THE END OF THE WAR AS WE KNOW IT: HOW AN ACT OF CYBER WARFARE COULD IMPACT THE U.S. ENERGY GRID

Ashley M. Berger[*]

"I don't know [what weapons will be used in the Third World War]. But I can tell you what they'll use in the Fourth—rocks!"[1]

I. INTRODUCTION

War has been an ingrained part of human culture.[2] So much so, that conflicted societies have engaged in social and political struggles that

* J.D. Candidate, Suffolk University Law School, 2018. B.A. History and Legal Studies, University of Massachusetts Amherst, 2013.

1. Interview by Alfred Werner with Albert Einstein (Apr.–May 1949), in ALBERT EINSTEIN, THE ULTIMATE QUOTABLE EINSTEIN 165 (Alice Calaprice ed., 2011).

2. *See* Joshua J. Mark, *War*, THE ANCIENT HISTORY ENCYCLOPEDIA (Sept. 2, 2009), https://www.ancient.eu/war/ [https://perma.cc/Z7Z2-KR86] (discussing the roots of war lie in ancient civilizations).

lasted for centuries.[3] Historically, wars have been extreme acts of physical engagement.[4] Traditional warfare has always been fought on a battlefield, in the sky or in the sea.[5] For centuries, scholars, soldiers, politicians and civilians have viewed war as having a necessary physical aspect and the word "war" is widely defined to include armed conflict.[6]

The advent of the Internet created a new method by which to both develop a more efficient and interconnected society but also developed new means by which adversaries could engage in conflict with one another.[7] Numerous cyber-incidents and cybercrimes on the U.S. critical infrastructures have been reported, and the likelihood of cyber-incidents occurring against the infrastructure has been recognized.[8] If a cyber-attack were to actually penetrate the systems of, for instance, the fuel-supply line, the electric grid or hydropower providers, the results would be devastating to life in the United States.[9]

---

3. *See id*. (describing the notion that war is an age-old concept within society).

4. *See id*. (emphasizing war has been understood to include physical contact).

5. *See id*. (characterizing the physicality of traditional warfare and highlighting the physical components); *see also* Timothy Noah, *Birth of a Washington Word: When Warfare Gets "Kinetic*," SLATE (Nov. 20, 2002, 6:40 PM), http://www.slate.com/articles/news_and_politics/chatterbox/2002/11/birth_of_a_washington_word.html [https://perma.cc/WX58-2FA3] (defining kinetic warfare that has a devastatingly physical component to it. Kinetic warfare is "active, as opposed to latent. Kinetic warfare is the act of "dropping bombs and shooting people" to kill people as society perceives traditional warfare).

6. *See* OFFICE OF GEN. COUNSEL, DEP'T OF DEF., LAW OF WAR MANUAL 7 (June 12, 2015) [hereinafter LAW OF WAR MANUAL] (providing the definition of the law of war).

7. *See* DEP'T OF DEF., THE DOD CYBER STRATEGY, (Apr. 17, 2015), https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf[https://perma.cc/V285-E7W5] [hereinafter DoD Strategy] (discussing the history of the Internet and its positive uses as well as the vulnerabilities. The true invention of the Internet has roots in the year 1969, when scientists created a tool to share information amongst one another. While the Internet provides much value to our social and economic society, "this reliance leaves all of us—individuals, militaries, businesses, schools and governments—vulnerable in the face of a real and dangerous cyber threat"). *See also* JEFFREY CARR, INSIDE CYBER WARFARE xv-xvi (Mike Loukides ed., 2d ed. 2012) (explaining the successes and drawbacks of the Internet as a token of society).

8. *See What is Critical Infrastructure?*, DEP'T OF HOMELAND SECURITY (last updated July 12, 2017), https://www.dhs.gov/what-critical-infrastructure [https://perma.cc/E2HS-QFDG] (defining "critical infrastructure" and highlighting the variety of components it has. "There are 16 critical infrastructure sectors that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national public health or safety, or any combination thereof." Critical infrastructure refers to the essential services that provide water, power and natural resources, financial assets and other systems and networks that serve as the skeletal structure for American life).

9. *See* Kelley Beaucar Vlahos, *Special Report: The Cyberwar Threat from North Korea*, FOX NEWS (Feb. 14, 2014), http://www.foxnews.com/tech/2014/02/14/cyberwar-experts-question-north-korea-cyber-capabilities.html [https://perma.cc/SM3C-YU2R] (illuminating the potential for grave danger the U.S. citizen population could be in following a cyber-attack).

Thus far, none of the past reported cyber-incidents or crimes have yet to be considered an "act of war" by lawmakers under the traditional definition of an act of war.[10] Policy makers and scholars are acknowledging the more physically destructive a cyber incident's effects are, the more likely it will be treated as an armed attack.[11] A cyber-attack causing the same level of physical destruction as its physical counterpart has not yet occurred in the United States.[12] Though an attack meeting this threshold has not occurred, the protocols in place adequately provide for and encompass an appropriate response by the United States in the event a cyber-attack does occur.[13]

This Note will discuss and compare the history and definitions of traditional warfare and contrast potential acts of war through the lens of the cyber realm and describe examples of past attacks on both the United States and other governments.[14] It will continue on to examine incidents that have occurred on various components of the U.S. grid and also explore the most famous and first true cyber-attack, the Stuxnet worm.[15] Finally, this Note will analyze and apply the existing laws and traditional legal framework surrounding the use of force and armed attack thresholds to ultimately conclude that a Stuxnet-like attack should legally be considered a true cyber-attack of war.[16]

---

10. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL] (explaining generally what international law encompasses in terms of what constitutes an act of war).

11. *See* OFFICE OF THE GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 24 (Nov. 1999) http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf [https://perma.cc/Q2WH-9X4W] [hereinafter LEGAL ISSUES IN INFORMATION OPERATIONS] (analogizing cyber-attacks to traditional warfare and how their outcomes must present different conclusions. "Computer network attacks are likely to present implication that are quite different from the implications presented by attacks with traditional weapons").

12. *See* Danny Vinik, *America's Secret Arsenal*, POLITICO (Dec. 9, 2015, 4:57 AM), https://www.politico.com/agenda/story/2015/12/defense-department-cyber-offense-strategy-000331 [https://perma.cc/QV55-RKVL] (realizing the United States has yet to truly face this potential disaster. When a cyber-attack does occur though, the American public is going to expect an adequate response).

13. *See* LAW OF WAR MANUAL, *supra* note 6, at 997 (highlighting the likelihood that cyber operations will be subject to the law of war rules depending on the nature of the cyber incident); *see also* William Jackson, *How Can We Be at Cyberwar if We Don't Know What It Is?*, GCN (Mar. 22, 2010), https://gcn.com/articles/2010/03/22/cybereye-cyberwar-debate.aspx [https://perma.cc/ 88L4-V5XB] (realizing the gray areas of this situation).

14. *See infra* Part II.

15. *See infra* Part III.

16. *See infra* Part IV.

II. HISTORY

In recent years, the international community has emphasized the need for clarification on what a cyber-attack would have to look like in order for a response to comply with the framework set forth by the U.N. Charter and how to distinguish these types of activities from widely recognized activities of cybercrime.[17] Part of this new problem is defining what cyberspace is and how it fits into the existing legal framework governing peacetime and times of war.[18] Cyberspace is a hybrid of tangible assets but also "the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures."[19] This means that the information can be physically stored on a computer system or in transit in a telecommunications structure.[20] Cybercrime, therefore, refers to a crime committed in cyberspace.[21]

Increasingly, more of the world's civilian population has access to a computer, making it easy for any deviant to infiltrate the grid.[22] In terms of holding someone responsible for masterminding an act against another state, both individual actors and state actors have been treated and prosecuted as criminals for financial hacks and data theft.[23] However, the potential result of a cyber incident causing physical property damage or civilian death needs to be analyzed in a different framework.[24] For

17. *See* TALLINN MANUAL, *supra* note 10, at 3 (addressing the need for clarification on how and what parts of international law applies to activities in cyber space).

18. *See* Walter Gary Sharp, Sr., CYBERSPACE AND THE USE OF FORCE 15 (1999) (articulating what cyberspace consists of).

19. *See* Sharp, *supra* note 18, at 15 (defining cyberspace).

20. *See id.* (defining further what constitutes as cyberspace).

21. *See* TALLINN MANUAL, *supra* note 10, at 4 (distinguishing cybercrime as different from a cyber-attack).

22. *See Examining How to Combat Cyber Attacks by Improving Prevention and Prosecution: Before the Subcomm. on Tech., Terrorism and Gov't Info. of the Comm. on the Judiciary*, 106th Cong. 1–3 (2000) (statement of Hon. Jon Kyl, Chairman, Subcomm. on Tech., Terrorism and Gov't Info.) (acknowledging that quite literally anyone with computer access and willingness to learn how to hack could perform malicious activity in cyberspace).

23. *See* Jackson, *supra* note 13 (distinguishing potential cyber warfare from cybercrime). *See also* Catherine A. Theohary & John W. Rollins, CONG. RESEARCH SERV., R43955, CYBERWARFARE AND CYBERTERRORISM: IN BRIEF (2015) (providing an example of a common type of attack). In a distributed denial of service ("DDoS") attack, servers are overwhelmed with traffic, so access is denied or degraded). *See also* SYMANTEC CORPORATION, INTERNET SECURITY THREAT REPORT 5, 8 (2016) (providing examples of different types of cyber incidents that are considered cybercrime).

24. *See* LAW OF WAR MANUAL, *supra* note 6, at 997 (providing an example of when a cyber-attack should be considered an act of war); *see also* Jarno Limnell, *The Danger of Mixing Cyberespionage with Cyberwarfare*, WIRED (last visited Oct. 15, 2016), https://www.wired.com/insights/2013/07/the-danger-of-mixing-cyberespionage-with-cyberwarfare/ [https://perma.cc/XE2D-XU7E] (comparing the aspects of cyber warfare and cyber espionage that are inherently linked

example, if an actor releases a piece of malware into one of the critical infrastructure systems, such as the electric grid, this could cause massive power outages, spoiling food supplies and leaving people freezing.[25] This action looks different than financial theft, where the "destruction" is found solely in the realm of cyberspace, with minor physical incidental costs.[26] The analysis is on the effect, rather than the cause, of the action to determine if the cyber-attack meets the threshold of an armed attack.[27] It is clear traditional laws of war will apply to cyber operations but it is unclear in exactly what capacity they will apply.[28]

A. *Current Applicable Law*

As a member of the United Nations, the U.N. Charter mandates when and how the United States can respond to an armed attack.[29] Article 2 of the U.N Charter advises all members to refrain from using force against any other state, while Article 51 is explicit in that all states have an inherent right to self-defense.[30] The main purpose of the United Nations, and specifically the Security Council, is to maintain international peace and security.[31] Members of the United Nations are subject to sanctions if they fail to abide by the U.N. Charter or engage in some act that disrupts

---

but also inherently different. Cyber espionage, or cyber spying, may be viewed as preparation for warfare as an intelligence effort or may be used to justify pre-emptive or preventative actions); *See also* 6 U.S.C.S. § 1531 (2012) (characterizing an "international cyber criminal" and recommending types of consequences for that actor. An international cyber criminal is an actor who is "believed to have committed a cybercrime or intellectual property crime against the interests of the United States).

25. *See* Vlahos, *supra* note 9 (offering a grave thought as to what the wake of a cyber-attack may look like).

26. *See* OFFICE OF INTELLIGENCE AND ASSESSMENT, INTELLIGENT ASSESSMENT: DAMAGING CYBER ATTACKS POSSIBLE BUT NOT LIKELY AGAINST THE US ENERGY SECTOR 1 (2016) [hereinafter INTELLIGENCE ASSESSMENT] (acknowledging most of the activity directed at critical infrastructure is financially or ideologically motivated).

27. *See* Jackson, *supra* note 13 (stressing the need to explicitly determine what distinguishes a cybercrime from a potential act of cyber warfare); *see also* Vinik, *supra* note 12 (contrasting conventional war's well-understood weapons and strategies from the unknown aspects of cyber-attacks and its capabilities).

28. *See* LAW OF WAR MANUAL, *supra* note 6, at 998 (stressing that the traditional law of war applies to non-traditional methods. "[C]yber operations may not have a clear kinetic parallel in terms of their capabilities and the effects they create . . . operations may have implications that are quite different from those presented by attacks using traditional weapons, and those different implications may yield different conclusions"); *see also* TALLINN MANUAL, *supra* note 10, at 3 (explaining the challenges law makers are facing when determining how to apply international law to cyber operations).

29. U.N. Charter art. 2, ¶ 4, art. 51 (binding the United States to its promulgations).

30. *See id.* (outlining the rules set forth by the applicable U.N. Charter provisions).

31. U.N. Charter art. 39 (providing the scope of the U.N. Charter).

international peace.[32] While the United Nations act as a police power, it has been criticized that the sanctions imposed may not achieve the intended goal.[33] Critics argue that sanctions do not work because the eventual effect of the sanctions has a negative humanitarian impact.[34] Sanctions function as a more peaceful alternative to further acts of aggression to punish or deter the aggressor state, but are often criticized for not being implemented effectively in the aftermath of an act of aggression.[35]

Specific to the United States, the Law of War Manual provides guidelines on how the laws of war apply to physical armed conflict and how conflicts are assessed and treated in times of war and peace.[36] However, the Law of War Manual acknowledges that "how the law of war applies to cyber operations is not well-settled" and there will be developments in the application of existing law to operations in cyberspace.[37] Additionally, the Rules of Engagement are defined as "directives issued by competent military authority that delineate the circumstances and limitations under which U.S. forces will initiate and/or continue combat engagement with other forces."[38] U.S. military

32. *See id.* (explaining the specific resolutions within the U.N. Charter that determine whether an engagement rises to the level of a threat of aggression); U.N. Charter art. 41 (providing for economic sanctions and exploring when it is appropriate to impose them); U.N. Charter art. 42 (imposing military sanctions on non-abiding member states); *see also* Ian Hurd, *The U.N. Security Council and the International Rule of Law*, CHINESE J. INT'L POL. 3, 5 (2014) (furthering the stance of when and what sanctions can be imposed on non-abiding states).

33. Dana Shamlawi, *The United Nation Security Council's Continued Use of Economic Sanctions*, E-INT'L RELATIONS (Apr. 17, 2015), *archived at* https://perma.cc/R76N-X9Z6 (criticizing the use and implementation of economic sanctions as a method of compliance, subversion, deterrence and symbolism).

34. *See id.* (providing an example of a group that has felt the negative impacts of the U.N. sanctions. For example, the sanctions imposed on Iraqi civilians in the 1990 invasion of Kuwait fueled an already injustice felt by the Iraqi people).

35. *See id.* (highlighting the stipulations within the U.N. Charter promoting the sanctions); *see also* Robert A. Pape, *Why Economic Sanctions Do Not Work*, 22 J. INT'L SECURITY, Fall 1997, at 90, 92–93 (cautioning that sanctions are not the most effective way to "punish" non-abiding Member States).

36. *See* LAW OF WAR MANUAL, *supra* note 6, at 7 (defining the law of war as a term of art) ("The law of war is part of international law that regulates the resort to armed force; the conduct of hostilities and the protection of war victims in both international and non-international armed conflict . . . and the relationships between belligerent, neutral, and non-belligerent States. [T]he law of war has been used to inform the content of general authorizations to conduct military operations. Generally, the law of war is treated as prohibitive, in the sense that it seeks to forbid the use and resort to armed force when deemed necessary to do so).

37. *See id.* at 994 (acknowledging the existing uncertainties in the realm of how the existing law applies to cyber operations).

38. *See* U.S. Marine Corps, *Law of War/Introduction to Rules of Engagement*, B130936, STUDENT HANDBOOK, 13, 16 [hereinafter *Rules of Engagement*] (qualifying the rules governing conflicts of war. The objectives are rooted in the theory that "the object of war is nonetheless to ensure the submission of the enemy as quickly and efficiently as possible).

personnel are expected to abide by both the laws of war and the rules of engagement when engaged in conflict to defeat the enemy as efficiently as possible with the least amount of force necessary.[39]

Much of the U.S. infrastructure is privately owned and government regulated.[40] Since 2005, the Federal Energy Regulatory Commission (FERC) has been the regulatory agency responsible for overseeing the reliability of the bulk power system with the goal of putting the necessary infrastructure on the "smart grid."[41] The "smart grid" is the system that incorporates information technology into the day-to-day operations of the critical infrastructure industry.[42] FERC ensures the physical safety and functionality of the smart infrastructure, but FERC's authority is extremely limited to regulation of the cyber grid.[43] Under the Energy Policy Act of 2005, FERC has the conferred authority to institute compliance and safety standards, but not explicit power to defend its systems.[44] Where FERC has the regulatory authority to oversee the protection of its systems, there is a disconnect between having protection power and immediate decision-making power to launch a retaliatory attack.[45]

The Department of Defense has developed protocols to encompass its responsibilities in the time of an attack.[46] Most incidents in the cyber

---

39. *See id.* (defining and explaining the Rules of Engagement. The purpose of the ROE is to achieve national policy goals while abiding by general principles of law while engaged with the enemy).

40. *See* Gordan Corera, CYBERSPIES: THE SECRET HISTORY OF SURVEILLANCE, HACKING, AND DIGITAL ESPIONAGE 290 (2015) (describing how the infrastructure is owned. Because the infrastructure systems are normally held in private hands, it asks the question of whose responsibility it is to defend them. Industry owners are typically incapable or not willing to spend the money on proper security measures and the government is hesitant to get heavily involved. Another issue with the infrastructure is that it was built long ago and is both complex and interconnected, making it difficult for both owners and the government to figure out how and what is truly critical to defend and protect).

41. *See Cyber & Grid Security*, FEDERAL ENERGY REGULATORY COMMISSION (explaining the purpose of FERC and defining the "smart grid"). Since 2005, the electric industry has been shifting its systems, including hydropower, natural gas and oil, to operate on the smart grid. FERC is aware that while seeking to be reliable and efficient, it also needs to be mindful of potential vulnerabilities and potential losses of service).

42. *See id.* (defining the "smart grid" and introducing the idea of putting critical infrastructure on a massive information technology system).

43. *See id.* (describing what FERC is allowed to do within its scope of authority).

44. *See* Corera, *supra* note 40, at 290–91 (questioning what body has the authority to protect the necessary infrastructure even if it is owned).

45. *See Cyber & Grid Security*, *supra* note 41 (explaining the regulatory authority of FERC. Additionally, FERC certified the North American Electric Reliability Organization (NERC) as the nation's reliability organization which has developed the Critical Infrastructure Protection cyber security reliability standards).

46. *See* DoD Strategy, *supra* note 7, at 4–5 (outlining the three-part strategy for missions in cyberspace. This three-part plan was established to ensure the United States is both prepared

realm are easier to classify as an intelligence operation rather than a military objective. Thus it is unclear how the Department of Defense should, could and would respond in the wake of a cyber-attack.[47] It is clear that the Department of Defense has set forth new strategies detailing how cyber capabilities can be integrated into the existing framework.[48] While these various sources of law dictate what the United States can and cannot do in times of war and peace, there is not explicit language explaining how cyber-attacks fit within the laws of war, if they are considered either a use of force or an armed attack, potentially requiring a requisite retaliatory attack.[49] However, the Law of War Manual does provide a catchall sort of analogy—if a cyber-attack looks like a kinetic attack, the response will be that of a kinetic attack.[50]

B. *Distinguishing "Attacks" and "Armed Attacks"*

The definitions of "attack" and "armed attacks" differ depending on the context and application of the terms.[51] An "attack" is a particular type of military operation that is an act of "violence against the adversary,

---

for an incoming cyber-attack as well as prepared to respond, if necessary to one. The three primary objectives of the Department of Defense are: (1) to defend its own networks, systems, and information; (2) be prepared to defend the United States and its interests against cyber-attacks of significant consequence and (3) if directed by the President or the Secretary of Defense, to provide integrated cyber capabilities to support military operations and contingent plans).

47. *See* Vinik, *supra* note 12 (indicating that potential cyber offensives attacks would be categorized as an intelligence movement for ease and to avoid taking responsibility for such an operations); *see also* David E. Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. TIMES (Feb. 3, 2013), *archived at* https://perma.cc/EC3T-Q9AF (declaring that the President of the United States acting as the Commander-in-Chief should have the sole authority to unleash a cyber weapon); *see also* Exec. Order No. 13636, 78 Fed. Reg. 33, 11739 (Feb. 19, 2013) (acknowledging the U.S. cybersecurity problem and promulgating the development of the Cybersecurity Framework); *see also* Establishment of the Cyber Threat Intelligence Integration Center, 80 Fed. Reg. 41, 11317 (Mar. 3, 2015) (establishing the Cyber Threat Intelligence Integration Center to analyze and investigate threats and incidents relating to national interests).

48. *See* Vinik, *supra* note 12 (emphasizing some framework has been set by the Department of Defense in regards of what should be done in connection with a potential cyber-attack).

49. *See* TALLINN MANUAL, *supra* note 10, at 5 (explaining "there are no treaty provisions that directly deal with 'cyber warfare'); *see also* LAW OF WAR MANUAL, *supra* note 6, at 994 (asserting that international law does apply to cyber warfare. The Law of War Manual expressly states that international law does apply to cyber capabilities, but the challenge is determining what considerations decision makers should apply to existing international law).

50. *See* LAW OF WAR MANUAL, *supra* note 6, at 997 (treating potential cyber-attacks causing physical destruction like a traditional kinetic attack).

51. *See* Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283, 285 (2012) (describing the definition and threshold of the word "attack" depends on the context in which it is being used).

whether in offence or in defence."[52] This is the threshold definition in international law on the grounds that most prohibitions and restrictions apply only to acts that qualify as "attacks."[53]

It is necessary to distinguish what constitutes an "attack" from an "armed conflict."[54] An "armed conflict" differs from an "attack" in the sense that an armed conflict refers to an "action that gives States the right to a response rising to the level of a 'use of force.'"[55] An "armed attack" would trigger a state's right to use force in self-defense.[56] The principle of an "armed attack" derives its legal threshold in international law from the U.N. Charter, which provides "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."[57] This allows States the authority to proportionately respond to an act when non-forceful means would otherwise be inefficient.[58]

Every member of the United Nations has an inherent right to self-defense and "competent authority" to wage war for a public purpose.[59] Under this theory, force may only be used as self-defense necessary "to repel . . . the armed attack and to restore the security of the party

52. *See id.* (exploring the definition of "attack" under the Geneva Convention's standards. The word "attack" as applicable is a neutral term in the realm of war because "some attacks are lawful, whereas others are not, either because of the status of the object of the attack or how the attack is conducted).

53. *See id.* (highlighting the threshold component of the definition of an "attack").

54. *See id.* at 286 (distinguishing the differences between an attack and an armed conflict).

55. *See id.* at 285 (defining an armed conflict. Two potential instances would create an armed conflict, the first being an international conflict between States and the second being non-international conflicts where a "certain level of intensity and organization between a State and an organized armed group or between organized armed groups").

56. Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, JOINT FORCE Q. 40, 42 (Oct. 2012), *archived a*t https://perma.cc/Z2NX-67VZ (discussing when a state could invoke their right to use force as a method of self-defense).

57. U.N. Charter art. 51 (providing the guidelines for when an attack can be considered armed); *see also* LAW OF WAR MANUAL, *supra* note 6, at 39, 78 (distinguishing between jus ad bellum and jus in bello theories. *Jus ad bellum* refers to the "law concerning the resort to force" whereas *jus in bello* refers to the "law concerning conduct during war." *Jus ad bellum* theory has the potential to raise questions of national policy that would ultimately be decided by the Executive Branch, National Security Council and other relevant departments and agencies. *Jus in bello* laws can be understood as arising from a party intending to conduct hostilities and when parties are actually conducting hostilities).

58. *See* Priyanka R. Dev, *"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*," 50 TEXAS INT'L L.J. 379, 384 (2015) (synthesizing when an act meets the threshold of an armed attack).

59. *See* LAW OF WAR MANUAL, *supra* note 6, at 40 (acknowledging the power to wage war in a power of the State); *see also* U.N. Charter art. 2, para 4 (explaining when states should not resort to force. "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations").

attacked."[60] Where there is physical damage or harm inflicted on person or property, an attack will be considered an "armed attack."[61]

C. *Distinguishing the Threshold of "Use of Force"*

The "use of force" threshold is slightly different and is a slightly lower bar than that of an armed attack.[62] The applicable U.N. Charter provisions states "[a]ll members shall refrain … from the threat of use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[63] Though there is no black letter rule of what constitutes as "use of force," the principle encompasses "consequences of coercive activities" and "consequences that pose the greatest threat to international peace and security."[64] The "use of force" threshold is considerably lower than the "armed attack" threshold because the U.N. Charter allows a response to an armed attack that could be potentially more devastating than the initial attack.[65] The Law of War Manual recognizes "if cyber operations cause effects that, if caused by traditional physical means, would be regarded as a use of force . . . then such cyber operations would likely also be regarded as a use of force."[66]

---

60. *See* LAW OF WAR MANUAL, *supra* note 6, at 41 (asserting the specific instances where proportionate means of force may be used. "Assessing the proportionality of measures take in self-defense may involve considerations of whether an actual or imminent attack is part of an ongoing pattern of attacks or what force is reasonably necessary to discourage future armed attacks or threats thereof").

61. *See* Dev, *supra* note 58, at 387 (stating the necessary physical aspect of an attack to qualify the act as an armed attack).

62. *See* Foltz, *supra* note 56, at 41–42 (explaining that there is not a clear definition of what use of force means); *see also* Harold Hongju Koh, *International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference*, 54 HARV. J. INT'L L. 1, 4 (2012) (explaining that the law allows States to respond to a cyber-attack with the use of force. "There is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality").

63. *See* U.N. Charter art. 2, para. 4; *see also* Foltz, *supra* note 56, at 41–42 (describing the problems with the U.N. Charter. The U.N. Charter only applies to members of the United Nations and therefore, does not encompass the conduct of non-state actors).

64. *See* Foltz, *supra* note 56, at 42 (describing the threshold of use of force. "**[**T]he use of force threshold has traditionally been viewed as lying somewhere between purely economic and political coercion on the one hand and activities that result in physical damage or injury on the other").

65. *See* Dev, *supra* note 58, at 387 (distinguishing the differences between the threshold levels of "use of force" and "armed attack"); *see also* Schmitt, *supra* note 51, at 285 (highlighting that Article 51 is an exception to Article 2(4) of the Charter. "Article 51, recognized as reflective of customary international law by the vast majority of legal scholars, is an express exception to Article 2(4)").

66. *See* LAW OF WAR MANUAL, *supra* note 6, at 997–98 ("[I]f the physical consequences of a cyber-attack constitute the kind of physical damages that would be caused by dropping a

The "use of force" threshold is a strict instrument-based approach and it is unclear when it could be applied to cyber activities that might not cause physical harm.[67] The "use of force" threshold differs from that of an armed attack and the "use of force" definition is understood "to include a military attack of one state by the organized military of another state" and also applies to "all agencies and agents of a state government."[68] Scholars have suggested that the more a cyber operation resembles an armed attack, the more likely and willing States will be to classify it as a prohibited use of force.[69]

D. *Potential of a Cyber-Attack on Critical Energy Infrastructure*

Though a cyber-attack has not yet occurred on the U.S. critical infrastructure, the threat is existent.[70] In 2016, the Department of Homeland Security released a report highlighting the history of threats against the U.S. energy sector, which classified the cyber activity as "low-level cybercrime that is likely opportunistic in nature rather than specifically aimed at the sector . . . and is not meant to be destructive."[71] The report attributes the fear to the overuse of the term "cyber-attack" in

---

bomb or firing a missile, that cyber-attack would equally be subject to the same rules that apply to attacks using bombs or missiles") (citing Koh, *supra* note 62, at 3–4).

67. *See* Foltz, *supra* note 56, at 42 (citing an example of where cyber operations may not meet the "use of force" threshold. "According to a strict instrument-based interpretation, even highly disruptive peacetime cyber operations may not qualify as a use of force because they lack the traditional kinetic characteristics associated with armed force").

68. *See* Sharp, *supra* note 18, at 82–83 (defining a "use of force." This category applies to a plethora of potential actors "such as the organized military, militia, security forces, police forces, intelligence personnel, mercenaries, and other surrogate forces or volunteers").

69. *See* Foltz, *supra* note 56, at 42–43 (likening cyber operations to traditional warfare).

70. *See* Office of Intelligence & Assessment, *Intelligence Assessment: Damaging Cyber Attacks Possible but Not Likely Against the US Energy Sector*, DEP'T OF HOMELAND SECURITY 1–3 (Jan. 27, 2016) [hereinafter *Intelligence Assessment*] (evaluating the actuality of an imminent cyber threat. Homeland Security assesses a targeted attack against the U.S. energy sector as a crime of cyber espionage and data threat. The report indicates that the media reports and overuses the phrase "cyber-attack" to encompass all incidents of cybercrime, rather than referring to activities that would cause severe disruption and destruction); *see also* U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, para. 4, U.N. Doc. A/70/172 (July 22, 2015) (describing how the development and usage of information and communications technologies (ICTs) are emerging military threats); *see also* Vinik, *supra* note 12 (noting that the world is in a state similar to that of the Cold War. The problem with cyber incidents is that there is so much that is invisible to the public as a whole, but also to lawmakers and experts. The invisibility of the cyber realm is a major reason it is difficult to completely quantify the threat accurately).

71. *See Intelligence Assessment*, *supra* note 70, at 1 (explaining the recent history of cyber activity in the United States).

open source media to refer to even the lowest level cybercrimes.[72] But simply because the threat is assessed as low and "opportune in nature," is not an excuse to not address the problem.[73] However, the advanced nature of these attacks is becoming more precise and targeted at specific pieces of infrastructure, emphasizing the growing need for adequate security measures and responses to be put in place.[74]

For example, in 2015, Ukraine power companies experienced widespread power outages in their critical infrastructures impacting about 225,000 customers.[75] Hackers synchronized their attacks, staggering the attacks within thirty minutes of each other at each affected power company.[76] In this case, the actors used remote administration tools and "KillDisk" malware to erase files on the targeted systems to prevent restoration and leave the system inoperable.[77] It appears that all actors had legitimate credentials to initially access the companies' systems however there is also a likelihood that "BlackEnergy" malware was used to initially access the systems.[78]

Following a variety of U.S. government sponsored teams, including the U.S. Computer Emergency Readiness Team (U.S.-CERT), the Department of Energy, the Federal Bureau of Investigation and the North American Electric Reliability Corporation traveled to Ukraine to assess the damage.[79] While this attack did not occur on U.S. soil, the occurrence demonstrated the possibility of an attack on the U.S. systems and the U.S. acknowledgment demonstrates a seriousness to determine appropriate response measures.[80]

---

72. *See id.* at 5 (qualifying the past incidents as low-level threats).

73. *See id.* at 2 (suggesting ways that owners of energy sector assets can better protect their systems).

74. IDAHO NAT'L LAB, CYBER THREAT AND VULNERABILITY ANALYSIS OF THE U.S. ELECTRIC SECTOR 2 (2016) (cautioning the developing sophistication of potential threats).

75. *See* ICS-CERT, DEP'T OF HOMELAND SECURITY, *Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure* (Feb. 25, 2016), *archived at* https://perma.cc/MFF9-MAGT (introducing the "Black Energy" attack on the Ukrainian power systems).

76. *Id.* (explaining how the attack was carried out).

77. *Id.* (describing the malware utilized to successfully execute the attack).

78. *Id.* (recognizing the various potential access points the actors had to execute the attack).

79. *Id.* (identifying the American response teams who assessed the damage overseas. The other group was the National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)).

80. *Id.* (discussing the reasons multiple U.S. teams traveled to Ukraine. The purpose of the trip from so many U.S. government agencies was to share information to prevent future cyber-attacks).

III. PREMISE

A. *The Dam*

In 2011, Iran-based hackers were able to remotely access the computer system that controlled a small dam in New York.[81] Though the dam was offline at the time, the hackers had access to the water temperature and ability to operate the sluice gate.[82] While the New York dam is exponentially smaller than the likes of the Hoover Dam, this attack demonstrated the abilities of hackers to target and infiltrate a piece of infrastructure on American soil.[83] This attack represented the very real ability of a group of hackers who were able to access the control systems of a dam, and the possibility and likelihood of success that other hackers will be able to infiltrate other pieces of vital infrastructure in the future.[84] The N.Y. Attorney General indicted the Iranian group for conspiracy to commit and aid and abet computer hacking and the individual defendant, Hamid Firoozi, who was specifically responsible for accessing the dam's controls was also charged with obtaining unauthorized access into the Supervisory Control and Data Acquisition systems of the dam.[85]

---

81. Joseph Berger, *A Dam, Small and Unsung is Caught Up in an Iranian Hacking Case*, N.Y. TIMES, Mar. 25, 2016, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0 (introducing an attack specifically targeted at U.S. infrastructure); *see also* Eric Larson et al., *Iranians Hacked From Wall Street to New York Dam, U.S. Says*, BLOOMBERG TECH. (Mar. 24, 2016), *archived at* https://perma.cc/5QUV-8DZE (outlining the Iranian groups mission and accomplishments); *see also* Max Kutner, *Alleged Dam Hacking Raises Fears of Cyber Threats to Infrastructure*, NEWSWEEK, Mar. 30, 2016, *http://www.newsweek.com/cyber-attack-rye-dam-iran-441940* (comparing the attack to Alfred Hitchcock's movie *Saboteur*. The plot of Hitchcock's classic was a conspiracy to blow up the Hoover Dam. This attack shows that the potential for hackers to actually blow it up and that it is not just a fiction only possible in a movie).

82. *See* Larson et al., *supra* note 81 (discussing that the actuality of the effects was not destructive but illustrating what could have happened. At the time of the attack, the gate was offline for scheduled maintenance).

83. Berger, *supra* note 81 (stressing the gravity of the attack even though the dam was a small one and acknowledging the potential damage would have been minimal in comparison to an attack on a much larger dam).

84. *See* Kutner, *supra* note 81 (opining on what kind of damage can potentially be done); *see also* Mark Thompson, *Iranian Cyber Attack on New York Dam Shows Future of War*, TIME (Mar. 24, 2016), *archived at* https://perma.cc/J4LP-85PP (illustrating how this attack shows what the future of warfare will look like).

85. OFFICE OF PUB. AFFAIRS, DEP'T OF JUSTICE, SEVEN IRANIANS WORKING FOR ISLAMIC REVOLUTIONARY GUARD CORPS-AFFILIATED ENTITIES CHARGED FOR CONDUCTING COORDINATED CAMPAIGN OF CYBER ATTACKS AGAINST U.S. FINANCIAL SECTOR (Mar. 24, 2016), *archived at* https://perma.cc/BQ23-CHMP [hereinafter DEP'T OF JUSTICE] (listing the charges for the charged individuals).

B. *Past Cyber Incidents*

In 1997, a Massachusetts teenager hacked into a Bell Atlantic computer system that managed flight control for the Worcester Regional Airport and his success of hacking into the system disrupted power to the control tower for nearly six hours.[86] In 1998, two California teenagers successfully disrupted troop deployments to the Persian Gulf.[87] The teenagers were influenced by a Middle Eastern hacker and the attack was coordinated with such skill, that it was initially believed to have been the work of Iraq.[88] The Massachusetts attack became the first time a juvenile was charged with a Federal computer crime; recognizing the criminality of the action in cyberspace.[89] In 2001, Chinese hackers infiltrated American domains, using early forms of "worms" to cause the systems to react in what became known as the "World Wide Web War."[90]

C. *The Stuxnet Worm*

There are various ways that an attack that could be detrimental to the U.S. grid and at the forefront of that discussion is the Stuxnet worm.[91] The Stuxnet worm has been labeled the most complex malware ever and has also earned the name of the world's "first real cyberweapon."[92] In

---

86. 146 CONG. REC. 28, 974–75 (2000) (explaining the potential danger this incident presented).

87. *Id.* at H974 (describing the gravity of this particular attack).

88. *Id.* (discussing the confusion and difficulty of initially identifying the hacker); *see also* Serge Schmemann, *As Iraqi Tension Eases, Arabs Criticize U.S. Role*, N.Y. TIMES (Feb. 27, 1998), http://www.nytimes.com/1998/02/27/world/as-iraqi-tension-eases-arabs-criticize-us-role.html (explaining the deep tensions between the United States and the countries in the Gulf in the late 1990s).

89. Carey Goldberg, *Federal Charges for Juvenile in a Case of Computer Crime*, N.Y. TIMES (Mar. 19, 1998), http://www.nytimes.com/1998/03/19/us/federal-charges-for-juvenile-in-a-case-of-computer-crime.html (explaining the circumstances of the charged crime and the general concern of government officials at the time regarding cyber-attacks).

90. Craig S. Smith, May 6–12; *The First World Hacker War*, N.Y. TIMES (May 13, 2001), http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html (terming the engagement the "World Wide Web War I"); *see also* Paul Kerr et al., CONG. RESEARCH SERV., R41524, THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY 1 (Dec. 9, 2010) (highlighting the powerful effect of 'worms' as a malicious software).

91. Foltz, *supra* note 56, at 41 (explaining the Stuxnet as the "watershed event" in the framework of what constitutes as use of force as a cyber-attack); *see also* Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED (July 11, 2011), https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ (describing why Stuxnet is such a threat).

92. Zetter, *supra* note 91 (distinguishing the Stuxnet worm from other forms of malware); *see also* Kerr et al., *supra* note 910 (differentiating between Stuxnet and its predecessors); Corera, *supra* note 40, at 278 (quoting former NSA and CIA director, Michael Hayden).

2009, the virus was released into Iran's nuclear program, destroying nearly one fifth of Iran's nuclear centrifuges and hindering the Iranian nuclear program, at least by a few years.[93] The reason why the Stuxnet virus is so dangerous is because of its "method of infection" in that the malware was "self-replicating and designed to infect systems that were not connected to the Internet."[94] It is estimated that Stuxnet was specifically directed at solely targeting the Iranian centrifuges and caused severe physical damage to as many as 1000 centrifuges.[95] The Stuxnet attack on a piece of Iran's critical infrastructure is an example of a cyber weapon causing physical damage, that some argue constituted a use of force.[96] So where does Stuxnet leave United States in law making and policy around cyber-attacks and should a Stuxnet-like attack on a piece of the U.S. critical infrastructure be categorized and codified as a "use of force?"

D. *Current Legislation*

The United States is working on legislation aimed at creating a more effective strategy for how the country would handle a cyber-attack and evaluating the unknowns about cyber capabilities and vulnerabilities.[97] Policy makers know what a traditional act of terrorism would look like; on the other hand, the scope of damage caused by a cyber-attack is unknown and unclear if and how the resulting damage would be similar to a traditional attack of war.[98] The unknown factor of the potential attack

93. *See* Zetter, *supra* note 91 (categorizing the type of damage done by the Stuxnet virus to Iran's nuclear program); *see also* Corera, *supra* note 40, at 273 (describing the process to enrich uranium and the moments after the attack).

94. *See* Foltz, *supra* note 56, at 44 (emphasizing the devastating and unique capabilities of Stuxnet).

95. *Id.* (highlighting the severity of the Stuxnet attack).

96. *Id.* (reiterating the severity and uniqueness of the Stuxnet attack); *see also* Henry Kenyon, *What Would a Stuxnet-type Attack in the US Look Like?*, GCN (Sept. 7, 2011), https://gcn.com/articles/2011/09/07/ds-summit-stuxnet-lessons-learned.aspx (describing the repercussions of an Stuxnet attack on the United States and contrasting it to that of the attack in Iran).

97. *See Intelligence Assessment*, *supra* note 70, at 4 (providing examples of potential mitigation strategies); *see also* Brent Kesler, *The Vulnerability of Nuclear Facilities to Cyber Attack*, NPS STRATEGIC INSIGHTS 15 (2011) (explaining that the discussion surrounding cyber security policy has been speculative); Vinik, *supra* note 12 (defining cyber weapons and comparing cyber weapons to "capabilities").

98. Press Release, Jim Himes, Members of Cybersecurity Subcommittee Call for Cyberwarfare Rules (Nov. 5, 2015), Cybersecurity Subcommittee Call for Cyberwarfare Rules (Nov. 5, 2015) (on file with the author) (explaining the unclear standards currently in place that would ward against a cyber-attack); *see also* 161 CONG. REC. 179, 9255 (2015) (extending the scope of the Homeland Security Act relating to providing assistance to state and local governments in regards to cyber security); Cyber Preparedness Act of 2016, H.R. Res. 5459, 114th Cong. (2016) ("An Act to amend the Homeland Security Act of 2002 to enhance preparedness

is why open source media describes a bleak picture of what life could be like following a cyber-attack.[99]

The effects of a potential cyber-attack could look like a traditional, kinetic destruction but the appropriate response is not codified, as the initial "attack" would not be launched utilizing physical force.[100] Sponsor of House Resolution 5220, known as the Cyber Act of War Act of 2016, Jim Himes explained:

> What if Iran melted down one server at Florida Power and Light? They do $5,000 worth of damage. That sounds to me like a crime," Himes said. "But what if they melt down a whole bunch of servers, a network goes down and a bunch of people die? That feels to me like an act of war. But these lines aren't drawn. Because they're not drawn, is our response to have the FBI investigate and file a diplomatic démarche? Or is our response to do a cyber reprisal? Or is our response to do a kinetic reprisal? We don't know. I think that's a real problem.[101]

Congressman Himes bill aims to have the Department of Defense

---

and response capabilities for cyberattacks, bolster the dissemination of homeland security information related to cyber threats, and for other purposes"); 146 CONG. REC. 28, *supra* note 86, at H974 (recognizing a potential cyber threat has been discussed in the legislature for nearly two decades).

99. *See* Bill Buchanan, *This is What Cyber Warfare Between Nations Would Look Like*, NEWSWEEK (Aug. 8, 2016), http://www.newsweek.com/cyber-warfare-between-countries-look-488267 [https://perma.cc/L3JM-86P2] (depicting what the actual scene would look like if there was to be a successful attack on the energy infrastructure); *see also* Kesler, *supra* note 97, at 18 (describing a hacker's success in getting in an Australia water control system thereby releasing raw sewage into parks, rivers, and hotels); *see also* Tara Dodrill, *Napolitano Warns Downed Power Grid Is Inevitable Due to Cyber Attack*, OFF THE GRID NEWS (last visited Nov. 25, 2016), http://www.offthegridnews.com/grid-threats/napolitano-warns-downed-power-grid-is-inevitable-due-to-cyber-attack/ [https://perma.cc/XZD4-33NT] (recounting former Department of Homeland Security Janet Napolitano's fears and views on what needs to be done to strengthen the energy grid. "While we have built systems, protections and a framework to identify attacks and intrusions, share information with the private sector and across government, and develop plans and capabilities to mitigate the damage, more must be done, and quickly"); *see also* Bill Hoffman & Jason Devaney, *Ex-Defense Chief, U.S. Vulnerable to Terror Attack on Power Grid*, NEWSMAX (June 29, 2015), http://www.newsmax.com/Newsfront/William-Cohen-defense-chief-terrorist-attack-power-grid/2015/06/29/id/652742/ [https://perma.cc/DR7Z-9BUG] (illustrating former Secretary of Defense William Cohen and former CIA analyst Peter Vincent Pry's stance on the notion that the U.S. energy grid is a "sitting duck" for an attack).

100. *See* Vinik, *supra* note 12 (addressing a cyber-attack's results might look like those of traditional drawn warfare, but the uncertainty and unknown response methods are detrimental).

101. *See* Himes, *supra* note 98 (emphasizing the need for a change in the laws to combat a changing landscape for terrorism. The goal of Congressman Himes' bill is to make people aware that the United States has the capability to protect itself and should use that capability accordingly).

amend the laws of war to create a clear plan of determining when an act in cyberspace meets the threshold of "use of force" and establish clear protocols when and if the United States was the receptor of a large scale attack.[102]

It is necessary that the government and military have a prepared response available if a cyber-attack were to occur on U.S. soil.[103] Since much of the U.S. infrastructure is privately owned, there is an inherent disconnect of communication between those who own and control our infrastructure and the government entities who would handle potential retaliation.[104]

IV. ANALYSIS

Cyber warfare is a military problem and cybercrime is an issue for law enforcement but activities classified as cybercrimes are likely the precursor to potential acts of cyber warfare.[105] The physical result of a cyber action is what would qualify a particular act as an act requiring responsive force; most activities that are currently perceived as a cyber-attack only merely amount to a cybercrime.[106] Data breaches and distributed denial of service "attacks" are both recognized as criminal activity and while intrusive and debilitating, neither of those examples

102. *See id.* (explaining what Congressman Himes hopes to achieve with his new bill. Included in Congressman Himes bill is a provision that would require the President to develop a policy from determining when an action in cyberspace constitutes as force against the United States and revise the Law of War Manual. Additionally, the bill asks the President to consider "the ways in which the effects of a cyber-attack may be equivalent to the effects of an attack using conventional weapons, including with respect to physical destruction or casualties" as well as examine the intangible effects of such an attack).

103. *See Intelligence Assessment*, *supra* note 70, at 2 (reiterating that government agencies have claimed the threat is low of a cyber-attack on the energy infrastructure); *but see* Vinik, *supra* note 12 (emphasizing the need for an implementation of guidelines and protocols in the time of a cyber emergency).

104. *See* Kenyon, *supra* note 96 (explaining that U.S. infrastructure is controlled by private firms. In order for an adequate response, there needs to be some sort of communication between the private firms and the government to create an appropriate prior response).

105. *See* CARR, *supra* note 7, at 5 (explaining the differences in repercussions of cybercrime versus cyber warfare. Though cybercrime may not initially be a threshold problem to be examined under the laws of war, cybercrime is the laboratory or playground for cyber warfare techniques to be developed. "Cyber Terror is often Cyber Warfare utilizing Cyber Crime").

106. *See Intelligence Assessment*, *supra* note 70, at 2 (assessing the incorrect uses of "cyber-attack" in reporting that has led to a societal misconception about cyber threats); *see also* Limnell, *supra* note 24 (stressing the importance of correctly labeling and distinguishing terms of a cyber-attack and an act of cyber warfare).

cause true physical damage to persons or property.[107]

Cybercrime is more common than attacks that meet the threshold of cyber warfare.[108] It is unlikely that entire wars will be fought online in the immediate future, but cyber operations should be viewed as the fifth dimension of warfare because there will likely not be a war fought without cyber technology.[109]

A *Cyber-Attack as a Use of Force*

A qualifier of an armed attack is the physicality of the attack.[110] As previously mentioned, there have been reported incidents of individuals using the Internet to disable power to the Worcester Regional Airport and of individuals disrupting troop deployments.[111] These two examples resulted in no known individual injuries or real damage to property, but demonstrated a potential for hackers to get into U.S. systems.[112] Though the U.N. Charter provides every State with an inherent right to self-defense, not every incident that resembles an attack warrants the usage of this power.[113] As the Charter provides, a State may respond with proportional force "reasonably necessary to promptly secure the permissible objectives of self-defense."[114] One of the main goals of the use of force threshold is to not cause unnecessary collateral destruction

---

107. *See* SYMANTEC CORPORATION, *supra* note 23, at 10 (discussing in 2010, there were 318 data breaches, 9 of which exposed 10 million identities. Smart phones are a major source of targets because of the amount of personal data that is stored on an individual's phone).

108. *See Intelligence Assessment*, *supra* note 70, at 1 (discussing the media frequently mislabels cybercrime as cyber-attacks).

109. *See* Limnell, *supra* note 24 (asserting that cyber capabilities are a weapon and the fifth dimension of warfare); *see* 146 CONG. REC. 28, *supra* note 86, at 974 (characterizing cyber conflict as different from traditional war because of its invisible components. "Unlike the growth of a large super-power army, unlike the proliferation of arms from a hostile nation state, we cannot readily or easily see the development of the cyber threat." Speaker Robert Andrews identified a cyber conflict is "unlike any threat that we have faced in the history of our republic . . . the silent but deadly threat of cyberterrorism" and "the quiet but lethal assault on our country's systems and people"); *see also* CARR, *supra* note 7, at 45–46 (acknowledging the difficulty in catching perpetrators when they are committing a cyber-attack).

110. *See* Dev, *supra* note 58, at 387 (highlighting the necessary physical component of an armed attack).

111. *See* 146 CONG. REC. H974, *supra* note 86 (detailing the 1997 incident that disabled power to the Worcester, Massachusetts airport. Though power was disrupted for a few hours, no one was injured as a result of the loss of power); *see also id.* at H974–75 (describing the 1998 troop disruption. Again, no injuries were reported as a result of the interception of communications).

112. *See id.* at H974 (detailing the results of the 1997 incident at the Worcester airport).

113. *See* Sharp, *supra* note 18, at 38 (highlighting when a use of force response is appropriate. A use of force as a means of self-defense is justified for many uses of force and especially at the time an armed attack occurs).

114. *See id.* (explaining when and how a Nation can use force as self-defense).

or injury to civilian humans.[115] Because the actors in those two incidents were groups of civilians with bad motives but sophisticated abilities and the amount of damage that they actually caused was minimal, the proper retaliation for their actions would not be using an responsive use of force.[116] Additionally, the U.N. Charter suggests that the use of force must reach a certain 'gravity,' following from the principle of proportionality.[117] Therefore, "minor frontier incidents are not per se uses of force that rise to the Article 2(4) threshold."[118]

However, these types of incidents differ drastically and should be categorized much differently than a potential attack similar to the Stuxnet attack.[119] Because the Stuxnet attack actually and physically crippled vital infrastructure in Iran, it follows that another attack of the same gravity would likely cripple its target to some degree.[120] What causes a Stuxnet-like attack to be treated differently than a cybercrime, is the potential effects that the cyber-attack to cause physical damage, like a bomb or a missile could.[121] This damage demonstrated the physical capacity of a cyber capability, this attack shows what type of effects a

115. *See id.* at 39 (discussing when a self-defense use of force would be inappropriate).

116. *See id.* at 37–38 (noting that international law prohibits purely retaliatory or punitive actions); *but see* Koh, *supra* note 62, at 4 (providing examples of when incidents would likely constitute an appropriate use of force. Among these examples is "operations that disable air traffic control resulting in airplane crashes"); *see* Sharp, *supra* note 18, at 37–38 (noting that international law prohibits purely retaliatory or punitive actions); *see also* 146 CONG. REC. 28, *supra* note 86, at 974–75 (explaining because neither of these attacks resulted in a calculable amount of damage or destruction, a self-defense response would have been inappropriate. Had the backup generators malfunctioned, this type of hacking attack, also could have potentially been considered an act of war); *but see* Koh, *supra* note 62, at 4 (providing examples of when incidents would likely constitute an appropriate use of force. Among these examples are "operations that disable air traffic control resulting in airplane crashes).

117. *See* Sharp, *supra* note 18, at 47 (illustrating when a use of force reaches a certain level of 'gravity').

118. *See id.* (citing that "the minor nature of an attack is prima facie evidence of absence of intention to attack, of honest mistake, or simply the limited objectives of an attack." This would mean that the attack is not grave enough to warrant an aggressive response of using force).

119. *See* 146 CONG. REC. H974, *supra* note 86, at H974–75 (detailing the previous low level cyber threats and attacks on the United States).

120. *See* Kenyon, *supra* note 96 (emphasizing the potential disaster a Stuxnet-like attack would have on the U.S. infrastructure. One of the reasons that Iran was able to combat the attack in such a quick and efficient manner was because the infrastructure is government owned. In the United States, much of the vital infrastructure is privately owned, raising issues on how quickly a response would occur, if such a response needed to occur); *see contra* Corera, *supra* note 40, at 277 (likening the characteristics of Stuxnet to traditional intelligence operations rather than an act of war. Because of how precise the virus was to Iran's centrifuges, it had to be specially designed to ensure the success).

121. *See* Vinik, *supra* note 12 (distinguishing cyber capabilities from traditional weaponry but alluding to the idea that the repercussions from a cyber capability could be similar to a traditional kinetic weapon).

cyber incident can produce.[122] In Iran, the nuclear plant was government owned property, while in the United States most of the infrastructure is privately owned.[123] It is understood that while civilian property may not be the object of the attack, states may use force during conflict against civilian property that supports "warfighting capability" during a conflict.[124]

B. *A Cyber-Attack as an Armed Attack*

Different considerations and qualifications constitute and distinguish an armed attack from just a use of force, and thus, the analysis must be slightly different.[125] An armed attack requires physical damage either to people or property, and a cyber-attack can produce those results as seen by the Stuxnet attack.[126] Examples of such armed attacks, as provided by the Law of War Manual liken cyber-attacks to traditional, physical attacks using the following example, "[A] bomb might break a dam and flood a civilian population, but insertion of a line of malicious code from a distant computer might just as easily achieve that same result."[127] While the hacker at the New York dam was criminally charged, this forces the analysis of whether this attack should have been considered an act of war.[128]

While this is a type of attack that the United States appears to recognize as one that is comparable to one that would warrant a use of force response, likely the proportionality of this attack on a small dam in

122. *See* LAW OF WAR MANUAL, *supra* note 6, at 998 (comparing results of cyber actions to the results of traditional warfare).

123. *See* Kenyon, *supra* note 96 (highlighting the differences between the Iran attack and the potential attack on the United States).

124. *See* Sharp, *supra* note 18, at 41 (explaining when State's may use force against civilian property. "States may use force during armed conflict, for example, against economic targets such as . . . enemy lines of communication . . . and power generation plants." Because civilian infrastructure is used for military purposes, it is subject to lawful attack during armed conflict. It is recognized that technology and the increasing dependence on the Internet exacerbates this issue and makes civilian infrastructure more vulnerable)*; see also* Vinik, *supra* note 12 (questioning how other similar rules may apply in the context of a cyber-attack. For example, in traditional warfare, hospitals are off limits to attacks so then perhaps cutting off electricity to a hospital is also an illegal act of warfare); Sharp, *supra* note 18, at 41.

125. *See* Dev, *supra* note 58, at 385 (citing to the Nicaragua judgment "measures which do not constitute an armed attack but may nevertheless involve a use of force").

126. *See id.* (recognizing the necessary physical component to an armed attack).

127. *See* LAW OF WAR MANUAL, *supra* note 6, at 998 (emphasizing the similar effect that a cyber-attack would have to have on physical structures or persons to warrant a similar legal and military response).

128. *See* DEP'T OF JUSTICE, *supra* note 85 (articulating the criminal charges against the Iranian hackers).

New York would not warrant a responsive armed attack.[129] While the scale of this particular incident was not enough to warrant a responsive use of armed force, this is likely the type of incident that, on a larger scale, would require a response of an armed attack.[130] However, had the hackers successfully gained control of a piece of infrastructure such as the Hoover Dam, the results likely would have been much graver—causing destruction to civilians and civilian property.[131] The fact that the hackers were able to gain access at all to the control systems of the dam, regardless of its size, demonstrates a potential vulnerability and opportunity for other hacker groups to take advantage of by manipulating the systems that control the U.S. infrastructure.[132]

Additionally, the Stuxnet worm was launched during a time of peace, which forces the considerations of proportional responses.[133] The alleged purpose of Stuxnet was to hinder Iran from having the ability to create an atomic bomb and to avoid "collateral damage" by releasing the virus into the networks controlling the centrifuges.[134] However, with this abnormal attack, it seems that the repercussions could be greater than anyone predicted and encourage other nations to create their own type of malware to destroy U.S. infrastructure.[135]

---

129. *See* Kutner, *supra* note 81 (explaining the physical appearance of the New York dam. The dam in Rye Brook, New York is fairly small and is used to prevent local homes basements from flooding. The dam is about 15 feet wide and two and a half feet tall. If the floodgate was open during the time of a storm, it would have caused flooding to surrounding areas. In 2007, when the dam flooded, a report suggested the damage cost nearly $80 million).

130. *See* Dev, *supra* note 58, at 387 (reemphasizing the necessity of resulting physical damage to qualify as an armed attack); *see also* Koh, *supra* note 62, at 4 (highlighting specific examples of when cyber activity would be categorized as a use of force. Examples of specific actions that would be considered a use of force include operations that: trigger a nuclear plant meltdown, open a dam above a populated area, and disrupt air traffic).

131. *See* Kutner, *supra* note 81 (speculating the potential damage to a more crucial piece of American infrastructure. Where the Rye Brook, New York dam stood just 15 feet wide and two and a half feet tall, the Hoover Dam is a concrete mammoth rising 726 feet high and 1244 wide).

132. *See id.* (recognizing the potential implications for other pieces of United States. "Cybersecurity experts say if the Iranians were able to access it control system, they could also likely get inside systems for more significant infrastructure, such as pipelines, mass transit systems and power grids").

133. *See* Corera, *supra* note 40, at 278 (describing the factors surrounding the launch of Stuxnet. While Stuxnet sent the signal that a cyber weapon was able to be made, essentially now the "cat is out of the bag." This means that presumably other nations will be racing to create a similar type of tool).

134. *See id.* at 276–77 (illuminating the purpose of what Stuxnet was designed to do. For example, unlike the atomic bomb, Stuxnet was supposed to be a stealthier than an overt use of force to achieve its objective).

135. *See id.* at 278–79 (predicting potential responses to Stuxnet. Former NSA and CIA director Michael Hayden alludes the release of Stuxnet to the atomic bomb. "The use of the weapon by the US is almost certain to act as a spur for others to try to develop the same capability

C. *Proportionality of a Cyber-Attack*

The United States is bound by the rules of proportionality, and before launching a responsive attack, it must consider the potential effects on military and civilian infrastructure, potential physical damage and the potential effects on civilians that are not military objectives.[136] Though the 1997 Worcester airport disruption and the more recent 2013 attack on the dam in New York are examples of the types of incidents that would likely be considered as types of attacks that could elicit an armed attack, likely in these two instances the projected gravity of damage incurred would not be considered enough to logically warrant a responsive use of force.[137] In both instances, the perpetrators were charged criminally instead of the U.S. military getting involved to launch a counter attack, demonstrating that the two incidents likely did not necessarily need a full scale military offensive to stop them from committing another offensive act against the United States.[138] In these cases, the proportionality of an armed attack likely would have been more devastating than a criminal charge.[139]

Both the disruption of air traffic and the hacking of the dam's control system are examples of incidents that have been considered armed cyber-attacks, yet neither were treated as such.[140] Both were treated as crimes with the only repercussions being potential jail time because the physical destruction was not grave enough to warrant a response of a retaliatory

---

as fast as they can. And Western countries may be most vulnerable to weapons like Stuxnet because they are most connected").

136. *See* Koh, *supra* note 62, at 5 (providing factors that must be considered when determining proportionality).

137. *See* 146 CONG. REC. 28, *supra* note 86, at 974–75 (explaining the consequences for the perpetrator in the 1997 attack); *see also* Kutner, *supra* note 81 (detailing the issues with the New York dam); *see also* Koh, *supra* note 62, at 4–5 (emphasizing the strict considerations a State needs to imagine before launching a proportionate counter attack with force).

138. *See* Koh, *supra* note 62, at 4 (applying when the use of force may or may not be the appropriate response. "The principles of necessity and proportionality limit uses of force in self-defense and would regulate what may constitute a lawful response under the circumstances).

139. *See id.* (acknowledging when a responsive attack may not be appropriate. "There is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality"); *see also* DEP'T OF JUSTICE, *supra* note 85 (discussing the monetary amount of damage. Though the remediation for the New York Dam was assessed at over $30,000, that amount was not significant enough to warrant a massive launch against a small group of Iranian hackers); *see also* Corera, *supra* note 40, at 285 (contrasting the effects of cybercrime to physical destruction. "Few would argue that taking down some websites justified a fighter jet dropping a bomb, although many scholars, including some in NATO, say the Stuxnet attack would").

140. *See* LAW OF WAR MANUAL, *supra* note 6, at 998 (stating examples of considerable cyber-attacks that mirror traditional physical attacks. The Law of War Manual expressly states that cyber operations that would cause the opening of a dam or a disablement of air traffic control services would be "regarded as a use of force under jus ad bellum").

attack.[141] Had the cyber-attack on the New York Dam been aimed at a larger scale target, such as the Hoover Dam, or if the air traffic control disruption occurred at a larger airport, sources of international law give authority to respond with a proportionate act of self-defense as well as being scrutinized under the same legal standard as traditional, kinetic attacks.[142]

In the current state of technology, releasing a bit of code is never going to be the same as physically dropping a bomb on a target and currently, more lethal, traditional weapons still outnumber and outweigh the effects of a potential cyber-attack.[143] The immediate severity of a cyber-attack would not necessarily put soldiers at risk and does not involve the movement of artillery or physical objects.[144] With so much critical infrastructure of the United States being connected, cyber warfare is a new route of warfare, but it does not yet replace traditional warfare, and other actions in cyberspace may be hard to distinguish from actual attacks of warfare.[145] A cyber-attack might be a part of warfare in the future, but an entirely cyber war is unlikely to replace traditional warfare, and it is necessary to evaluate and determine the current holes in the systems that are in place now in order to install effective security measures so that they are less susceptible to an attack.[146] Because it is accepted by the U.S. Law of War Manual that international law applies in cyber space, and since the United States abides by the U.N. Charter, it should follow that it would be lawful to launch a proportionate cyber-attack on a nation who launched one on U.S. infrastructure.[147]

---

141. *See* Sharp, *supra* note 18, at 47 (reiterating a State's right to use self-defense and that an armed attack is not always justified. A State always has an inherent right to self-defense, however, it may not always be appropriate to respond with an act that falls short of an armed attack).

142. *See* LAW OF WAR MANUAL, *supra* note 6, at 998 (reinforcing the types of cyber-attacks that would mirror traditional acts of war. Where cyber-attacks that would cause the same level of destruction as a traditional physical attack, they should be categorized similarly, therefore warranting analysis under the same legal standard); *see also* Himes, *supra* note 98 (emphasizing the need for clarification and codification on the proper legal response if a large scale cyber-attack occurs. In Congressman Himes' call for proper legislation articulating what the proper legal response would be for the types of cyber-attacks that have already occurred in the United States on a larger scale).

143. *See* Corera, *supra* note 40, at 292 (comparing traditional warfare with potential acts of cyber warfare).

144. *See* Vinik, *supra* note 12 (declaring that cyber warfare in a way causes less damage because there is not as much threat to human life).

145. *See* Corera, *supra* note 40, at 292 (highlighting the problems with defining what constitutes cyber warfare).

146. *See id.* (illuminating the unlikely possibility in the foreseeable future that a war be solely comprised of cyber capabilities).

147. *See* LAW OF WAR MANUAL, *supra* note 6, at 994 (reiterating that "long-standing international norms guiding state behavior—in times of peace and in times of conflict—also apply in cyber space").

V. CONCLUSION

Applying the traditional principles set forth by the U.N. Charter and other governing laws, a cyber-attack that causes physical destruction to civilians or property will likely be construed as an attack of war, allowing the United States to respond with proportionate force in the name of self-defense. The United States has already been the target of attacks that could be regarded as a lawful military engagement rising to a responsive use of force, however, most incidents simply are heightened cyber espionage actions. The U.S. energy grid is a target. Even though a cyber-attack has yet to occur, the definitions and provisions of the Law of War Manual, combined with the promulgations set forth by the U.N. Charter, encompass and incorporate a cyber-attack to fit into the pre-existing legal frameworks of both domestic and international law.