NOTE

HACK AND BE HACKED: A FRAMEWORK FOR THE UNITED STATES TO RESPOND TO NON-STATE ACTORS IN CYBERSPACE

I. INTRODUCTION

Computer networks are constantly bombarded by malicious attacks. In 2014, Symantec, a premier cybersecurity service, reportedly blocked 496,657 web attackers per day and encountered over 317 million new variants of malware that infect computers.[1] In 2015, McAfee, another cybersecurity service, encountered over 1.2 million new variants of malware that infect mobile devices, raising the grand total of malware variants our devices are susceptible to to 8.5 million variants.[2] These numbers, reported by only two services, reflect an infinitesimally small portion of malicious activities. Without question, the number of web attacks, mobile attacks, and variants of malware worldwide is incalculable, largely for two reasons. First, investigating attacks in cyberspace is not like investigating an attack in the physical world, and while industry experts work furiously to develop better forensic tools, the fact of the matter remains that most malicious cyber activities go unnoticed. Second, if or when the activity is detected, there remains the costly and time-consuming problem of figuring out who did it and how to prevent that activity in the future.

Cyber-based threats are as varied in nature, scale, and scope as the actors that perpetrate them.[3] To name a few, the U.S. Department of Defense (DoD) has been the victim of an ongoing cyber espionage campaign directed by the People's Republic of China since 2002.[4] In 2007, Russian operatives launched a series of distributed denial-of-

---

1. "Malicious software," often referred to as "malware," refers to information designed to cause damage or disruption to a computer or computer system. *Malware,* TECHTERMS.COM, http://techterms.com/definition/malware (last visited Feb. 26, 2016). 20 SYMANTEC, INTERNET SECURITY THREAT REPORT 11, 17 (2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

2. INTEL SECURITY, MCAFEE LAB THREATS REPORT, 31 (2015), http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-aug-2015.pdf.

3. Allison Gual, *Neutrality in the Digital Battle Space: Applications of the Principle of Neutrality in Information Warfare*, 29 SYRACUSE SCI. & TECH. L. REP. 51, 53 (2013); Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 MELB. J. OF INT'L L. 1, 6 (2013).

4. JEFFREY CARR, INSIDE CYBER WARFARE 4 (Mike Loukides ed., 2d. ed. 2012).

service attacks (DDoS)[5] against websites of Estonian Government agencies, political parties, media companies, and financial firms.[6] From 2013 to 2015, a syndicate of cybercriminals repeatedly hacked over 100 banks around the world, including banks in Britain, stealing over £650 million what was one of the largest cybercriminal schemes in history.[7] Finally, in late July and early August of 2015, Islamic State of Iraq and Syria (ISIS) hackers posted the personal identifying information of some 1,300 military and government employees on "jihadi forums" and social media sites.[8] Each posting included a message urging ISIS supporters to attack the soldiers whose information was listed.[9] This spectrum of malicious cyber activity illustrates the varied legal challenges cyber attacks pose to the United States and governments worldwide.[10] Moreover, it illustrates how both state-sponsored and non-state actors use the Internet to perpetrate wrongful cyber-acts.

---

5. A distributed denial-of-service attack uses many computers to attack a single target. The computers are hijacked by a single operator or group of operators who command them to attack the target. This causes the single target to be shut down, "thereby denying service to the system to legitimate users." Margaret Rouse, *Distributed Denial-of-Service (DDoS)*, TECHTARGET.COM, http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack (last visited Feb. 26, 2016).

6. Margulies, *supra* note 3, at 6-7.

7. Martin Evans, *Hackers Steal £650 Million in World's Biggest Bank Raid*, THETELEGRAPH.CO.UK (Feb 15, 2015, 4:09 PM), http://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html.

8. Steven Stalinsky & R. Sosnow, *Hacking in the Name of the Islamic State ISIS*, MEMRI JIHAD AND TERRORISM THREAT MONITOR, MEMRIJTTM.ORG (Aug. 21, 2015), http://www.memrijttm.org/hacking-in-the-name-of-the-islamic-state-isis.html; *US Airstrike Killed Top ISIL Hacker - CENTCOM*, GLOBALSECURITY.ORG, (Aug. 28, 2015, 11:26 PM), http://www.globalsecurity.org/military/library/news/2015/08/mil-150828-sputnik03.htm [hereinafter *US Airstrike*].

9. Stalinsky & Sosnow, *supra* note 8.

10. *See generally* Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 546 (2012) (In cyberspace private non-state actors "present a complicated issue for targeted states."); *Foreign Policy - Cybersecurity*, WHITEHOUSE.GOV, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity (last visited Apr. 8, 2016).

This Note will focus on the cyber activities of non-state actors and the relevant law that can be synthesized into a threat-response framework for United States law enforcement and military. "Non-state actor" is used in this article to denote "an individual or organization that has significant political influence but is not allied to any particular country or state."[11] A clear example is ISIS, an organization that has significant political influence in the Middle East.[12] However, ISIS is not a governmental organization of a state recognized by the international community, despite calling themselves the "Islamic State of Iraq and Syria."[13]

International non-state actors present an interesting legal question for the U.S. Government because, as it stands, the United States is largely limited in responding to these issues through the domestic criminal system. For example, the Federal Bureau of Investigation's Cyber's Most Wanted list includes individuals like Firas Dardar, a hacker for the Syrian Electronic Army, and Evgeniy Mikhailovich Bogachev, a Russian national who has run notorious financial schemes.[14] However, these malicious attacks can be launched remotely from anywhere in the world, and domestic prosecution is not always an option for international perpetrators. This leaves many cyber criminals, terrorists, and spies to their devices, costing the global economy an estimated $455 billion annually.[15]

---

11. *Non-state actor*, OXFORDDICTIONARIES.COM, http://www.oxforddictionaries.com/us/definition/english/non-state-actor (last visited May 29, 2016).

12. *See* Ben Smith, *ISIS and the sectarian conflict in the middle east*, Research Paper 15.16 HOUSE OF COMMONS LIBRARY 14-15 (Mar. 19, 2015), http://www.parliament.uk/briefing-papers/rp15-16.pdf.

13. *See generally id.* at 7-10.

14. THE FEDERAL BUREAU OF INVESTIGATION, *Cyber's Most Wanted*, https://www.fbi.gov/wanted/cyber (last visited Apr. 8, 2016); *See also* Laurie R. Blank, *International Law and Cyber Treats from Non-State Actors* 89 INT'L L. STUD. 406, 407 (2013) (domestic criminal law and national security law are the most relevant legal regimes governing cyber activity).

15. Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and Espionage Costs $455 Billion Annually*, THEWASHINGTONPOST.COM (June 9, 2014), https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html.

Despite the United States' inability to prosecute international hackers, "hacking-back" remains a controversial solution.[16] "Hacking-back" includes a broad range of offensive cyber tactics to attack attackers.[17] For example, security professionals can set up a range of automatic or manually initiate responses, called active defenses, when they experience an attack.[18] These active defenses can be thought of as "electronic countermeasures designed to strike attacking computer systems and shut down cyber attacks midstream."[19] Alternatively, security professionals can attach a "beacon" to sensitive data.[20] That way, if the information were stolen, the beacon would be stolen with it, making it easier for the owner to find the stolen data in cyberspace.[21] Finally, if circumstances justify targeting a foreign government's cyber infrastructure, a DDoS attack could be used to temporarily disable the computer networks in the state.

Given the controversial nature of hacking-back, and concerns for escalation, it is essential that there be clear parameters for the action. Thus, creating a clear framework to determine how to respond to the range of bad cyber-acts that exist is critical. Clear legal guidelines are essential to set the limits of government action and to empower victims of cyber attacks to vindicate their rights. Most importantly, a threat-response framework must be developed to punish and deter malicious activity because, should it go unaddressed, it will continue

---

16. *See generally* CARR, *supra* note 4, at 194-96 (discussing baiting techniques and active defenses that may be used against attacks on certain sectors of cyberspace); Craig Timberg, et al., *Cyberattacks trigger talk of 'hacking back'*, THEWASHINGTONPOST.COM (Oct. 9, 2014), https://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html (discussing how "going on the offensive" is being discussed in cybersecurity circles); Eduard Kovacs, *Hacking Back: Industry Reactions to Offensive Security Research*, SECURITYWEEK.COM (Nov. 13, 2015), http://www.securityweek.com/hacking-back-industry-reactions-offensive-security-research (discussing the controversy between cybersecurity experts with regard to active defenses).

17. *See generally* CARR, *supra* note 4, at 194-96; Timberg et al., *supra* note 16.

18. CARR, *supra* note 4, at 46 n.2.

19. *Id.*

20. Timberg et al., *supra* note 16.

21. *Id.*

to cost the global economy billions, jeopardize our national security, and invade the most intimate aspects of our private lives.

This Note seeks to provide such a framework. Part II will discuss areas where cyberspace complicates traditional legal schemes. Part III will break down the spectrum of cyber-based threats into four broad categories—crime, espionage, warfare, and terrorism—and discuss the law applicable to each. Particular attention will be given to warfare and terrorism as these laws are relevant to the example the framework will be applied to in Part V. Part IV will lay out the threat-response framework, combining the discrete laws discussed in Part III. Finally, in Part V, the framework will be applied to the case of an ISIS hacker to provide an example of how the framework would apply to cyber terrorism.

II. THE UNIQUE ATTRIBUTES OF CYBERSPACE

Part of the difficulty in developing a clear legal framework stems from the novel character of cyberspace as compared with the physical world. The architecture of cyberspace is multi-dimensional like the physical world, but unlike physical structures which are relatively permanent, data structures within cyberspace can be easily altered within minutes.[22] Cyberspace's novelty is evidenced by one commentator's struggle to define it, settling on cyberspace as "a malleable realm of transitory data structures in which [real time] is measured in nanoseconds and spatially exists somehow both globally and invisibly."[23] In sum, efforts to investigate and reverse-engineer an attack to identify the attacker are frustrated by sophisticated actors' ability to alter data and easily hide their tracks. Indeed, there is the well-recognized issue of the difficulty of determining the identity of an attacker.[24] The real-world equivalent would be something like a

---

22. *See* Jack M. Beard, *Article: Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under Int'l Humanitarian Law*, 47 VAND. J. TRANSNAT'L L. 67, 106-07 (2014).

23. SCOTT BUKATMAN, TERMINAL IDENTITY: THE VIRTUAL SUBJECT IN POSTMODERN SCIENCE FICTION 18 (1993)

24. *See* Dimitar Kostadinov, *The Attribution Problem in Cyber Attacks*, INFOSECINSTITUTE.COM (Feb. 1, 2013), http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/.

super-criminal with the power to open walls as if they were doors and to shape-shift, taking on the identity of another when desired. Such an individual might, understandably, evade law enforcement's efforts.

Another aspect of cyberspace that thwarts responses is that the infrastructure that composes cyberspace is largely privately owned.[25] Therefore, governments lack the same kind of control over information and evidence that they have over physical territory, objects, and persons in the real world.[26] In addition, cyberspace defies territorial boundaries, challenging principles underlying domestic governance and international responsibility.[27] For example, jurisdiction over persons and property is largely based on their relationship to a physical location.[28]

To understand these problems and some of their plausible solutions, it is helpful to start at the beginning.

---

25. *See* Beard, *supra* note 22, at 87.

26. *See e.g.*, Robert Chesney and Steve Valdeck, *A Coherent Middle Ground in the Apple-FBI All Writs Act Dispute?*, LAWFAREBLOG.ORG (Mar. 21, 2016) https://www.lawfareblog.com/coherent-middle-ground-apple-fbi-all-writs-act-dispute (discussing the FBI's legal struggle to compel Apple to comply with a search warrant to access the phone of a terrorist with ties to ISIS who executed a deadly attack in San Bernardino on December 2, 2015).

27. *See* Beard, *supra* note 22, at 87.

28. *See Jurisdiction, Preliminary, and Procedural Concerns*, in BENCHBOOK ON INTERNATIONAL LAW § II.A.1 (Diane Marie Amann ed., 2014), www.asil.org/benchbook/jurisdiction.pdf (indicating the following five bases of jurisdiction: (1) "territoriality" which focuses on conduct taking place within a country's sovereign territory; (2) "nationality" which provides jurisdiction over the activities of a country's nationals; (3) "passive personality" which provides jurisdiction over conduct that victimizes a country's nationals; (4) "protective principle" which focuses on activities against a country's vital interests; and (5) "universality" which provides jurisdiction over *erga omens*, or conduct recognized by all nations as a criminal.) Thus, with the exception of universal, jurisdiction is inextricably linked to territory in that it is based on an act that occurred in a country's territory; by one of its nationals [who is often a national by virtue of being born or residing within a country's territory]; or, by harm to a country's territory or nationals. *See id.*

A. A Brief History of the Internet

In 1967, the DoD built the first network called the Advanced Research Projects Agency Network (ARPANET).[29] APRANET began as a small closed-network comprised of only four nodes.[30] At first ARPANET expanded slowly into a patchwork of local, regional, or private networks.[31] In 1974, Bob Kahn and Vint Cerf introduced a technology that standardized how users could send information across networks.[32] This allowed the existing isolated networks to connect. [33] Once networks connected, ARPANET grew exponentially.[34] By 1996, the "World Wide Web" was born, bringing with it a handful of cybersecurity problems.[35] Today, nearly three billion people are connected to the Internet, and nearly all are vulnerable to cyber attacks.[36]

---

29. SCOTT J. SHACKELFOLD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 20-21 (2014).

30. *See generally* SHACKELFOLD, *supra* note 29, at 21. A closed network is a network that does not connect with other networks, but rather only allows recognized participants to connect. *See* Ken Stanick, *Open vs Closed Networks – What is the difference?*, B2BNETWORKSTRATEGY.COM (Apr. 19, 2013), http://b2bnetworkstrategy.com/2013/04/19/open-vs-closed-networks-what-is-the-difference/. "Any system or device connected to a network is also called a node. For example, if a network connects a file server, five computers, and two printers, there are eight nodes on the network." *Node*, TECHTERMS.com, http://techterms.com/definition/node (last visited May 29, 2016).

31. SHACKELFOLD, *supra* note 29, at 21.

32. *Internet History 1962 to 1992,* COMPUTERHISTORY.ORG, http://www.computerhistory.org/internethistory/1970s/ (last visited Feb. 27, 2015) (explaining that this uniform technology was called Transmission Control Protocol and the Internet Protocol (TCP/IP)) [hereinafter *Internet History*].

33. SHACKELFOLD, *supra* note 29, at 21.

34. *See generally Internet History, supra* note 32.

35. *See generally* Craig Timberg, *Net of Insecurity—A Flaw in the Design*, THEWASHINGTONPOST.COM (May 30, 2015), http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

36. Salvador Rodriguez, *60% of World's Population Still Won't Have Internet by the End of 2014*, LATIMES.COM (May 7, 2014 10:30 AM), http://www.latimes.com/business/technology/la-fi-tn-60-world-population-3-billion-internet-2014-20140507-story.html.

Each time the technology behind the Internet advanced and networks expanded, threats to cybersecurity increased.[37] Kahn and Cerf's technology proved to be inherently insecure.[38] For example, when users send information, it can travel through any node in the world to its destination.[39] Once it arrives, there is no way to be sure who sent it, whether someone else modified it, or whether anyone spied on it en route.[40] This insecurity enables a range of malicious activity, from spying to masking a cybercriminal's identity.[41] Moreover, just as information is sent, malicious code, or malware, can also be sent—with little chance of verifying the sender or detecting it en route.[42]

As the software used to program computers advanced, so too did malware.[43] As early as 1982, an early version of a "logic bomb"[44] caused a Soviet gas pipeline in Serbia to explode.[45] In 1988, the "Morris Worm" crashed thousands of machines and cost millions in damage.[46] In 2010, a highly sophisticated malware called "Stuxnet" caused irreversible damage to centrifuges at Iranian nuclear facilities.[47] Today, one of the most common tools of cybercriminals, known as a "Botnet," allows a single hacker to commandeer millions of computers and carry out cyber attacks through the commandeered

---

37. Gervais, *supra* note 10, at 530.

38. *See* Timberg, *supra* note 35.

39. SHACKELFOLD, *supra* note 29, at 118.

40. *Id.*

41. *See generally id.* at 119.

42. *See* Timberg, *supra* note 35.

43. Gervais, *supra* note 10, at 530.

44. "A logic bomb is a malicious program timed to cause harm at a certain point in time, but is inactive up until that point. A set trigger, such as a preprogrammed date and time, activates a logic bomb. Once activated, a logic bomb implements a malicious code that causes harm to a computer . . . A logic bomb is also known as slag code." TECHOPEDIA.COM, https://www.techopedia.com/definition/4010/logic-bomb (last visited Feb. 27, 2016).

45. Beard, *supra* note 22, at 79.

46. Timberg, *supra* note 35.

47. Reese Nguyen, Comment, *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1099 (2013).

computers.[48] Ultimately, we are left with a cyberspace made insecure by aspirations to facilitate the most efficient exchange of information possible and a spectrum of actors exploiting those insecurities.

B. Problems with Controlling Cyberspace and the Actors Within it

One of the most challenging aspects of responding to similar malicious attacks is that, potentially, millions of users share the same networks at any given time. Public and private; civilian and military; and the United States and its adversaries all share the same Internet.[49] The communal nature of cyberspace limits possible responses because some reactions will necessarily interfere with the rights of innocent parties. This is especially true with Botnets.[50] Where innocent users' computers are hijacked to carry out attacks, any response would affect those computers in an effort to dismantle the Botnet.[51] Thus, particularly for a hack-back response to a cyber-based threat to be lawful, it must consider how that response will affect innocent parties.

Because many different people and entities use and own the Internet, the U.S. Government lacks control, let alone a presence in most of cyberspace. [52] The government's lack of authority is potentially catastrophic because principles underlying domestic governance and international responsibility are centered on a government's ability to exercises sovereign control over its territory.[53] Territorial sovereignty carries with it certain privileges and obligations.[54] It empowers countries to prosecute internal threats and

---

48. Beard, *supra* note 22, at 76-77.

49. Gervais, *supra* note 10, at 530.

50. *E.g.,* Sam Zeitlin, Note, *Botnet Takedowns and the Fourth Amendment*, 90 N.Y.U.L. REV. 746, 748 (2015) (discussing law enforcement efforts to shut down a Botnet as a violation of users' fourth amendment rights).

51. *See* Beard, *supra* note 22, at 76-77.

52. *Id.* at 87.

53. *See* CLETE D. JOHNSON, PANELIST, CYBERSECURITY AND NATIONAL DEFENSE: BUILDING A PUBLIC-PRIVATE PARTNERSHIP, OCCASIONAL PAPERS 15 (Laura Tate Kagel ed., Spring 2015).

54. Wolff Heintschel von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, 4th International Conference on Cyber Conflict 7-19, 8 (C. Cozosseck, et al. eds., 2012), http://insct.syr.edu/wp-content/uploads/2015/06/Heinegg_Sovereignty_In_Cyberspace.pdf.

protect against foreign invaders.[55] It obligates a country to ensure actors within its territory do not commit acts that unlawfully interfere with a foreign country.[56]

There has been much debate over how the concept of territorial sovereignty should translate to cyberspace.[57] Even if cyberspace traverses territorial boundaries and is not itself physical, cyberspace still requires physical equipment in order to exist.[58] This physical architecture is composed of human users, cables, servers, computers, and other equipment.[59] Collectively, this is referred to as "cyberinfrastructure."[60] It is over cyberinfrastructure that governments attempt to assert their sovereign control.[61] Indeed, the *Tallinn Manual on the Law Applicable to Cyber Warfare* (*Tallinn Manual*) and other sources of international law seem to support this theory.[62]

Under this theory, the same privileges that allow governments to prosecute internal threats and protect their territory from foreign invaders, similarly permit the government to protect its cyberinfrastructure. Governments exercise their right to prosecute

---

55. JOHNSON, *supra* note 53, at 15; Heinegg, *supra* note 54, at 8.

56. Heinegg, *supra* note 54, at 8-9.

57. *See generally* Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV 1 (2009); Margulies, *supra* note 3, at 1; Susan W. Brenner, *Cyber-threats and the Limits of Bureaucratic Control*, 14 MINN. J.L. SCI. & TECH. 137 (2013).

58. Franzese, *supra* note 57, at 17.

59. NATIONAL SCIENCE FOUNDATION ADVISORY COMMITTEE FOR CYBERINFRASTRUCTURE TASK FORCE ON CAMPUS BRIDGING, FINAL REPORT 3 (Mar. 2011), http://www.nsf.gov/cise/aci/taskforces/TaskForceReport_CampusBridging.pdf ("Cyberinfrastructure consists of computational systems, data and information management, advanced instruments, visualization environments, and people, all linked together by software and advanced networks").

60. *See* NATIONAL SCIENCE FOUNDATION, http://www.nsf.gov/news/special_reports/cyber/ (last visited Nov. 25, 2015).

61. Heinegg, *supra* note 54, at 10.

62. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE Rule 2, para. 2 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN].

cybercriminals who use or interfere with their cyberinfrastructure.[63] Governments have also asserted the right to protect their cyberinfrastructure against any interference by individuals in foreign countries.[64]

However, following this logic, the obligations attached to territorial sovereignty also apply to infrastructure. Thus, a state that exercises territorial sovereignty over its cyberinfrastructure may be held responsible for malicious cyber-acts that affect foreign countries. Commentators who argue for a "sanctuary theory" of liability contend that the international community may hold a state responsible for cyber attacks continuously launched from its cyberinfrastructure.[65] In effect, governments are obligated to take precautionary measures to ensure their portion of cyberspace does not provide a "sanctuary" for hostile cyber activities.[66] Both the International Court of Justice (ICJ) jurisprudence and the *Tallinn Manual* seem to support this theory of liability in cases where the state knows, or in some circumstances should have known, of the malicious activity.[67] Considering these conditions are met, the country from which malicious cyber activity emanates may be held accountable.

C. Issues with Anonymity and Attribution

The final notable challenge to responding to cyber-based threats is the difficulty in identifying the attacker. Anonymity is the

---

63. Heinegg, *supra* note 54, at 9. *E.g.*, 18 U.S.C. § 1030 (2011) (U.S. domestic criminal law on cybercrime, the Computer Fraud and Abuse Act); *See* Convention on Cybercrime, Council of Europe, Nov. 23, 2001, C.E.T.S. No. 185 (multilateral treaty on cybercrime that forty-seven countries have ratified).

64. Heinegg, *supra* note 54, at 10.

65. Beard, *supra* note 22, at 87-88 (internal quotation omitted); Nguyen, *supra* note 47, at 1104. *E.g.*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 92-96 (2010).

66. *See* Beard, *supra* note 22, at 87-88.

67. *See, e.g.*, Corfu Channel Case, Judgment, 1949 I.C.J. 4, at 18 (Apr. 9); TALLINN, *supra* note 62, Rule 5 ("A state shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for act that adversely and unlawfully affect other States.").

"cornerstone of Internet culture."[68] Users commonly use aliases and download free software to mask their identity.[69] In cyberspace, there are many ways to hide who you are. A simple way to mask identity is to register for services using false information, making it so that your online activity is not connected to your real personal identifying information. Another way to hide your identity is to mask the address that uniquely identifies your device—the IP address.[70] Still another way is to use "Tor" software which allows users to access an encrypted layer within the Internet, often referred to as the "Dark Web" or "Deep Web."[71] Finally, there is always the option of routing the attack and acting through another user's computer and identity,[72] an act known as "spoofing."[73]

Anonymity complicates response schemes because the first step in responding to any cyber attack is to find out who executed it and where it came from.[74] Computer specialists and experts are working to develop better methods for identifying the sources of attacks.[75] However, the dark heart of the Internet breeds ambiguity and anonymity. This is problematic because the identity of the actor and

---

68. David Davenport, *Anonymity on the Internet: Why the Price May be Too High*, 45 COMMUNICATIONS OF THE ACM 33, 33 (Apr. 2002), http://www.csl.mtu.edu/cs6461/www/Reading/Davenport02.pdf.

69. *See generally* Jonha Ravesencio, *Understanding the Benefits and Limits of Internet Anonymity*, THEHUFFINGTONPOST.COM (Oct. 15, 2015 2:34 PM), http://www.huffingtonpost.com/jonha-revesencio/understanding-the-benefit_b_8305984.html; TOR, https://www.torproject.org/ (last visited Dec. 1, 2015).

70. *See* MASKMYIP.COM, http://www.mask-myip.com/ (last visited Dec. 1, 2015).

71. Matt Egan, *What is The Dark Web? How to Access the Dark Web. What's the Difference Between the Dark Web and the Deep Web*, PCADVISOR.CO.UK (Nov. 23, 2015), http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/; *see also* TOR, https://www.torproject.org/ (last visited Dec. 1, 2015).

72. *See* Beard, *supra* note 22, at 76-77.

73. *Spoofing*, TECHOPEDIA.COM, https://www.techopedia.com/definition/5398/spoofing (last visited Apr. 8, 2016).

74. Margulies, *supra* note 3, at 7-8.

75. Beard, *supra* note 22, at 75-76.

the actor's motive are crucial to electing a lawful response, as will become evident in the discussion below.[76]

The fact that actors are difficult to identify once they have perpetrated an attack, coupled with the U.S. Government's limited ability to control bad-actors and prevent damage to innocent parties, justifies a hack-back response. If the actor cannot be identified after the attack, no response can be taken. This justifies attaching a beacon to data so that it and its captor are easier to find after the fact. Alternatively, if the attack can be detected in real-time, deploying electronic countermeasures to automatically shut down an attack midstream would be justified because it may be the only opportunity to respond to the attack. Unfortunately, the legality of these responses remains controversial under domestic an international law.[77] One reason is that hacking-back involves measures that affect computer networks belonging to both culpable and innocent actors.[78] Another reason is because the actual act of hacking-back is, in essence, a cyber attack and the line between what is and is not a lawful attack in response is not at all clear.[79] Thus, such a response, if not carefully articulated by both domestic and international law, risks escalation and may overall be counter-productive to achieving greater cyber security.

III. THE LAW RELEVANT TO CYBER-BASED ACTIVITIES

The United States has been developing domestic law to address cyber-based activities since 1986.[80] As for international law,

---

76. Margulies, *supra* note 3, at 8 ("Identifying the source of harm is crucial for the allocation of legal consequences.").

77. *See generally* CARR, *supra* note 4, at 46-47; Timberg et al., *supra* note 16; Kovacs, *supra* note 16.

78. Kovacs, *supra* note 16 (Attackers using hijacked computers constantly "change through multiple compromised computers to ensure their identities and locations remain unknown. This creates a big problem for hacking back. Although the attack may have been tracked to a certain computer, that computer is probably owned and used by some innocent party; a previous victim of the same hacker.").

79. *See generally* CARR, *supra* note 4, at 46-47; Kovacs, *supra* note 16.

80. OFFICE OF LEGAL EDUCATION EXECUTIVE OFFICE FOR THE UNITED STATES ATTORNEY, PROSECUTING COMPUTER CRIMES 1 (2015) (noting that with the dawn of the computer age in the early 1980s, law enforcement struggled to prosecute

President Barack Obama and the DoD have made clear that "[l]ong-standing international norms . . . apply in cyberspace."[81] However, existing laws provide incomplete and insufficient remedies to address the full spectrum of cyber attacks committed by non-state actors. Cyber activities can be broken down into four general categories: crime, espionage, warfare, and terrorism.[82] Currently, cyber-acts within these categories are largely being addressed by merely tacking on the existing law applicable to their respective real-world counterparts.[83] In the real world what constitutes crime, espionage, warfare, and terrorism is relatively well established.[84] However, this is not true of their cyber complements.[85] Therefore, applying existing laws, while sometimes effective, will not always be.

The following categories broadly define different cyber activities, focusing on their distinguishing factors. Within each category, the relevant law is discussed to identify existing laws that may be synthesized to formulate a threat-response framework. It is important to note that non-state actors' cyber-based activities may not neatly fall into only one category, but may, in fact, bleed into others. Therefore, the following categories are meant to broadly encompass the activities described within them—they are not exhaustive or all-inclusive, but

---

computer crimes, prompting Congress to create a new statute, 18 U.S.C. § 1030) [hereinafter PROSECUTING COMPUTER CRIMES].

81. U.S. PRESIDENT BARAK OBAMA, INTERNATIONAL STRATEGY FOR CYBERSPACE, PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. *See generally* U.S. DEP'T OF DEF., CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 943, 5-9 (Nov. 2011).

82. Most commentators break cyber-based activities into these four categories and attempt to define the kinds of activities encompassed in each category. However, the categories remain unsettled, and are used here to set the parameters of the threat-response framework contemplated by this Note. *See generally* Brenner, supra note 57.

83. Brenner, *supra* note 57, at 144. (The categories tack on to their real-world counterparts. In the real-world "the categories evolved as pragmatic responses to the challenges [States] must confront and overcome if they are to survive.").

84. *Id.*

85. *See* Brenner, *supra* note 57, at 145-46.

provide a starting point to understand the type of activity each category addresses.

A. Cyber Crime

Conventional crime is an act committed by an individual that a government criminalizes and punishes under domestic law.[86] The U.S. Department of Justice broadly defines cyber crime as "any violation of criminal law that involve[s] a knowledge of computer technology for their perpetration, investigation, or prosecution."[87]

Historically, cyber-acts have been treated as criminal matters rather than acts of espionage, warfare, or terrorism.[88] One reason for this is that criminal cyber-acts share features of many other cyber-based threats.[89] However, cyber crime can typically be distinguished as activity perpetrated by non-state actors exploiting financial data.[90]

As to criminal matters, governments have largely responded to cyber crime with domestic prosecution.[91] The United States criminalizes cyber crime under a few statutes, most notably the Computer Fraud and Abuse Act, Title 18 of the United States Code, section 1030 (CFAA).[92] The current CFAA is extremely broad because it has grown in response to concerns about the lack of "laws available to fight emerging computer crimes," and as cyber crime has grown in sophistication and complexity, so too has the statute.[93] It includes nearly every computer-related activity, provides civil and criminal remedies, and permits territorial and extraterritorial jurisdiction.

---

86. *See id.* ("A crime consists of violating a rule—a law—that prohibits certain conduct or causing certain 'harm' . . . [The criminal] system assumes individuals commit crimes.").

87. NAT'L INST. OF JUSTICE & DEP'T OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCES MANUAL 2 (1989); *see also* BLACK'S LAW DICTIONARY 427 (9th ed. 2009) (defining computer crimes as "[a] crime involving the use of a computer").

88. *See* CARR, *supra* note 4, at 62.

89. *See* Beard, *supra* note 22, at 131.

90. Beard, *supra* note 22, at 131.

91. *See* Heinegg, *supra* note 54, at 9.

92. 18 U.S.C. § 1030 (2011).

93. *See generally* PROSECUTING OFFICE CRIMES, *supra* note 80.

Essentially every kind of cyber act could be prosecuted domestically under the CFAA. For example, section 1030(a)(3) criminalizes unauthorized access to nearly any computer.[94] Sections 1030(a)(1) and (a)(2) criminalize unauthorized access to a computer to obtain or transmit classified or protected government information.[95] Acts that cause physical damage to computers can be prosecuted under 1030(a)(5).[96] Further, cyber terrorism can be prosecuted under Title 18 of the United States Code, section 2332b(g)(5)(B)(i), which specifically reference sections 1030(a)(1), 1030(a)(5)(A), and 1030(c)(4)(A).[97] While the CFAA provides these options for domestic prosecution, bringing international offenders to justice within the United States is easier in theory than in practice.

B. Cyber Espionage

Espionage has primarily been a government-on-government affair since time immemorial, but, recently, corporate, industrial, and economic espionage have become prevalent.[98] Broadly defined,

---

94. 18 U.S.C. § 1030(a)(3) (2011) ("Whoever... intentionally, without authorization to access any nonpublic computer of a department or agency of the United States... or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by of for the Government of the United States.").

95. 18 U.S.C. §§ 1030(a)(1)-(2) (2011).

96. 18 U.S.C. §§ 1030(a)(5) (2011) ("(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss").

97. 18 U.S.C. § 2332b(g)(5)(B)(i) (2011).

98. Espionage can be linked back to Sun Tzu's Art of War. SUN TZU, THE ART OF WAR 145 (513 B.C.). Chapter 13 specifically refers to "The Use of Spies." *Id.*; *see generally* Noah Leavitt, *Sun Tzu and the Art of Spying*, ALTERNET.ORG (Jan. 4, 2006), http://www.alternet.org/story/30394/sun_tzu_and_the_art_of_spying (last visited Mar. 2, 2016). As of 2013, Symantec estimated cyber economic espionage accounted for some $250 billion a year in intellectual property theft. Pierluigi Paganini, *Cyber-Espionage: The Greatest Transfer of Wealth in History*, INFOSECINSTITUTE.COM (Feb. 12, 2013), http://resources.infosecinstitute.com/cyber-

espionage is the "deceitful collection of information, ordered by a government or organization hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the collecting."[99]

Cyber espionage may be defined as the "unauthorized probing to test a target computer's configuration or evaluate its system defenses, or the unauthorized viewing and copying of data files."[100] Cyber espionage does not greatly differ from conventional espionage: both target the same kind of information for the same purpose. What remains critical to the act being characterized as espionage is that some foreign government or instrumentality is involved in the act.[101] Where cyber espionage differs is that a vast amount of information can easily be acquired from a remote location.[102] For example, a spy no longer needs to infiltrate a foreign government office and rummage through filling cabinets for state secrets. He may access those secrets from halfway across the world, safely out of the target state's reach.

Despite espionage's international component, international law does not address espionage.[103] Rather, espionage is proscribed under domestic law.[104] Title 18 of the United States Code, sections 794, 1831, and 1832 criminalize espionage.[105] Specifically, section 794(a)

---

espionage-the-greatest-transfer-of-wealth-in-history/ (last visited Mar. 3, 2016). McAfee estimated the global impact at $1 trillion per year. *Id.*

99. Lt. Col. Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 325-26 (1996).

100. Clay Wilson, CONG. RES. SERV., RL32114, BOTNETS, CYBERCRIME AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 12 (2008) [hereinafter CRS, BOTNETS, CYBERCRIME AND CYBERTERRORISM].

101. *E.g.*, 18 U.S.C. §§ 791-799 (2011); 18 U.S.C. §§ 1831-1837 (2011).

102. Neil Webb, *A New Age of Espionage*, THEECONOMIST.COM (Aug. 1, 2015) http://www.economist.com/news/international/21660104-electronic-spycraft-getting-easier-more-controversial-old-style-human-sort (last visited Mar. 4, 2016).

103. Beard, *supra* note 22, at 114.

104. Demarest, *supra* note 99, at 331; *e.g.* U.S. ATTORNEY'S MANUAL, TITLE 9: CRIMINAL, 9-59.000. JUSTICE.GOV, http://www.justice.gov/usam/usam-9-59000-economic-espionage (last visited Mar. 4, 2016) ("evidence of involvement by a foreign government, foreign agent or foreign instrumentality" is a factor considered in deciding whether to prosecute economic espionage).

105. Espionage Act of 1917, 18 U.S.C. §§ 791-799 (2011); Espionage Act of 1996, 18 U.S.C. §§831-1837 (2011).

forbids gathering information with the intent to transmit that information to a foreign government, to the benefit of that government or the detriment of the United States.[106] Economic espionage is criminalized under sections 1831 and 1832, which prohibit stealing, copying, downloading, uploading, or conveying any trade secret (1831) or information (1832) for the benefit of a foreign government or instrumentality.[107] Both individuals and organizations can be penalized for economic espionage.[108]

Sections 749, 1831, and 1832 have language that translates well to cyber espionage and are applicable without modification. Specifically, these sections already address transmitting information and do not limit the mode of transmission.[109] Thus, stealing and transmitting information in cyberspace may be domestically prosecuted under these sections.

Non-state actors who steal government information or intellectual property can also be prosecuted as cybercriminals.[110] This is because a cyber attack that gains unauthorized access to another computer to view or copy information would also be in violation of the CFAA. In such circumstances, spies can be prosecuted under either the statutory provisions relevant to espionage or under the CFAA. However, there will again remain the issue of whether domestic prosecution is a viable remedy. Given that it is foreign actors who engage in espionage, a logical inference can be made that most spies will go unprosecuted.

---

106. 18 U.S.C. §794(a) (2011) ("Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits. . . to any foreign government. . . shall be punished. . .").

107. 18 U.S.C. §§ 1831-1837 (2011).

108. 18 USC § 1831 (2011).

109. 18 U.S.C. § 794 (2011) (transmits or attempts to communicate information through any signal or instrument); 18 U.S.C. §1831(a)(2) (2011) (copies, downloads, uploads, alters, transmits, delivers, sends, communicates or conveys); 18 U.S.C. §1832(a)(2) (2011) (same).

110. CRS, BOTNETS, CYBERCRIME AND CYBERTERRORISM, *supra* note 100, at 12-13.

C. Cyber Warfare

Throughout history, warfare and armed conflict involved one country's military pitted against another's.[111] The contemporary battlefield is changing, but it remains controversial whether non-state actors are capable of waging war.[112] Warfare is defined as the "military operations between enemies . . . undertaken by [one nation] to weaken or destroy another."[113] Indeed, both U.S. domestic law and international law governing warfare focus primarily on a country's military activities.[114]

The DoD has stated that international legal norms governing armed conflicts apply in cyberspace.[115] The International Committee of the Red Cross defines cyber warfare as follows:

> [O]perations against or via a computer or a computer system . . . [which] aim to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system. By these means, a variety of "targets" *in the real world* can be destroyed, altered or disrupted, such as industries, infrastructures, telecommunications, or financial systems.[116]

---

111. *See generally* Military History Encyclopedia on the Web, HISTORYOFWAR.ORG, http://www.historyofwar.org/ (last visited Nov. 26, 2015).

112. Int'l Comm. of the Red Cross, *Int'l Humanitarian Law and the Challenges of Contemporary Armed Conflict* 42, AI Index EN 31IC/11/5.1.2 (Geneva Oct. 2011), https://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf [hereinafter *Challenges of Contemporary Armed Conflicts*]. International Humanitarian Law applies to civilians in situations where they directly participate in hostilities. However, generally speaking, non-state actors do not wage war. *See* Emily Crawford, *Virtual Battlegrounds: Direct Participation in Cyber Warfare* 9 I/S J. OF L. & POL'Y 1, 3 (Spring 2013).

113. *Warfare*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/warfare (last visited Nov. 26, 2015).

114. *See* Beard, *supra* note 22, at 83.

115. Beard, *supra* note 22, at 69 n. 5.

116. *Challenges of Contemporary Armed Conflict*, *supra* note 112, at 36.

While this definition seems incredibly broad, acts of war, such as armed attacks, are similarly broadly understood as discussed below in this section.

Cyber warfare differs from crime and espionage in that cyber warfare only covers a small section of attacks that can be considered either armed attacks or cyber operations committed by a nation's military forces during a period of armed conflict.[117] In other words, only where the scale and effects of an act of cyber crime or cyber espionage is sufficiently severe will it fall under the umbrella of cyber warfare.

Law governing warfare is divided into two broad areas: *jus ad bellum* and *jus in bello*. *Jus ad bellum* governs the transition from peace to war.[118] *Jus in bello*, or International Humanitarian Law (IHL) regulates wartime conduct.[119] For IHL to be applicable, either an "international armed conflict" or "non-international armed conflict" must be in progress.[120]

Jus ad bellum refers specifically to what must happen before a country may lawfully resort to armed force.[121] The United Nations Charter (U.N. Charter or Charter) is the starting point for these conditions.[122] Article 2(4) of the Charter prohibits the "use of force against the territorial integrity or political independence of any

117. *See* CARR, *supra* note 4, at 48.

118. *Id.*

119. Int'l Comm. of the Red Cross, *What are Jus ad Bellum and Jus in Bello?*, ICRC.ORG (Jan. 22, 2015), https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 [hereinafter ICRC, *Jus ad Bellum and Jus in Bello*].

120. Beard, *supra* note 22, at 82.

121. ICRC, *Jus ad Bellum and Jus in Bello, supra* note 119.

122. *See id.* While the Charter is binding only on members of the United Nations, the prohibition on the use of force (Article 2(4)) and right to self-defense (Article 51) are generally accepted and represents customary international law, binding on all states regardless of U.N. membership. U.N. Charter, art. 2, ¶. 4; U.N. Charter, art. 51. *See also* Statute of the International Court of Justice, art. 38; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986 I.C.J. REP. 14 (June 27) [hereinafter Nicar. v. U.S.].

state...."[123] Only where the use of force rises to the level of an "armed attack" may a state respond with military action in kind.[124]

However, the Charter does not define "force" or "armed attack."[125] The ICJ in *Military and Paramilitary Activities in and Against Nicaragua* explains it is the "scale and effects" of the force that determine whether it constitutes an armed attack justifying a state's recourse to armed force.[126] At minimum, "force" and "armed attack" include conventional armed force employed by a nation's military.[127] On the other end of the spectrum are coercive forces like espionage and economic or political sanctions.[128] Article 2(4) does not prohibit these forms of "force" even though they may interfere with another country's sovereignty.[129]

There are several analytical approaches to determining when a cyber attack is an armed attack, and thus, an unlawful use of force.[130]

---

123. U.N. Charter, art. 2, ¶ 4.

124. U.N. Charter, art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs . . . .").

125. Nicar. v. U.S., *supra* note 122, ¶ 176. "Armed attacks" are referred to in the U.N. Charter as acts that "authorize the 'inherent right' of self-defense, but the Charter provides no definition for 'armed attack.'" *Id.*

126. *Id.* ¶ 195.

127. Nguyen, *supra* note 47, at 1114.

128. *Id.*

129. *Id.*; *see also* TALLINN, *supra* note 67, Rule 11, paras. 10-11.

130. The common approaches for analyzing cyber attacks are: (1) the "instrument-based approach" which looks to whether the form of weapon used to carry out the attack is like the "physical characteristics traditionally associated with military coercion" (Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1041 (2007); *see also* Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L.J. 272, 289 (1996)), (2) the "target-based or strict-liability approach" which focuses on the attack's target (Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1041 (2007); *David E. Graham, Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 91 (2010); Eric T. Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 228-31 (2002)) (3) the effects- or consequence based approach which is discussed in this Note; and (4) the cyber-physical system approach which holds a cyber attack constitutes an armed attack when it cases

The consequentialist approach or effects-based approach is the leading view among experts and is prevalent among the United States' analysis of cyber actions.[131] This approach looks at the consequences of the cyber attack in determining how to categorize it.[132]

Cybersecurity analyst and expert Jeffery Carr adopted international-law-scholar Michael N. Schmitt's widely-employed consequentialist framework for analyzing when a cyber attack constitutes an armed attack.[133] Schmitt's six criteria are severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[134]

(1) Severity looks to whether the attack caused physical injury or destroyed property. The greater the damage, the more likely the cyber attack was an armed attack.
(2) Immediacy looks to whether the attack occurred "with great immediacy" or developed slowly. The negative effects of armed force require an immediate armed response in self-defense. Where an attack develops slowly, it is more likely to resemble a lesser form of force and the targeted state or international community have an opportunity to resolve the issue peacefully. Thus, there is less justification for treating the attack as an armed attack.
(3) Directness looks to whether the attack directly caused the consequences. The more contributory factors at play, the less likely the attack was an armed attack.
(4) Invasiveness looks to whether the attack physically or electronically crossed international borders and caused harm within a targeted country. The greater the intrusion into the targeted country's rights, the more it looks like an armed attack.

---

irreversible damage to a physical system controlled by computers. Nguyen, *supra* note 47, at 1084.

131. Beard, *supra* note 22, at 115-116; Nguyen, *supra* note 47, at 1122.

132. Beard, *supra* note 22, at 115-116; Nguyen, *supra* note 47, at 1122.

133. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA J. OF TRAN'L L. 885, 913-15 (1999). *Cf.* CARR, *supra* note 4, at 60-61; Gervais, *supra* note 9, at 539; Nguyen, *supra* note 43, at 1122-24.

134. CARR, *supra* note 4, at 61 citing Schmitt, *supra* note 133, at 913-15.

(5) Measurability looks to the quantifiable damage caused by the cyber attack. The greater the demonstrable harm, the more likely the attack was armed attack.
(6) Presumptive legitimacy looks to whether domestic or international law treats the activity as presumptively lawful. This factor examines state practice and international norms. The less the attack conforms to accepted state practice, the more likely it was an armed attack. [135]

If the cyber attack does not fit the criteria, military action is an inappropriate response. When more of the factors are satisfied, proportional and necessary military force in self-defense may be justified.[136]

Once armed conflict has broken out, *jus in bello* controls combatants' conduct. *Jus in bello* is governed by a combination of treaties.[137] Under IHL, four basic principles dictate responses:

(1) The principle of discrimination requires attacks never be directed against civilian objects.
(2) The principle of distinction requires attacks to distinguish between civilian and military objects.
(3) The principle of proportionality requires attacks not cause injury or damage to civilian objects in excess of the concrete and direct military advantage to be gained.
(4) The principle of precautionary measures requires those responsible for planning and carrying out attacks take measures to ensure the operations adhere to the principles of distinction and proportionality.[138]

Any cyber operations carried out during armed conflict would also have to abide by these principles. In other words, countries would have to respond to cyber attacks with these principles in mind.

---

135. CARR, *supra* note 4, at 61; Schmitt, *supra* note 133, at 913-15.

136. CARR, *supra* note 4, at 61; Schmitt, *supra* note 133, at 913-15.

137. *See generally* Int'l Comm. of the Red Cross, *Customary IHL—Helping to Improve the Protections of Victims of Armed Conflict*, ICRC.ORG (July 19, 2014), https://www.icrc.org/eng/resources/documents/interview/2014/07-29-customary-international-humanitarian-law-cihl.htm.

138. Beard, *supra* note 22, at 81-82.

As an aside, law governing warfare is set out here because it dictates responses by the U.S. military. Moreover, *jus ad bellum* and *jus in bello* are important because, depending on the intensity and severity of a cyber attack, military action may be justified. While non-state actors are not necessarily considered here to wage war, their malicious cyber activities may be comparable to acts of cyber warfare. In such cases, this paper contemplates non-state actors' activities as either criminal or terrorist acts. Thus, it is under either of these categories acts that could otherwise be considered warfare are accounted for.

D. Cyber Terrorism

Cyber terrorism represents an intersection between cyber crime and warfare. While terrorist acts may be violent and give way to armed conflict, non-state actors are not traditionally "understood to be capable of committing acts of war."[139] The ongoing conflict between a U.S.-led coalition and terrorist organizations in the Middle East may be challenging this notion.[140] However, as it stands, where terrorists carry out armed attacks or participate in hostilities during a period of armed conflict, they are not considered soldiers fighting a war, but civilians committing acts of terrorism.[141] Therefore, acts of cyber terrorism are not considered acts of cyber warfare.

Acts of cyber terrorism can be considered acts of cyber crime, however. Like cyber crime, cyber terrorism is carried out by

---

139. Gill v. Arab Bank, PLC, 891 F. Supp. 2d 335 (E.D. N.Y. 2012). *See also* Gervais, *supra* note 10, at 546.

140. Int'l Comm. of the Red Cross, *Int'l Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 31st Int'l Conference of the Red Cross and Red Crescent, Geneva 42 (Oct. 2011), https://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf [hereinafter *Challenges of Contemporary Armed Conflicts*]. There are instances where International Humanitarian Law applies to civilian. This is where they "directly participate in hostilities." *See* Emily Crawford, *Virtual Battlegrounds: Direct Participation in Cyber Warfare* 9 I/S JOURNAL OF LAW & POL'Y 1, 3 (Spring 2013). However, generally speaking, non-state actors do not wage war.

141. *Id.*

individuals or groups.[142] Moreover, the way current U.S. legislation deals with terrorism leads directly to prosecution under the CFAA, as is discussed below in this section. The United States defines terrorism under two categories—domestic and international. The difference between the two is where the terrorist acts occurred. Domestic terrorism is defined as:

> activities that involve acts dangerous to human lives that are a violation of the criminal laws of the United States . . . intended to intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; or to affect the conduct of the government . . . and occur primarily within the territorial jurisdiction of the United States.[143]

International terrorism is similarly defined, but *differs* in that it occurs "primarily outside the territorial jurisdiction or the United States, or transcends national boundaries . . . ."[144]

Cyber terrorism covers actions taken by both domestic terrorists, often referred to as Hacktivists,[145] and international terrorist like ISIS.[146] Cyber terrorism has been defined as "any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[147]

---

142. The criminal justice system is predicated on societal norms that discourages individuals from acting in certain way. Criminal justice does not have an eye on regulating behaviors between sovereign states. Rather, "[t]his system assumes individuals commit crimes. That assumption also applies to terrorism, which consists of committing what would otherwise be routine crime(s) but for ideological reasons." Brenner, *supra* note 57, at 145-46.

143. 18 U.S.C. § 2331(5) (2011).

144. 18 U.S.C. § 2331(1) (2011).

145. Gervais, *supra* note 10, at 546 ("Hacktivists are usually private citizens motivated by nationalistic or ideological feelings who possess sufficient skill to participate in a cyberattack.").

146. In this paper, hacktivists and cyber terrorism *will not* be used synonymously. Rather, cyberterrorists will refer specifically to hackers who attack on behalf of a transnational terrorist organization such as al-Qaeda or ISIS.

147. Sue Marquette Poremba, *Cyber terrorist threats loom 10 years after 9/11*, NBCNEWS.COM (last updated Sep. 6, 2011, 5:40 PM),

One possible response to cyber attacks that may be categorized as acts of cyber terrorism is domestic prosecution. As indicated, there is significant overlap between cyber crime and cyber terrorism. In fact, cyber terrorism is currently criminalized under the same statute that criminalizes cyber crime. Title 18 of the United States Code, sections 2331 to 2339, provide for domestic prosecution for a spectrum of terrorist activities.[148] Within these sections, section 2332b(g)(5)(B)(i) explicitly refers to computer crimes under the CFFA.[149] Section 2332b(e) even provides extraterritorial jurisdiction over persons who violate these laws.[150] Thus, both domestic and international cyberterrorists can be prosecuted domestically under these sections. However, these sections do not govern military action against international terrorists.

It is not clear under what circumstances the government may respond to international acts of cyber terrorism with armed force. The law governing the current "Global War on Terror" is not an extension of domestic criminal law, but seems to be governed by a series of ad hoc decisions.[151] After the September 11 terrorist attacks, Congress's Authorization for the Use of Military Force (AUMF) gave the President legal authority to use armed force against the Taliban and Al-Qaeda.[152] Additionally, a few sources of international law

---

http://www.nbcnews.com/id/44415109/ns/technology_and_science-security/t/cyber-terrorist-threats-loom-years-after/#.ViKzStKrRpg.

148. 18 U.S.C. §§ 2331-2339 (2011); 18 U.S.C. §§ 2331 and 2333.

149. *See* 18 U.S.C. §2332b(g)(5)(B) (2011) (referring to the "federal crime of terrorism" as any violation of 18 USC §§ 1030(a)(1), (a)(5)(A) [Computer Fraud and Abuse Act: relating to protection of computers], resulting in damage as defined in 1030(c)(4)(A) [relating to protection of computers] among others).

150. 18 U.S.C. § 2332b(e) (2011).

151. The War on Terror describes the United States' "military efforts against in insurgencies in Afghanistan and Iraq (which can be viewed as fronts in the larger Global War on Terror) and the global insurgency being waged by the al Qaeda terrorist network." Donald J. Reed, *Why Strategy Matter in the War on Terror*, 2 HOMELAND SEC. AFF. 10 (2006), available at https://www.hsaj.org/articles/685. *See also* Guy Raz, *Defining the War on Terror*, NPR (Nov. 1, 2006), http://www.npr.org/templates/story/story.php?storyId=6416780.

152. S.J. Res. 23, 107th Cong. (2001). There was a second AUMF against Iraq in 2002. This resolution is not included within the scope of this argument as it authorized use of force against a State. *See* H.J. Res 114, 107th Cong. (2002).

provided a legal basis for the United States to deploy its military to combat terrorists.[153] However, Congress never officially declared war against the groups and never extended the AUMF to include ISIS.[154]

Additionally, determining which regime of international law would apply to military action against terrorist acts, including those committed in cyberspace, is controversial. This is largely because of the significant classification problems of non-state actors, which arise under the law of war.[155] The United States' Global War on Terror is a kind of quasi-war, often classified as a non-international armed conflict (NIAC), in spite of the fact that the conflict is transnational.[156] A NIAC occurs when a State is fighting non-state groups.[157] For some time, NIAC has applied to instances of armed conflict against domestic terrorism.[158] An example is when a government fights

---

153. *See* 18 U.S.C. §§ 2331-2339 (2011); *e.g.*, International Convention for the Suppression of Terrorist Bombings (Jan. 12, 1998); International Convention for the Suppression of the Financing of Terrorism (Dec. 9, 1999); S. Con. Res. 1373 (Sept. 28, 2001); S. Con. Res. 1377 (Nov. 12, 2001).

154. Russell Berman, *The War Against ISIS Will Go Undeclared*, THE ATLANTIC (Apr. 15, 2015), http://www.theatlantic.com/politics/archive/2015/04/the-war-against-isis-will-go-undeclared/390618/. *See generally* Tanya Somanader, *The Authorization of Military Force Against ISIL Terrorists: What you need to Know*, WHITEHOUSE.GOV (Feb. 11, 2015), https://www.whitehouse.gov/blog/2015/02/11/authorization-military-force-against-isil-terrorists-what-you-need-know.

155. *See* Beard, *supra* note 22, at 84.

156. There have been questions about how to categorize the "War on Terror" (WOT). Some argue the WOT "is not an armed conflict." *International Humanitarian Law Overview*, Int'l Justice Res. Ctr, http://www.ijrcenter.org/international-humanitarian-law/ (last visited Nov. 1, 2015) [hereinafter *International Humanitarian Law Overview*]. The United States seems content with this claim, categorizing WOT as a political, symbolic war. *See generally* Guy Raz, *Defining the War on Terror*, NPR (Nov. 1, 2006), http://www.npr.org/templates/story/story.php?storyId=6416780; *but see* John C. Yoo and James C. Ho, *International Law and the War on Terrorism*, BERKELEYLAW.EDU (Aug. 1, 2003 11:47 AM), https://www.law.berkeley.edu/files/yoonyucombatants.pdf. In 2001, President Bush concluded the "attacks of September 11 placed the United States in a state of armed conflict, to which the laws of war apply." *Id.*

157. *International Humanitarian Law Overview*, *supra* note 156.

158. *See id.*; Int'l Comm. of the Red Cross, Unit for Relations with Armed and Security Forces, *Lesson 10: The Law of Armed Conflict - Non-international Armed*

armed dissidents within its territory.[159] In such circumstances, the conflict is not governed by the law of war, but by a handful of provisions that ensure the government does not violate individuals' human rights.[160] The complication here arises from the fact that the United States is not fighting armed terrorists or cyberterrorists within its territory. Rather, the conflict is international. However, classification problems also exist when attempting to term the conflict international because an international armed conflict (IAC) can "only be between two or more [s]tates."[161] IACs are governed by *jus in bello* as discussed above in the previous section on cyber warfare, and, as indicated, non-state actors are not traditionally understood to be capable of engaging in war.[162]

One solution is to extend the United States' current doctrine for international terrorism to include international acts of cyber terrorism. The United States has developed the "unwilling and unable" test to justify using armed force against terrorist groups located within other countries.[163] Under the unwilling and unable test, where country X suffers an armed attack by a non-state group, country X may use force in country Y against the group if country Y is unwilling or unable to suppress the threat.[164] Thus, where a cyberterrorist carries out a cyber attack comparable to an armed attack, responding with armed force may be justified under the unwilling and unable standard. Additionally, this standard could also be extended to allow for responses to any act of cyber terrorism, not with armed force, but with a proportional countermeasure. In other words, to justify hacking-back.

Conflict 2 (June 2002), https://www.icrc.org/eng/assets/files/other/law10_final.pdf [hereinafter *The Law of Armed Conflict - Non-international Armed Conflict*].

159. *International Humanitarian Law Overview*, *supra* note 156; *The Law of Armed Conflict - Non-international Armed Conflict*, *supra* note 158, at 2.

160. *See International Humanitarian Law Overview*, *supra* note 156; *The Law of Armed Conflict - Non-international Armed Conflict*, *supra* note 158, at 4.

161. *International Humanitarian Law Overview*, *supra* note 156.

162. *See Challenges of Contemporary Armed Conflicts*, *supra* note 140; Crawford, *supra* note 140, at 3.

163. *See generally* Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense* 52 VA. J. INT'L L. 483 (2012).

164. *Id.* at 486.

IV. THE THREAT-RESPONSE FRAMEWORK

As the above discussion makes clear, current legal solutions to the variety of cyber-acts a victim may experience exist in discrete bodies of law. However, in cyberspace acts of cyber crime, espionage, warfare, and terrorism exist concurrently and often intersect. Moreover, cyber attacks are not always neatly addressed by one body of law. Therefore, synthesizing these discrete categories is essential to providing U.S. law enforcement or military with an appropriate response framework to counter and deter malicious cyber activities.

The following methodology is one plausible response to cyber-based threats. The framework incorporates an option to hack-back for instances where domestic prosecution is unavailable. It begins the moment the cyber attack occurs and ends the moment a response is elected. Importantly, if a hack-back response is justified it must be proportionate to the attack experienced and must minimize collateral damage to innocent parties. A hack-back response risks escalating as opposed to deescalating situations and if too severe, risks being an unlawful cyber act itself. Therefore, it is critical that such a response is used cautiously and abides by the principles of proportionality and necessity.

To begin, an attack occurs. Can the identity of the actor or origin of attack be determined? If neither can, then no response may be taken because it is impossible to know who or what to respond to. On the other hand, *if only the origin* may be determined, a hack-back response may be justified against the country under the sanctuary theory.[165] Thus, the state's computer networks may be temporarily disabled or permanently destroyed depending on the severity of the attack the victim state experienced; the damage that innocent parties will suffer; and, the advantage sought to be gained by hacking-back.

---

165. *See* Beard, *supra* note 22, at 87-88 (describing the sanctuary theory). This justification, in international law is well founded, beginning with the Corfu Channel Case, Judgment, 1949 I.C.J. 4, at 18 (Apr. 9), and recently adopted by the TALLINN, *supra* note 67, Rule 5, which indicates that, "a state shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for act that adversely and unlawfully affect other States."

If the cyber attack is an armed attack under Carr-Schmitt's six criteria, responding with military force may be justified.[166]

On the other hand, *if the actor's identity* can be determined, is domestic prosecution available? If so, then the individual could be prosecuted under the relevant domestic law or CFAA provision.[167] If domestic prosecution is unavailable, does the attack constitute an armed attack under Carr-Schmitt's six criteria? If not, the justified response is to hack-back with beaconing or electronic countermeasures against the actor. For example, the attack could be shut down midstream, if possible. Alternatively, the individual's access to the internet could be restricted or his device effectively destroyed. If the actor is located in the territory of a state where the sanctuary theory is applicable, then that state's computer networks may be temporarily disabled. If, on the other hand, the cyber attack was an armed attack, military retaliation could be appropriate against the individual under the unwilling and unable standard or against the state if the sanctuary theory applies.

For more clarity, Figure 1 on the next page lays out the definition, key distinguishing factors, and relevant law for each category of cyber attack. The responses are then set out to address low-to-high intensity cyber attacks. Where there is less damage, a lower intensity solution is more appropriate. Where the damage the cyber activity causes is extensive, a high intensity response is justified. As an aside, warfare is not set out in its own category here because non-state actors are not encompassed in the laws of war. Rather, this paper contemplates non-state actors' armed activities as either criminal or terrorist acts. Thus, it is under either of these categories acts that could otherwise be considered warfare are accounted for.

---

166. *See* CARR, *supra* note 4, at 61; Schmitt, *supra* note 133, at 913-15.

167. For cybercrime, the individual could be prosecuted under 18 U.S.C. §1030 (the CFAA); for cyber espionage 18 U.S.C. §§ 794, 1831, and 1832; and, for cyber terrorism 18 U.S.C. § 2332b(g)(5)(B)(i), which specifically reference §§1030(a)(1), 1030(a)(5)(A), and 1030(c)(4)(A).

Figure 1: A Framework for Assessing the United States' Responses to Non-state Actors' Cyber-Based Activities

Cyber-Based Activity	**Distinguishing Characteristics**	**Low-Level Response**	**Mid-Level Response**	**High-Level Response**
Crime	Any violation of criminal law that involves the use of computer technology to exploit financial data purely for the sake of criminal enterprise.	Domestic criminal prosecution under 18 U.S.C. § 1030.	Hack-Back: Electronic countermeasures to stop the attack midstream, or block the accounts or device(s) associated with the actor.	Hack-Back: Destroy the devices associated with the actor. OR Sanctuary Theory: Target the state's cyberinfrastructure with a DDoS attack. The force used must not rise to the level of "armed attack" under Carr-Schmitt's six criteria.
Espionage	Deceitful collection of valuable or sensitive information by someone unauthorized to do so for the benefit of a foreign government or organization.	Domestic criminal prosecution under 18 U.S.C. §§ 794 (espionage) or 1831, 1832 (economic espionage and theft of trade secrets).	Hack-Back: Set beacon on sensitive data, and then remove data from computer system it is later found on. OR Electronic countermeasures to stop the attack or block the accounts or device(s) associated with the actor.	Hack-Back: Destroy the devices associated with the actor. OR Sanctuary Theory: Target the state's cyberinfrastructure with a DDoS attack. The force used must not rise to the level of "armed attack" under Carr-Schmitt's six criteria.
Terrorism	Violence or the threat of violence intended to intimidate the populace or a government, which is politically or ideologically motivated	Domestic criminal prosecution under 18 U.S.C. §§ 2331-2339 → § 1030.	Hack-Back: Electronic countermeasures to stop the attack or block the accounts or device(s) associated with the actor.	Hack-Back: Destroy the devices associated with the actor. OR Resort to military force against actor under the unwilling and unable standard if attack satisfies Carr-Schmitt's six criteria. OR Hack-Back under Sanctuary Theory: Target the state's cyberinfrastructure with a DDoS attack or permanently disable or destroy the hardware.

V. THE FRAMEWORK APPLIED TO AN EXAMPLE OF CYBER TERRORISM

On August 24, 2015, the United States killed a top hacker for ISIS with a military airstrike.[168] The United States targeted the cyberterrorist for hacking and posting the personal identifying information of military and government personnel on the Internet.[169] In March 2015, a few months before the airstrike, the hacker posted a list of one hundred soldiers with their photos, email addresses, and physical addresses on an ISIS website.[170] In late July and early August of 2015, he posted similar information of another 1,300 military and government employees on "jihadi forums" and social media sites.[171] With each posting, the hacker added a message urging ISIS supporters to carry out "lone wolf attacks"[172] on the soldiers whose information he listed.[173]

As early as the mid-1980s, the United States recognized cyber terrorism posed a threat to national security.[174] However, the August

---

168. *US Airstrike Killed Top ISIL Hacker—CENTCOM*, GLOBALSECURITY.ORG, (Aug. 28, 2015) http://www.globalsecurity.org/military/library/news/2015/08/mil-150828-sputnik03.htm; Mark Hosenball and Andrea Shalal, *U.S. Confirms Islamic State Computer Expert Killed in Air Strike*, REUTERS.COM (Aug. 28, 2015), http://www.reuters.com/article/2015/08/28/us-mideast-crisis-hacker-idUSKCN0QX2A420150828#YpSJt3SOc08Jv0ec.97. The hacker was Junaid Hussain was a British citizen who left Britain to join ISIS in 2013. *Id.*

169. Hosenball, *supra* note 168; Stalinsky, *supra* note 8.

170. Hosenball, *supra* note 168.

171. *Id.*

172. *See generally* Naina Bejekal, *The Rise of the Lone Wolf Terrorist*, TIME.COM (Oct. 23, 2014), http://time.com/3533581/canada-ottawa-shooting-lone-wolf-terrorism/ (A lone wolf attack is an attack carried out by an independent individual in the name of a terrorist organization.).

173. Stalinsky, *supra* note 8; *US Airstrike Killed Top ISIL Hacker—CENTCOM*, *supra* note 8.

174. *E.g.*, Robert Kelly-Gross, *1983 Hacking Investigation: EC's Sauls was Involved*, DAILYADVANCE.COM (Jan. 10, 2015), https://www.dailyadvance.com/features/1983-hacking-investigation-ecs-sauls-was-involved-2767759. (In 1983, the United States House of Representatives began holding hearings on hacking and computer security after the 414s broke into computer systems at a range of institutions including Los Alamos Laboratories.); Urizenus Sklar, *More About Electronic Disturbance Theater*, HUGFFINGTONPOST.COM (Oct. 20, 2010), http://www.huffingtonpost.com/urizenus-sklar/more-about-the-electronic_b_

24, 2015 attack was the first time the United States countered cyber terrorism with a military airstrike. The United States and its allies experienced multiple cyber attacks at the hands of ISIS hackers.[175] The specific hacker targeted by the United States was attributed with stealing and posting personal identifying information of over one thousand military and government personnel.[176] It is not clear whether any direct harm was caused by these postings in particular, but it is not hard to imagine the potential for grave injury that could have been caused. For example, if soldiers or personnel who were on covert missions were exposed by the posts, they could have been tortured or killed.

Once the United States experienced these attacks, in time, it was able to identify the actor. Because the hacker was linked to ISIS, was politically motivated, and used the threat of violence (calling for others to attack the soldiers posted), the act is best categorized as one of cyber terrorism. This conclusion is furthered by the fact that these attacks were not carried out for financial gain, and, therefore, less appropriately categorized as cyber crime. Domestic prosecution was likely unavailable considering the hacker was located either in Iraq or Syria where no government could be bargained with for extradition. Additionally, the hacker was part of ISIS's armed terrorist activities as an unlawful combatant, and if he were taken into custody Guantanamo Bay would have been a likely destination.

Despite the potential for danger, the cyberterrorist attack was not an armed attack under Carr-Schmitt's criteria:

(1) Severity: There was no physical injury or property destroyed.

770735.html. In 1998, The Electronic Disturbance Theater orchestrated a protest in support of the Zapatista guerilla movement in Mexico where individuals targeted the Pentagon, the White House, the School of the Americas, the office of Mexico's President, the Mexican Stock Exchange, and the Frankfurt Stock Exchange. *Id.* An estimated 10,000 people attacked the targeted websites, overloading the sites and shutting them down. *Id.* Chaos Computer Club, "Europe's largest association of hackers" claims to have been in business for over thirty years. CHAOSCOMPUTERCLUB.COM, https://www.ccc.de/en/ (last visited Nov. 24, 2015).

175. *See* Hosenball, *supra* note 168; Stalinsky, *supra* note 8.

176. *See* Hosenball, *supra* note 168; Stalinsky, *supra* note 8.

(2) Immediacy: The attack occurred relatively quickly, but there was time to use lesser force to resolve the danger. For example, the postings could be taken down.
(3) Directness: As of the writing of this paper, no one was injured as a direct consequence of the attack.
(4) Invasiveness: Additionally, posting the personal information of soldiers and government personnel was almost certainly an invasion of their privacy, and may have placed their lives in danger. Thus, the relative intrusiveness is moderately high.
(5) Measurability: There was no quantifiable damage caused by the attack.
(6) Presumptive legitimacy: Finally, the attack was not presumptively legitimate. No domestic or international law treats unprivileged posting of personal information with a call to assassinate those posted as a lawful activity.

Because four out of the six factors clearly weigh in favor of *not* classifying the attack as an armed attack, the United States' armed response is not justifiable under *jus ad bellum*.

Under these restrictions, hacking-back with a cyber attack targeting the hacker would have been justified and possible. If the United States knew who the hacker was and where he was, it is likely they were aware of at least some of his cyber activities. The United States could have sought to ban any online accounts associated with the hacker's activities, or deployed electronic countermeasures to disable or destroy any devices he was using.

The example of the ISIS hacker's cyber activities is but one small glimpse of when a hack-back response would have been appropriate. True, this response could have inadvertently interfered with the rights of innocent users if the hacker was sharing accounts of devices with others. However, this collateral interference seems negligible by comparison to that caused by a drone strike. Terrorist acts are, without question, vile and intolerable, but responding to a cyberterrorist's online postings with such deadly force is excessive and difficult to justify. Hacking-back, on the other hand, is proportionate and justifiable.

VI. CONCLUSION

The unique aspects of cyberspace can be accounted for when considering an appropriate legal regime for responding to international cyber attacks. However, the technology behind the Internet continues to advance, and more and more users are connecting. Lawmakers are considering ways to address the challenges posed by non-state actors in cyberspace, but many unsolved legal questions have gone unanswered in the face of politics and policy.[177] Meanwhile, law enforcement and the military are playing catch-up to investigate and respond to cyber attacks. A framework must be synthesized before the problem becomes too unwieldly.

It is essential for the U.S. Government to adopt a legal framework to effectively address the full spectrum of cyber attacks. The framework of this Note drew on domestic law as well as established and nascent principles of international law to solve this problem. However, this framework is but one example of solutions available, and, because of the scope of this paper, cannot possibly be all-inclusive. Indeed, other existing laws may effectively be combined to provide responders with a clear methodology to deal with non-state actors in cyberspace. What this Note sought to clarify was that cyber attacks can vary as widely as the groups who perpetrate them. This variety implicates a range of traditional laws that can be transposed onto cyberspace. However, whatever the framework the United States adopts to respond to non-state actors in cyberspace, it ought to be one that does not unnecessarily impede a free and open Internet, and this is arguable best achieved by permitting law enforcement or military to hack-back.[178]

Adopting a hack-back response is critical to protect our personal computers and cyberinfrastructure from malicious international actors. True, hacking-back carries with it the possibility that fickle cyber conflicts may escalate. However, when considering the alternatives, hacking-back may be the lesser of two evils. It is better than permitting malicious cyber actors to go unpunished, leaving the world economy to suffer billions in losses annually. It is better than running drone strikes on hackers. Moreover, it is the most viable way to

177. Beard, *supra* note 22, at 47 (internal quotations omitted).

address our cybersecurity concerns if we intend to keep the Internet a fluid, free exchange of information between autonomous, anonymous users. Indeed, hacking-back empowers victims of cyber attacks to protect their interests without burdening them with the charge of increasing their cybersecurity to a level where they can or should be able to prevent *all* malicious attacks. Such an alternative in unrealistic and may even be impossible. Thus, it is essential that lawmakers develop clear guidelines as to when and how to hack-back to deal with the broad range of cyber attacks the United States experiences daily.

*Jessica R. Gross**

* J.D. Candidate 2017, California Western School of Law.