis, *supra* note 21, at 399–400.

81. Friesen, *supra* note 80, at 103.

82. Hollis, *supra* note 21, at 378.

83. *A Code of Chaos*, *supra* note 50.

84. *See* Leaven & Dodge, *supra* note 20, at 25.

85. Sklerov, *supra* note 3, at 8–9.

86. Leaven & Dodge, *supra* note 20, at 17 ("As one might expect, current international agreements that might be translated to cyber-warfare are presumed to concern relations among different nations, instead of individual actors. Uncertainty still remains, therefore, in how the same law can be translated to individuals, acting independently from any government, who may engage in cyber-warfare.").

structure and architecture of the Internet changes,[87] it will be impossible to accurately trace back to the original entity every time. However, thorough and stringent enforcement of criminal law can minimize the attribution problem,[88] and Part IV of this Note will explain how the international agreement to use military force can compel countries to exercise their domestic law enforcement to deter cyberattacks.

III. THE INEFFECTIVENESS OF THE CURRENT AND FUTURE INTERNATIONAL AGREEMENTS IN ADDRESSING CYBERATTACKS ON NATIONAL CRITICAL INFRASTRUCTURE

A. Current International Treaty

The development in capabilities and sophistication of cyberattacks led to a widespread call for an international treaty expanding to cyberattacks the current application of the law of war.[89] However, preexisting international treaties are inadequate to address and deter cyberattacks on a nation's critical infrastructure. The European Convention on Cybercrime treats cyberattacks as only a criminal matter, rather than as a national security matter. Also, the current bodies of international law, such as the Geneva Convention and the United Nations Charter, primarily govern relations among nation states and not non-state actors. Moreover, it is ambiguous whether the issue of cyberattacks can fit into the legal regime of the current international law.

1. The Convention on Cybercrime

In 2001, the Council of Europe adopted the Convention on Cybercrime, the first international treaty addressing cyberat-

87. Although some scholars argue for the change in the very architecture of the Internet, most scholars believe that such a change will not solve the attribution problem. *See* Clark & Landau, *supra* note 24, at 533 ("Redesigning the Internet so that all actions can be robustly attributed to a person would not help to deter the sophisticated attacks we are seeing today. At the same time, such a change would raise numerous issues with respect to privacy, freedom of expression, and freedom of action . . . .").

88. *See* COLARIK, *supra* note 1, at 39; *see also* Christopher E. Lentz, *A State's Duty to Prevent and Respond to Cyberterrorist Acts*, 10 CHI. J. INT'L L. 799, 820–22 (2010).

89. Leaven & Dodge, *supra* note 20, at 15.

tacks.[90] The Convention "requires parties to adjust their domestic criminal law to proscribe certain commonly defined offenses such as illegal access and data interference."[91] It also requires member states to cooperate in investigating cybercrimes, to disclose digital evidence, and to prosecute cybercriminals.[92] Currently, this is the only cyber-specific treaty, and so far twenty-nine European states and the United States have joined the Convention on Cybercrime.[93]

Although the Convention on Cybercrime tries to promote cooperation among member states to prosecute and deter cybercriminals, it has numerous flaws. First of all, it does not involve many key nations that are often at the center of cyberattack incidents and not even all of the European nations have ratified it.[94] Outside of the twenty-nine European states, the United States is the only non-European nation to join the treaty.[95] Second, the Convention on Cybercrime, as the title of the treaty suggests, specifically focuses on criminal laws and criminal prosecution of cyberattackers.[96] The purpose of the Convention is to effectively fight against cybercrime by "requir[ing] increased, rapid and well-functioning international cooperation in criminal matters."[97] The Convention does not mention any situations involving cyberattacks initiated by a member state's government or military. This poses a problem because if a cyberattack comes from a government agency or military, "neither domestic nor international rules regulating cy-

---

90. *See* Convention on Cybercrime, *supra* note 20.

91. Hollis, *supra* note 21, at 392; Convention on Cybercrime, *supra* note 20, art. 2–13.

92. Convention on Cybercrime, *supra* note 20, art. 14–35.

93. *Id.*

94. *Id.* Russia, a European nation that is often associated with both cyberattacks and cybersecurity, did not join the treaty. Hollis, *supra* note 21, at 393 n.124.

95. Convention on Cybercrime, *supra* note 20. Asian countries such as China and South Korea have been heavily involved in cybersecurity incidents and they have not joined the Convention on Cybersecurity. *See Convention on Cybercrime CETS No.: 185*, Treaty Office, COUNCIL OF EUROPE, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (last visited Jan. 23, 2013).

96. Convention on Cybercrime, *supra* note 20, at 169–70.

97. *Id.* ("The Present Convention is intended to . . . make criminal investigations and proceedings concerning criminal offenses related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence.").

bercrime will apply."[98] Thus, a member state's cyberattack upon another member state's critical infrastructure will not fall within the scope of the Convention on Cybercrime.

In addition, treating a cyberattack as a criminal matter does not effectively address national security concerns deriving from cyberattacks, generally. Criminal investigation requires a methodical process of gathering evidence.[99] This can lead to a slow and unsuccessful response to a cyberattack.[100] Even if the Convention on Cybercrime is effective at increasing the speed of criminal procedure, it does not guarantee that member states will practice stringent criminal laws to oversee their cyberattack activities.[101]

2. The Geneva Convention and the U.N. Charter

Ambiguities in various provisions of current international treaties and agreements create confusion and doubt as to whether they encompass the issue of cyberattacks.[102] Also, the legal structures of current international law do not adequately deal the increasing threat of cyberattacks.[103] Although some scholars have broadly interpreted the law of war under the Geneva Convention to include cyberattacks,[104] others have widely criticized it as being inapplicable to address evolving forms of cyberattacks.[105] The Geneva Convention is a body of law that deals with the law of war; however, Professor Duncan Hollis argues that the existing legal system under the Geneva Convention suffers from

---

98. Hollis, *supra* note 21, at 393.

99. Condron, *supra* note 5, at 407.

100. *Id*.

101. Sklerov, *supra* note 3, at 8–9 ("When states fail to pass stringent criminal laws or look the other way when attackers strike rival states, criminal laws are rendered impotent.").

102. *See* Waxman, *supra* note 8, at 443.

103. *See* Leaven & Dodge, *supra* note 20, at 16–17; *see also* Hollis, *supra* note 21, at 405–06 (arguing not only that the current law's response to cyberwarfare is insufficient, but it can also be dangerous; since it is not clear who launched the cyberattack due to the attribution problem, a mistake in responding to a wrong, innocent target can be devastating).

104. *National Infrastructure Protection Plan*, U.S. DEP'T OF HOMELAND SEC., at 57, Feb. 2009, *available at* http://www.fas.org/irp/agency/dhs/nipp.pdf; *see also* Leaven & Dodge, *supra* note 20, at 16.

105. *See id*.

> several, near-fatal conditions: *uncertainty* (i.e., states lack a clear picture of how to translate existing rules into the IO [information operations] environment); *complexity* (i.e., overlapping legal regimes threaten to overwhelm state decision makers seeking to apply IO); and *insufficiency* (i.e., the existing rules fail to address the basic challenges of modern conflicts with non-state actors and facilitate IO in appropriate circumstances).[106]

Scholars have argued that a cyberattack may constitute "use of force" under Article 2(4) of the U.N. Charter and are therefore already prohibited.[107] However, it is not clear whether a cyberattack can fall within the scope of Article 2(4).[108] There are multiple possible interpretations of this provision,[109] which can create confusion and vagueness with regard to its precise meaning.[110] Traditionally, the extent of the meaning of Article 2(4) was narrowly focused on military violence.[111] Although a cyberattack on certain infrastructure can bear some similarities to physical military force, the issue of cyberattacks is a new one—with unique and unpredictable characteristics—that does not fall neatly into the category of military force.[112]

Furthermore, it is unclear whether a cyberattack can constitute an "armed attack" under the doctrine of self-defense pursuant to both Article 51 of the U.N. Charter and customary international law.[113] Scholars have argued that a nation can respond to a cyberattack with military force based on Article 51

---

106. Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1029 (2007).

107. U.N. Charter art. 2, para. 4; *see* Waxman, *supra* note 8, at 427.

108. *See id*. at 431.

109. *See* Hollis, *supra* note 21, at 427–30 (offering three possible interpretations of "use of force" of the U.N. Charter, Art. 2(4): force as armed violence, force as coercion, and force as interference); *see also* Waxman, *supra* note 8, at 428–30 (discussing the possible meanings of "force" under U.N. Charter 2(4) as armed force, coercion, or interference).

110. *See* Oscar Schachter, *The Rights of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1624 (1984) ("The paragraph is complex in its structure[,] and nearly all of its key terms raise questions of interpretation."); *see also* Hollis, *supra* note 21, at 427.

111. *See* Waxman, *supra* note 8, at 431.

112. *See id*.

113. *See* Condron, *supra* note 5, at 413; *see also* Sklerov, *supra* note 3, at 31–33 (providing an in-depth discussion on the subject of the self-defense under the U.N. Charter, Article 51 and customary international law).

of the U.N. Charter,[114] which provides that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defen[s]e if an armed attack occurs against a Member of the United Nation."[115] Also, under customary international law, a victim-state and its allies have authority to use force in response to an armed attack.[116] However, the U.N. Charter offers no definition of the meaning of "armed attack."[117] Although certain cyberattacks that are capable of inflicting physical damage will challenge the bounds of the meaning of "armed attack,"[118] a cyberattack is often deemed to fall short of "armed force."[119]

Moreover, current international treaties apply only to relations among different nation states, and not individual non-state actors.[120] This is an important issue because the ability of a nation to appropriately retaliate within an international legal regime depends on what type of entity initiated the attack.[121] Since the terrorist attacks of September 11, 2001, the United States and other countries have interpreted customary international law to allow "states to now treat the law of self-defense as applicable to acts by non-state actors."[122] Nevertheless, it is uncertain whether these international treaties can govern individual attackers who act independently of any government.[123]

---

114. *See* Waxman, *supra note* 8, at 427.

115. U.N. Charter art. 51. This provision serves as an exception to the general prohibition of use of force laid out in the U.N. Charter, Article 2(4).

116. *See* Michael Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 513, 529 (2003) (describing how a response under the self-defense doctrine must comply with principles of customary international law—necessity, proportionality, and imminency—discussed *infra* Part IV); *see also* Sklerov, *supra* note 3, at 28 n.179 ("Unlike treaty-based law, which only binds parties to the treaty, customary international law binds all states to it. Customary international law is formed when state practice mature to the point that it evidences *opinio juris sive* necessitates, a belief on the part of states that engaging in that practice is legally obligatory.").

117. WINGFIELD, *supra* note 2, at 78.

118. Waxman, *supra* note 8, at 431.

119. Sklerov, *supra* note 3, at 31.

120. Leaven & Dodge, *supra* note 20, at 17.

121. *Id.*

122. Schmitt, *supra* note 116, at 539; Sklerov, *supra* note 3, at 40.

123. Leaven & Dodge, *supra* note 20, at 17.

B. The Difficulty of Establishing an Effective Future International Agreement on Cyberattacks

In order to address flaws and uncertainties regarding the current international agreements, scholars and politicians have called for a more effective international cyber-warfare treaty.[124] However, it is unlikely that the international community will establish such a treaty anytime soon.[125] Unless there is a complete overhaul of the current structure of the Internet and cyberspace, the attribution problem will always exist.[126] If a government cannot trace and prosecute the attacker, then any such treaty will have no enforcement power.[127]

Moreover, Russia and the United States, two nations heavily involved in the growing area of cyberattacks, are currently in disagreement over an international treaty.[128] In 1998, the Russian government proposed that U.N. member states form a treaty to ban cyberweapons.[129] Russia, concerned with increasing danger of military activities on civilian networks, argued for its proposed treaty by comparing it to existing treaties regulating nuclear, chemical, and biological weapons.[130] However, the United States disagreed and argued that it is "impossible to

---

124. *See id.* at 19–20.

125. *See id.*; *see also* Adam Segal & Matthew Waxman, *Why a Cybersecurity is a Pipe Dream*, CNN (Oct. 27, 2011, 2:01 PM), http://globalpublicsquare.blogs.cnn.com/2011/10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/?iref=allsearch ("Different interests among powerful states—stemming from different strategic priorities, internal politics, public-private relationships and vulnerabilities—will continue to pull them apart on how cyberspace should be used, regulated, and secured.").

126. Hollis, *supra* note 21, at 398–99; Leaven & Dodge, *supra* note 20, at 22.

127. Leaven & Dodge, *supra* note 20, at 22.

128. *Id.* at 19–20; Hollis, *supra* note 21, at 406–07; *see* Segal & Waxman, *supra* note 125 ("With the United States and European democracies at one end and China and Russia at another, states disagree sharply over such issues as whether international laws of war and self-defense should apply to cyber attacks, the right to block information from citizens, and the roles that private or quasi-private actors should play in Internet governance.").

129. *See* U.N. GAOR, 53d Sess., 1st Comm., Letter dated 23 September 1998 from the Minister for Foreign Affairs of the Russian Federation Addressed to the Secretary-General, U.N. Doc. A/C.1/53/3 (Sept. 30. 1998); *see also* Hollis, *supra* note 21, at 406–07.

130. *See* John Markoff & Andrew E. Kramer, *In Shift, U.S. Talks to Russia on Internet Security*, N.Y. TIMES (Dec. 12, 2009), http://www.nytimes.com/2009/12/13/science/13cyber.html?scp=1&sq=u.s.%20talks%20to%20russia%20on%20web%20security&st=cse.

draw a line between the commercial and military uses of hardware and software."[131] Instead, the United States called for increased cooperation among nations in opposing cybercrime and stronger cybersecurity measures within each nation's network.[132]

The United States' position is understandable. The total banning of cyberattacks, made up entirely of computer codes, presents a difficulty in enforcement that is entirely different than that of nuclear or chemical weapons.[133] Unlike nuclear or chemical weapons, hacking skills and hacking codes are available to the general population throughout the world, and many entities can develop and obtain them without as much expense or difficulty as a nuclear weapon would require.[134] Also, any international treaty banning cyberweapons will limit the United States' position in cyberspace.[135] The United States is continuously and consistently the target of a countless number of cyberattacks, and the functionality of the country heavily depends on sophisticated and well-connected computer networks.[136] Furthermore, about 80 percent of the global Internet traffic passes through the United States.[137] Yet despite the United States' constant threat of suffering cyberattacks, the nation still holds the premier position in cyberspace. Thus, the United States is not likely to limit its available responses to a cyberattack by agreeing to a total-ban treaty of any potential cyberweapons.[138]

IV. INTERNATIONAL AGREEMENT GRANTING AUTOMATIC LEGAL AUTHORITY TO RESPOND WITH MILITARY ACTION

To effectively protect nations from a cyberattack, there must be an international agreement ("Proposed Agreement" or "Agreement") that grants a member state the legal authority to respond with a military action to a cyberattack to its critical

131. *Id.*
132. *See id.*
133. Hollis, *supra* note 21, at 407.
134. *Id.*
135. Leaven & Dodge, *supra* note 20, at 26.
136. Friesen, *supra* note 80, at 97–98.
137. Leaven & Dodge, *supra* note 20, at 26.
138. *Id.* Also, the United States "will resist banning of cyberespionage [and cyber exploitation, which] the international law currently tolerates." Hollis, *supra* note 21, at 407.

infrastructure. The military response under the Proposed Agreement will adhere to the customary international law principles of necessity and proportionality. Since the threat of cyberattack on a country's critical infrastructure is real and imminent, the international committee should view such an attack as a threat to national security. Also, the Proposed Agreement will minimize the attribution problem of cyberattacks to critical infrastructure by compelling member states to exercise rigorous criminal law enforcement of cyberattacks. The Proposed Agreement will create a strong incentive for nations, especially those that depend heavily on computer networks to operate their critical infrastructure, to join the Agreement because it will prevent cyberattacks on their critical infrastructure.

As for selecting or creating a body to pass the Proposed Agreement, it makes sense that the U.N. should be in charge of the task. The Proposed Agreement's goal is to prevent a sophisticated cyberattack from seriously harming a country's critical infrastructure, which certainly falls within the scope of the U.N.'s mission to "maintain[] international peace and security."[139] Additionally, the U.N. has 193 member states,[140] and has vast experience in passing international treaties and agreements.[141] Therefore, the U.N. is an ideal body to effectively pass and implement the Proposed Agreement.

A. Components of the Proposed Agreement

The Proposed Agreement should contain the following components: (1) a clear definition of what constitutes a nation state's critical infrastructure;[142] (2) a requirement that each

---

139. *UN at Glance*, UNITED NATIONS, http://www.un.org/en/aboutun/index.shtml (last visited Jan. 21, 2013).

140. *Member States*, UNITED NATIONS, http://www.un.org/en/members/growth.shtml (last visited Jan. 21, 2013).

141. *See International Law*, UNITED NATIONS, http://www.un.org/en/law (last visited Jan. 21, 2013).

142. *See supra* text accompanying note 5. The United States of America Patriot Act of 2001 defines critical infrastructure as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e). Critical infrastructure thus includes: "agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications,

member state maintain a public list of existing critical infrastructure and give notice that such infrastructure is covered and protected under the Agreement;[143] (3) a confirmed attribution of a cyberattack that identifies the origin of the attack on protected critical infrastructure of a member state; (4) automatic legal authority to respond with a military action against the imputed member state from which the attack originated absent further attribution;[144] and (5) a requirement that the military response to the cyberattack meets the necessity and proportionality requirement under the self-defense principle pursuant to customary international law.[145]

Scholars argue that when the subject of a cyberattack is a nation's critical infrastructure, the targeted nation should possess a protected right to initiate a good-faith response to the attack.[146] Still, the Proposed Agreement's requirement of following the principles of existing customary international law will prevent possible overreaction to a cyberattack. [147] Necessity exists when "self-defense is actually required under the circumstances because a reasonable settlement could not be attained through peaceful means." [148] Proportionality requires "self-defense action to be limited to the amount of force necessary to defeat an ongoing attack or to deter future aggression."[149]

Imposing such a necessity requirement will restrain military response such that it remains the option of last resort. Although the Proposed Agreement may not specifically mention which type of cyberattack on critical infrastructure triggers a

---

energy, transportation, banking and finance, chemical industry and hazardous materials, and postal and shipping." *See* Condron, *supra* note 5, at 406–07 (citing Directive on Critical Infrastructure Identification, Prioritization, and Protection, 39 WEEKLY COMP. PRES. DOC. 1816 (Dec. 17, 2003)).

143. *See* Condron, *supra* note 5, at 416.

144. *See id*.

145. *See* Sklerov, *supra* note 3, at 28.

146. *See* Condron, *supra* note 5, at 415 ("To address the unique nature of cyber warfare, international law should provide a safe harbor for states who initiate a good-faith response to an attack."); *see also* Sklerov, *supra* note 3, at 58–59 ("[W]hen a threat is considered urgent, such as an attack against [critical national infrastructure], the potential severity and imminence of the attack may be great enough to outweigh all other considerations.").

147. *See* Condron, *supra* note 5, at 415–16; *see also* Sklerov, *supra* note 3, at 58.

148. Sklerov, *supra* note 3, at 32.

149. *Id.* at 32–33.

military response, the necessity requirement will limit the victim-member state to military action only when the damage to critical infrastructure is substantial. Article 41 of the U.N. Charter states that a "complete or partial interruption of economic relations and of rail, sea, postal, telegraphic, radio, and other means of communications" is not a measure constituting armed attack[150] and a cyberattack on critical infrastructure does not necessarily result in loss of lives or massive property damage.[151] Thus, responding with military action when a cyberattack does not result in substantial property damage or loss of lives would be unreasonable under the context of the attack,[152] and would violate the necessity principle.

If a cyberattack on a victim-member state's critical infrastructure results in loss of lives or massive property damage, then the military response must be proportional to the damage inflicted by the cyberattack. Since a nation's survival can very well depend on the wellness of its critical infrastructure, the nation may have to resort to "an immediate, robust, and aggressive response."[153] In addition, under the proportionality principle, the victim-member state can respond with force that will have a deterrent effect,[154] and responding with military action to a cyberattack resembling an armed attack would be proportional.[155] However, it would extend beyond the scope of the proportionality requirement for the victim-nation to engage in a full-on invasion when, for example, it suffered the destruction of a nuclear plant or a power outage that resulted in a train crash.[156]

---

150. U.N. Charter art. 41.

151. *See* Susan Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare"*, 97 J. CRIM. L. & CRIMINOLOGY 379, 391–97 (2007) (noting that a cyberattack can result in "mass interference" or "mass disruption" of a country's communications or other infrastructure).

152. *See* Sklerov, *supra* note 3, at 32.

153. *See* Condron, *supra* note 5, at 415.

154. *See* Sklerov, *supra* note 3, at 32–33.

155. *See* Shackelford, *supra* note 21, at 236–39.

156. *See* Sklerov, *supra* note 3, at 33.

B. Remediating Failures of Existing Treaties

1. Cyberattack on National Critical Infrastructure as a National Security Matter

A successful cyberattack on a nation's critical infrastructure can have a devastating effect,[157] and such an attack should be a matter of national security rather than treated merely as a criminal act. As evident in the Stuxnet attack on the Iranian uranium enrichment plant, certain cyberattacks on national critical infrastructure can inflict damage equivalent to physical damage.[158] Despite the gravity of such an attack, the United States and other countries have always treated cyberattacks as a criminal activity and not a national security matter.[159] The problem with treating a cyberattack as a criminal matter, especially when it targets a nation's critical infrastructure, is that doing so can result in a delayed response because investigation of a criminal act often requires a process of evidence gathering, which could take potentially up to several months.[160] Such delayed responses may result in lives lost, massive property damage,[161] or both.

---

157. *See* Condron, *supra* note 5, at 407 ("Critical infrastructure is by definition essential for the survival of the nation."); *see also supra* Part II.

158. *See* Brenner, *supra* note 151, at 390–91 (describing such a cyberattack as a "weapon of mass destruction").

159. *See* Condron, *supra* note 5, at 407; *see also* Convention on Cybercrime, *supra* note 20, pmbl. (The Convention treats cybercrime as a criminal matter.). The White House's Cybersecurity Proposal also seems to classify cyberattacks as criminal matter. *Cybersecurity Proposal*, *supra* note 17. *See* Schmitd, *supra* note 18 ("The Administration proposal advances the security of our increasingly "wired" critical infrastructure, strengthens the criminal penalties for hacking into the systems that control these vital resources, and clarifies the ability of companies and the government to voluntarily share information about cybersecurity threats and incidents in a privacy-protective manner.").

160. *See* Eric Talbot Jensen, *Computer Attacks on Computer National Infrastructure: A Use of Force Invoking the Right of Self Defense*, 38 STAN. J. INT'L L. 207, 232 (2002); *see also* Condron, *supra* note 5, at 407 ("Because law enforcement investigations that require the methodical collection of evidence are often protracted and resource-intensive, typically taking days, weeks, or even months, this presumption may result in a very slow response that may come too late to confront a cyber attack successfully.").

161. Condron, *supra* note 5, at 407.

However, due to the increasing danger of cyberattacks,[162] the U.S. government has already taken a position that a cyberattack can constitute an act of war, triggering a military response from the United States.[163] Colonel David Lapan, the Director of the Press Office at the Department of Defense, stated that "if we are attacked we reserve the right to do any number of things in response just like we do now with kinetic attack . . . . So it makes the idea that attacks in cyber would be viewed in a way that attacks in a kinetic form are now, the military option is always a resort."[164] The U.S. government's position on this point reflects its view, framed within debate on the interpretation of "armed attack" under the U.N. Charter and customary international law,[165] that a cyberattack can elevate to the status of an armed attack.[166]

Any country that relies heavily on networked computer systems to control the country's critical infrastructure must act

---

162. *See* Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J. (May 31, 2011), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html ("Recent attacks on the Pentagon's own systems—as well as the sabotaging of Iran's nuclear program via the Stuxnet computer worm—have given new urgency to U.S. efforts to develop a more formalized approach to cyber attacks.").

163. Larry Shaughnessy, *Pentagon Doesn't Rule out Military Force Against Cyberattacks*, CNN (May 31, 2011), http://articles.cnn.com/2011-05-31/us/military.cyberattack_1_cyberattacks-military-force-military-computers?_s=PM:US. Colonel David Lapan said that if a cyberattack is serious enough, "a response to a cyberincident or attack on the U.S. would not necessarily be a cyber response, so as I said all appropriate options would be on the table." *Id*. In May, 2011, the White House said "[w]e reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests." *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, WHITE HOUSE 14 (May 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter *International Strategy for Cyberspace*].

164. Shaughnessy, *supra* note 163.

165. *See supra* Part III.3

166. *See* Sklerov, *supra* note 3, at 57 (citing Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 913-15 (1999)) (Lieutenant Commander Sklerov cites and discusses Schmitt's explanation of six criteria for evaluating cyberattacks as armed attack: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy).

immediately to protect itself in the face of the continuous and ongoing danger of cyberattack, considering the ever-present danger of one on a nation's critical infrastructure. As noted above, the threat of Stuxnet virus is far from being over, and viruses that have the equal or more advanced capacity than Stuxnet have emerged in cyberspace.[167] For example, federal officials of the U.S. government are investigating a possible cyberattack that occurred in November 2011 that caused a shutdown of a public water pump in Illinois.[168] A dangerous cyberattack such as Stuxnet, or any redesigned form of Stuxnet, can strike anytime on any country's critical infrastructure network.

Unlike the Convention on Cybercrime, [169] the Proposed Agreement will treat a cyberattack on a nation's critical infrastructure as a national security matter, and not a criminal act.[170] Doing so can overcome the faults of treating it as a criminal matter, including, specifically, the potential for a delayed response by allowing for a response "nearly simultaneous with the attack itself."[171] The Proposed Agreement should accelerate the responding time to a cyberattack because it will not require a process of evidence gathering, and its attribution requirement is only to the level of a member state, not a machine or an individual attacker. Thus, the Proposed Agreement gives a member state authority to instantly take action once its critical infrastructure becomes the target of a cyberattack.

2. Criminal Law Enforcement and the Attribution Problem

Due to the attribution problem, a country planning to respond with military action will have difficulty trying to pinpoint the origin of a cyberattack; tracking down the country,

---

167. *See supra* Part II.

168. Mike M. Ahlers, *Feds Investigating Illinois 'Pump Failure' as Possible Cyber Attack*, CNN (Nov. 22, 2011), http://www.cnn.com/2011/11/18/us/cyber-attack-investigation/index.html?hpt=hp_t2 ("Such an attack would be noteworthy because, while cyber attacks on businesses are commonplace, attacks that penetrate industrial control systems and intentionally destroy equipment are virtually unknown in the United States.").

169. Convention on Cybercrime, *supra* note 20.

170. *See* Condron, *supra* note 5, at 419.

171. *Id.* at 407–08; *see also* Sklerov, *supra* note 3, at 58 (noting that some scholars believe that "it is too dangerous to waste time analyzing the attack when [critical national infrastructure] is at risk").

entity, or machine responsible.[172] However, the Proposed Agreement will not require the responding country to track down the source of the attack to the exact machine or person of origin. The Agreement has a narrow scope and it only applies to cyberattacks on critical infrastructure, meaning that the cyberattack must be capable of infiltrating complex systems and defensive mechanisms. Such sophisticated cyberattacks most likely require advanced technology and government resources not readily available to a single individual or non-government affiliated group,[173] which, for example, accounts for the widespread attribution of the Stuxnet virus to the U.S. and Israeli governments.[174] Other examples abound: experts believe that the Russian government was behind the cyberattack on Estonia, and that either China or North Korea was behind the cyberattack that targeted government websites in South Korea and the United States.[175] Thus, since cyberattacks in issue under the Proposed Agreement are likely to be launched by a government, the Agreement will require the responding state to only find out which country launched the attack, not which specific machine or person did so.

Nonetheless, the Proposed Agreement can seek to further mitigate the attribution problem and any related misattribution by incentivizing each member state to prevent and regulate cyberattack activity within its borders. Although this Note is skeptical of the efficacy of treating a cyberattack on critical infrastructure as a criminal act, that skepticism is confined to the problem of possible delayed police response. Properly enacted, the Proposed Agreement can incentivize member states to prevent cyberattacks domestically by engaging in heavy preventative measures and strict local law enforcement. On the one hand, rigorous and stringent criminal laws and law enforcement can have a deterring effect on cyberattack.[176] On the other hand, certainly, when "states fail to pass stringent crimi-

---

172. *See* Hollis, *supra* note 21, at 405–06.

173. *See* Gorman & Barnes, *supra* note 162 ("Pentagon officials believe the most-sophisticated computer attacks require the resources of a government. For instance, the weapons used in a major technological assault, such as taking down a power grid, would likely have been developed with state support, Pentagon officials say.").

174. *See Cyberattacks Against Iran*, *supra* note 50.

175. *See supra* Part I.A

176. *See* COLARIK, *supra* note 1, at 39.

nal laws or look the other way when attackers strike rival states, criminal laws are rendered impotent."[177] However, the Proposed Agreement can force member states to increase their effort to prevent and catch those who engage in cyberattacks because a cyberattack originating within its borders can trigger a military response from other member states. Each member state will thus be more cautious and thorough in their effort to regulate cyberattacks.

3. Why Join the Proposed Agreement?

The Proposed Agreement provides strong incentives for countries to join. It addresses increasingly dangerous threats of sophisticated cyberattacks on national critical infrastructure, which have the potential to cause loss of life and property damage.[178] It provides an instant and efficient legal route to address a national security threat by granting an authorization to respond with military action to a cyberattack.[179] Moreover, the Agreement minimizes the attribution problem by incentivizing each member state to practice more rigorous law enforcement, potentially resulting in an even greater degree of cyberattack prevention.[180]

Of course there will still be shortcomings to the Agreement. One major concern is that signing onto the Agreement will subject a member state to be the target of military force when a cyberattack is determined to come from within its borders. This will not likely be an appealing aspect of the Proposed Agreement and may possibly deter countries from joining it. Yet, there are several reasons why this concern should not play a large role in a nation's decision to join the Agreement. First, under the necessity and proportionality requirement pursuant to component (5) of the Proposed Agreement, the threshold to trigger military response is very high.[181] Recall that under this requirement, a cyberattack that does not cause loss of life or massive property damage would not initiate a kinetic military

177. *Sklerov*, *supra* note 3, at 9. "Unfortunately, several major states[, such as China and Russia,] refuse to take part in international efforts to eliminate cyberattack and seem unlikely to do so in the near future." *Id*.

178. *See* Shimeall, *supra* note 46, at 17.

179. *See infra* Part IV.B.1.

180. *See supra* Part IV.B.2.

181. *See supra* Part IV.A.

reaction.[182] Second, engaging in military action is not cheap,[183] and countries are not likely to resort to military action unless deemed necessary.[184]

Third, developed countries with significant military power will have a greater incentive to join the Agreement because a country that is more developed is likely to suffer more devastating impacts from a sophisticated cyberattack.[185] Some states are more dependent on computer networks, and a cyberattack to such states' critical infrastructure, compared to attacks on less developed countries' infrastructure, can have a larger and more disastrous impact.[186] Thus, member states will be more reluctant to launch a cyberattack against, and risk military response from, more developed countries.

Yet, at the same time, this does not mean that smaller, less developed countries are at a disadvantage by signing onto the Agreement.[187] Critical infrastructure of less developed countries is not likely to be the target of a sophisticated cyberattack. Since their infrastructure system does not rely heavily on cyber networks to function, the impact of a cyberattack on their criti-

---

182. For example, authorizing military air strikes to destroy banking facilities in response to a cyberattack that infiltrated banking facilities and destroyed some of the financial system infrastructure would not meet the necessity and proportionality requirement. *See* Waxman, *supra* note 8, at 428.

183. For example, a week of military intervention in Libya during March 2011 cost the United States $600 million. *See* Z. Byron Wolf, *Cost of Libya Intervention $600 Million for First Week, Pentagon Says*, ABC NEWS (Mar. 28, 2011, 6:50 PM), http://abcnews.go.com/blogs/politics/2011/03/cost-of-libya-intervention-600-million-for-first-week-pentagon-says ("One week after an international military coalition intervention in Libya**,** the cost to U.S. taxpayers has reached at least $600 million, according figures provided by the Pentagon . . . . And operation of the war craft, guzzling ever-expensive fuel to maintain their positions off the Libyan coast and in the skies above, could reach millions of dollars a week, experts say.").

184. *See* Shaughnessy, *supra* note 163. Colonel David Lapan stated that there is no clear threshold that would trigger a military action from the United States government in response to a cyberattack, but it would have to resemble a kinetic attack. *Id*.

185. *See* Waxman, *supra* note 8, at 455.

186. *See id.*; *see also International Strategy for Cyberspace*, *supra* note 163.

187. However, their involvement in the Agreement could prove to be irrelevant since the scope of the Proposed Agreement is very narrow and only deals with cyberattacks on critical infrastructure that could cause kinetic force-like damages.

cal infrastructure is less likely to have a devastating effect.[188] For example, a cyberattack on North Korea would not have much effect on its critical infrastructure because its networked system is very outdated compared to other developed countries such as the United States or South Korea.[189] Also, these less developed countries are not likely to have resources or funding to develop a cyberattack that is advanced and sophisticated enough to effectively infiltrate other countries' cyber defense system and cause massive damage to their infrastructure.[190] As a result, it is not probable that their actions in cyberspace will trigger military response under the Proposed Agreement and, thus, they stand to gain more than they risk by signing on.

CONCLUSION

As technology advances, countries will only increase their dependence on cyber networks to operate their national infrastructure. The national critical infrastructure will continue to be essential to governmental functions and to how people communicate, travel, obtain their necessities, and maintain their safety and health. Thus, a successful cyberattack on national critical infrastructure can cause an immense amount of damage, a threat that grows ever more dangerous due to increasing sophistication of cyberattacks. Therefore, it is critical that the international community respond promptly to meet the challenge of preventing such threats.

The Proposed Agreement provides an automatic authorization for injured member states to engage in military action in response to a cyberattack on their critical infrastructure. The Agreement remedies the flaws of the existing international treaty framework and international law by treating cyberattacks as a national security matter, by offering an immediate response to the danger of such an attack, and by minimizing the attribution problem. Furthermore, the Agreement's narrow

---

188. *See* Waxman, *supra* 8, at 455 (stating, "[Cyber] attacks could have a disproportionately large impact on countries or militaries that have a higher reliance on networked information systems.").

189. Peter Apps, *Analysis: Iran "Attack" Points to Rising Cyber Warfare Risk*, REUTERS (Sept. 24, 2010, 2:14 PM), http://www.reuters.com/article/2010/09/24/us-security-cyber-warfare-idUSTRE68N45Q20100924.

190. *See Cyberattacks Against Iran*, *supra* note 50; *see also* Flanagan, *supra* note 65.

scope will only govern cyberattacks on critical infrastructure that will cause loss of lives or massive property damage while its necessity and proportionality requirements will prevent overreaction to a cyberattack. The Proposed Agreement will offer incentives for countries to join so they can prevent cyberattacks from causing disastrous damage to their government infrastructure and to their citizens.

We have a tendency to wait too long—until it is too late. Technology advances and changes at an exponentially rapid speed. And with that, greater risks are posed to national critical infrastructure from dangerous cyberattacks. Countries around the world should act now and not wait until massive, key infrastructures are destroyed or, worse, lives are lost.

Gabriel K. Park[*]

---

[*] B.A., Wake Forest University (2008); J.D., Brooklyn Law School (expected 2013); Executive Articles Editor of the *Brooklyn Journal of International Law* (2012-2013). I would like to thank my family for their love and support, and my friends for their feedback and encouragement. I would also like to thank MAJ Sean Condron and MAJ Rob Barnsby for inspiring me to write this Note and helping me along the way. Finally, thanks to the *Journal* staff and editors for their hard work and assistance on this Note. I am very grateful. All errors and omissions are my own.