Journal of Business & Technology Law

Volume 8 | Issue 1 Article 3

Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense

Shane McGee

Randy V. Sabett

Anand Shah

Shane McGee*, Randy V. Sabett**, and Anand Shah***†

Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense

"Security against defeat implies defensive tactics; ability to defeat the enemy means taking the offensive." —Sun Tzu, The Art of War [4:5][1]

"Only the active defense is the real defense, and is the defense for the counter attack and offense." —Attributed to Mao Zedong[2]

* Shane McGee, J.D., CISSP, is General Counsel & VP of Legal Affairs at Mandiant. Most of his career has been spent practicing at large firms in the areas of data privacy and security law. Shane, who has a J.D. from the University of Cincinnati, enjoys technology almost as much as he does the law, having worked as a programmer, consultant and instructor prior to law school. Prior to joining Mandiant, Shane spent eight years at SNR Denton where he was a partner and co-chair of the Internet and Data Protection Group. At SNR Denton, he also managed the firm's Investigations, Computer forensics and Electronic discovery (ICE) lab, and utilized that resource to conduct internal and external investigations.

** Randy V. Sabett, J.D., CISSP, is Counsel in the Washington, DC office of ZwillGen PLLC and has over 20 years of infosec experience, including as an NSA crypto engineer. His practice focuses on data security, privacy, licensing, and IP, dealing with such issues as identity management, active cyber defense, information security laws, and security breaches. He served as a Commissioner for the Commission on Cybersecurity for the 44th Presidency and is an adjunct professor at GWU, a Board member for the Northern Virginia chapter of ISSA, a frequent lecturer and author, and has appeared on or been quoted in a variety of national media sources. Previously, Mr. Sabett was a Partner at SNR Denton and a Special Counsel at Cooley LLP. He holds a B.S. in Computer Engineering from Syracuse University and a J.D. from the University of Baltimore.

*** Staff Attorney at MANDIANT Corp.; Technology Law Fellow at ZwillGen PLLC; 2010-2011 Research Assistant, NATO Cooperative Cyber Defence Centre of Excellence Tallinn Manual project; J.D., Emory University School of Law; B.A., George Washington University.

† The authors would like to thank and acknowledge the helpful input from Paul Byron Pattak on the early structuring of this article and the exceptional efforts of Dan Sachs, J.D. Candidate 2013, at the George Washington University School of Law, in helping with this article.

1. Sun Tzu, on the Art of War: The Oldest Military Treatise In the World 99 (Bob Sutton ed., Lionel Giles trans., Wiretap 2000) (c. 500 B.C.E.), *available at* http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2009229&site=ehost-live.

2. Wang Naiming, *Adhere to Active Defense and Modern People's War, in* Chinese Views of Future Warfare 37, 38 (Michael Pillsbury ed., rev. ed. 1998).

I. Introduction

Once primarily the domain of the federal government and a few specialized defense contractors, "active defense" has become an increasingly common topic even in unclassified circles due to (a) much more media exposure, (b) a general relaxing of attitudes toward offensive cyber behavior and, to some extent, (c) a frustration with the ability for companies to protect themselves with a purely defensive posture. Whether called active defense, standing your cyber ground, or hacking back, the notion of offensive use of cyber capability continues to gain considerable attention. As we ponder the implications of publicly-reported cyberattacks with a kinetic component (e.g., America's alleged involvement in Stuxnet[3] and the appearance of Flame[4]), we also need to determine if other broad attacks (e.g., Duqu[5] and Shamoon[6]) should be viewed as significant steps forward in attack vectors or simply more annoying distractions in the cyber landscape. In any event, no one can deny that offensive operations must be considered as a possible device in the cyber toolkit.[7] The logic seems valid — the right of self-defense has existed for hundreds of years in the physical realm; it should have a corresponding construct in the cyber world. Unfortunately, a lack of clarity in current law and policy has not allowed that to happen.

The U.S. military defines active defense as "[t]he employment of limited offensive action and counterattacks to deny a contested area or position to the enemy,"[8] but the government more generally has had a difficult time defining "active defense" in the civilian cyber realm.[9] For a host of reasons, ethical and legal issues associated with active defense have consistently served as barriers to having a

3. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times, June 1, 2012, at A1 (describing the Stuxnet worm as part of a secret U.S. government cyberattack program against Iran's nuclear enrichment efforts, code-named Olympic Games).

4. Nicole Perlroth, *Researchers Find Clues in Malware*, N.Y. Times, May 31, 2012, at B1 (describing Flame as "a data-mining virus designed to steal information from computers across the Middle East," and indicating that it may have been developed by the authors of Stuxnet).

5. *See* Mathew J. Schwartz, *3 Lessons Learned from Duqu Malware*, InformationWeek (Oct. 20, 2011), http://www.informationweek.com/security/cybercrime/3-lessons-learned-from-duqu-malware/231901299 (describing Duqu as a Trojan that "was designed to collect information for cyberespionage purposes").

6. *See* Phil Stewart, *"Shamoon" Virus Most Destructive Yet for Private Sector, Panetta Says*, Reuters, Oct. 12, 2012, *available at* http://www.reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012 (describing the Shamoon virus as having infected, and rendered useless, over 30,000 computers at Saudi Arabia's Armaco and Qatar's RasGas in August 2012).

7. In fact, at least one expert has observed that "[w]e can prevail only if we mount near-perfect defenses . . . . This . . . is, quite simply, too hard. A wholly passive strategy almost never works in the real world." Stewart A. Baker, Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism 228 (2010).

8. U.S. Dep't of Def., Joint Pub. 1-02, Department of Defense Dictionary of Military and Associated Terms 2 (2012), *available at* http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

9. *See* Ellen Nakashima, *When is a Cyberattack a Matter of Defense?*, Wash. Post Checkpoint Wash. (Feb. 27, 2012, 3:07 PM), http://www.washingtonpost.com/blogs/checkpoint-washington/post/active-defense-at-center-of-debate-on-cyberattacks/2012/02/27/gIQACFoKeR_blog.html (noting discord between the White House and the Department of Defense as to the definition of the term).

robust private sector dialog about the issue (though military analyses have been conducted).[10] For example, President Obama signed Presidential Policy Directive 20 in October 2012, which provides federal agencies with guidelines for conducting cyber operations, however, this remains secret from the public despite how it governs protection of private sector networks that support critical national infrastructure.[11]

Several reports and commentators have referred to the use of "all the tools of U.S. power"[12] or confronting cyberattacks "with all available means"[13] in discussing the overall aspects of the government's approach to cybersecurity. Many view these types of phrases as indirect references to offensive use of cyber capabilities. Other dialog related to military use of cyber capabilities has included more direct references to "use of force,"[14] "cyberattack[s],"[15] and "act[s] of war."[16] Further confusing the issue are discussions that conflate cyber espionage and cyberattacks.[17] For the commercial and private sectors, regardless of the terms used, an attack on their networks is just that, an attack that must be dealt with in some manner.

We have begun to see, however, certain progress being made toward gradually (and appropriately) shifting our military policy to deal with current threats. In his

10. *See* Comm. On Offensive Info. Warfare, Nat'l research Council of The Nat'l Acads., Technology, Policy, Law, And Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities x–xi, 28 (William A. Owens et al. eds., 2009) (describing how the recent emergence of cyberattack technologies coupled with the secrecy of the U.S. government on the issue has prevented a full dialog on the subject from occurring).

11. *See* Ellen Nakashima, *Obama Issues Guidance on Cyberwarfare*, Wash. Post, Nov. 15, 2012, at A07 (finding the PPD as the most sweeping effort by the White House to set forth "offensive" and "defensive" standards for cyber activities).

12. The Commission on Cybersecurity for the 44th Presidency recommended the creation of "a comprehensive national security strategy for cyberspace" that would include "*all the tools of U.S. power*—international engagement and diplomacy, *military planning and doctrine*, economic policy tools, and the work of the intelligence and law enforcement communities." Ctr. For Strategic & Int'l Studies, Securing Cyberspace for the 44th Presidency 17 (2008) (emphasis added), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

13. Specifically, Senator Joseph Lieberman said that "Google's experience should be a lesson to us all to confront this ever growing problem aggressively and *with all available means*." Paul Eckert, *U.S., Google and China Square Off Over Internet*, Reuters, Jan. 13, 2010, *available at* http://www.reuters.com/article/idUSTRE60C1TR20100113 (emphasis added).

14. White House, Cyberspace Policy Review 20 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf ("The United States needs to develop a strategy [for cybersecurity] designed to shape the international environment and bring like-minded nations together on a host of issues, including acceptable [legal] norms regarding territorial jurisdiction, sovereign responsibility, and use of force.").

15. Comm. On Offensive Info. Warfare, *supra* note 10, at 1.

16. Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War — Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force*, Wall St. J., May 31, 2011, at A1.

17. *Compare* Comm. On Offensive Info. Warfare, *supra* note 10, at 1, 261 (distinguishing cyber espionage, defined as non-destructive "intelligence gathering activity" from cyberattacks, defined as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks"), *with* Gorman & Barnes, *supra* note 16 (providing an example of an incorrect reference to cyber break-ins and data theft as cyberattacks).

remarks on Department of Defense (DoD) Cyber Strategy at the National Defense University in July 2011, Deputy Secretary of Defense Bill Lynn focused on the notion that "our posture in cyberspace must mirror the posture we assume to provide security for our nation overall."[18] He went on to state that:

> *Rather than rely on the threat of retaliation alone to deter attacks in cyberspace, we aim to change our adversaries' incentives in a more fundamental way. If an attack will not have its intended effect, those who wish us harm will have less reason to target us through cyberspace in the first place.*[19]

His additional remarks focused on enhancing our cyber defenses, but numerous other commentators have made it clear that offensive tactics must be a part of the strategy.[20]

Lynn also talked about the Defense Industrial Base (DIB) and the importance of the relationship between the government and private sector.[21] The DIB Cyber Pilot provided companies with enhanced and robust protection for their networks by allowing classified threat intelligence to be shared "with defense contractors or their commercial Internet service providers along with the know-how to employ it in network defense. By furnishing this threat intelligence, we are able to help strengthen these companies' existing cyber defenses."[22]

Analogizing between active defense and self-defense can be a useful analytical starting point. While self-defense in one's home clearly enjoys legal protection,[23] no such clarity exists in cyberspace. Despite this, many purported advantages of active cyber defense exist, including the ability to respond promptly to an attack, control over the situation by the victim, and no need for a victim to rely on or report the incident to anyone else, such as law enforcement. There are disadvantages, though. For example, the response from a victim against an attacker could lead to an

18. William J. Lynn, III, Deputy Sec'y of Def., Remarks on the Department of Defense Cyber Strategy (July 14, 2011), *available at* http://www.defense.gov/speeches/speech.aspx?speechid=1593.

19. *Id.*

20. *See id.* (discussing why the military needs offensive cyber capabilities); *see also, e.g.*, Comm. On Offensive Info. Warfare, *supra* note 10, at 69 (recommending that the United States maintain and acquire effective offensive cyber capabilities).

21. Lynn, *supra* note 18.

22. *Id.* The Defense Industrial Base pilot has since had its mission widened to include all critical infrastructure sectors and has been officially sanctioned as the Enhanced Cybersecurity Services program. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

23. *See, e.g.*, Crawford v. State, 190 A.2d 538, 541 (Md. 1963) (stating that "[t]here is also a generally accepted rule, which we think is correct, that a man faced with the danger of an attack upon his dwelling need not retreat from his home to escape the danger, but instead may stand his ground and, if necessary to repel the attack, may kill the attacker").

escalation — a digital "arms race;"[24] determining absolute attribution[25] can be difficult if not near impossible;[26] the retaliatory or defensive strike may cause more harm than the original attack and could easily impact innocent bystanders.[27] Furthermore, legal uncertainties exist as to whether active defense as a form of self-defense would be permitted.[28]

Those in favor of employing active defense are in general agreement about its inherent dangers.[29] On the fundamental issue of identifying the attacker, some commentators point out that increasing the accuracy of attribution would actually be detrimental as it would impinge on privacy rights.[30] Such a premise, however, is based on the overly restrictive assumption that "[r]etaliation requires knowing with full certainty who the attackers are."[31] While that would be an ideal situation, the reality differs significantly. Absolute technical attribution rarely can be achieved.[32] The question becomes, then, what level of attribution would be appropriate from a policy perspective in order to justify the use of active defense.

By far, attribution arises as the most significant issue around active defense.[33] As many commentators have somewhat erroneously noted, the Internet developed as an open environment without security in mind.[34] A somewhat more precise

24. *See* David E. Graham, *Cyber Threats and the Law of War*, 4 J. Nat'l Security L. & Pol'y 87, 97–98 (2010) ("[D]ecisions inherent in the use of active defense measures in response to a cyber attack are . . . fraught with policy considerations and risks of conflict escalation . . . .").

25. "Attribution" in this context refers to definitively and demonstrably identifying the attacker despite any ruses employed. Attribution, Merriam-Webster's Collegiate Dictionary 80 (11th ed. 2007) (defining attribution as "the ascribing of a work (as of literature or art) to a particular author or artist [or] . . . an ascribed quality, character, or right").

26. Jeffrey Hunker et al., Institute for Info. Infrastructure Protection, Role and Challenges for Sufficient Cyber-Attack Attribution 5 (2008).

27. Comm. On Offensive Info. Warfare, *supra* note 10, at 210.

28. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 Harv. J.L. & Tech. 429, 521 (2012) [hereinafter Kesan & Hayes, *Mitigative Counterstriking*] (noting that the common law claim of defense of property has never been invoked as a defense by a party being sued or prosecuted for engaging in a mitigative counterstrike to a cyberattack).

29. *See, e.g.*, *id.* at 486.

30. Hunker, *supra* note 26, at 11–12, 16, 19; *see also* David D. Clark & Susan Landau, *Untangling Attribution, in* Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Strategy 25, 25 (2010), *available at* http://www.nap.edu/openbook.php?record_id=12997&page=25.

31. Clark & Landau, *supra* note 30, at 25.

32. *See infra* note 37 and accompanying text; David Hollis, *USCYBERCOM: The Need for a Combat Command versus a Subunified Command*, Joint Force Q., July 2010, at 48–53, *available at* http://www.ndu.edu/press/lib/images/jfq-58/JFQ58_48-53_Hollis.pdf; Herbert Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. Nat'l Security L. & Pol'y 63, 77 (2010).

33. *Cyber-warfare: Hype and Fear*, Economist, Dec. 8, 2012, at 62–63, *available at* http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may.

34. Thomas A. Longstaff et al., *Security of the Internet*, *in* 15 The Froehlich/Kent Encyclopedia of Telecommunications 233 (Marcel Dekker ed., 1997) ("The ARPANET protocols . . . were originally designed for openness and flexibility, not for security.").

statement would be: what has become the *commercial* Internet developed without security in mind. Although originally developed out of a military/governmental project, the transition to a commercial environment meant that some of the very first attempts to add security clearly were not followed.[35] Regardless, anonymity occurred on the Internet more through evolution than as a result of ardent privacy activists.[36] As observed in a critique of a documentary about the early days of computing:

> *The upcoming shift, from in [sic] invite-only world to what we have today, is important; that's when hackers realized they were no longer alone on the Internet and had to go underground. Jeff Moss, founder of Black Hat and DefCon, describes in one of his interview segments growing up in the Bay Area in the 1980s and having one of the first affordable home computers that, with a modem, connected over the phone to various bulletin boards. He says that he could connect and no one would know his true identity or age; he would only be judged by what he wrote. For a 14 year old boy, Moss says it was liberating to be able to talk about sex and drugs.*[37]

Ultimately, we must contend with the fact that the current Internet is "flat," meaning the lack of ability to accurately identify people or devices can significantly inhibit online trust.[38] As such, even someone with no authority can at least "knock on the door" of any network around the world within his or her reach. Until we get to a point with better authentication (and, therefore, better ability to keep even more sophisticated intruders out), the ability to use offensive cyber methods at least to some level is needed. Such use necessarily depends on a clear national policy and legal position that addresses active defense. Such a policy will require a workable framework toward attribution (i.e., the identification of the attacker), including a determination of the nature and scope of the attack, along with a risk assessment

35. Paul Baran, RAND Corp., Mem. RM-3765-PR, On Distributed Communications: IX. Security, Secrecy, And Tamper-Free Considerations iii–iv (1964), *available at* http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3765.pdf ("The present Memorandum . . . [considers] the security aspects of a system of the type proposed, in which *secrecy is of paramount importance*" and evaluating the premise that the existence of spies within the supposedly secure system must be anticipated. Security provisions are based on the belief that protection is best obtained by "raising the 'price' of espied information to a level which becomes excessive." (emphasis added)).

36. *See, e.g.*, Daniel B. Levin, Note, *Building Social Norms on the Internet*, 4 Yale Symp. on L. & Tech. 97, 119 (2002) (attributing anonymity on the Internet to architectural features of the "code of basic Internet protocols, of Internet service providers, and of websites").

37. Robert Vamosi, *The Best Hacking Film You Haven't Seen (Yet)*, Forbes (July 20, 2012, 1:19 PM), http://www.forbes.com/sites/robertvamosi/2012/07/20/the-best-hacking-film-you-havent-seen-yet/.

38. White House, *supra* note 14, at 33 ("With the systems available today for most Internet transactions, the electronic equivalent of cues people use to establish trust might be absent, incomplete, or difficult to understand and act upon.").

considering the implications of mistakenly employing countermeasures (e.g., misattribution).

The nagging question involves picking the level of certainty required by a victim of cyberattack in the identity of the attacker before responding. At one extreme would be absolute knowledge of the identity of the attacker.[39] However, several scholars agree that significant difficulty exists in attaining 100% certainty of an attacker's identity and that even identifying an attacker beyond a reasonable doubt is "bordering on impossible."[40] At the other extreme would be a policy where little, if any, diligence would be required prior to attacking back. Richard Clarke provides perhaps the most accurate answer by stating that it will "depend upon the real-world circumstances at the time."[41] In this paper, we will lay out an argument that, since absolute identification of a cyber attacker is unrealistic, a national dialog should occur around what constitutes adequate attribution.[42] We will then provide a normative framework for use by the private sector when contemplating the use of active cyber defense.[43]

II. Interested Stakeholders and Their Role in Cyber Offense

It is no secret that the U.S. government as well as many other governments around the world have the ability to conduct offensive cyber operations.[44] The U.S. government's offensive cyber resources are shared between the military and intelligence communities.[45] While the extent and capabilities of those offensive assets are not public, it is reasonable to assume that they are substantial.[46]

---

39. *See* Clark & Landau, *supra* note 30, at 25 ("Retaliation requires knowing with full certainty who the attackers are." (emphasis omitted)).

40. Willie D. Jones, *Declarations of Cyberwar: What the Revelations about the U.S.-Israeli Origin of Stuxnet Mean for Warfare*, IEEE Spectrum (Aug. 2012), http://spectrum.ieee.org/computing/networks/declarations-of-cyberwar (quoting Larry Constantine, a software developer and professor at the University of Madeira in Portugal, as saying "it's difficult, bordering on impossible, to identify a cyberattacker beyond a shadow of a doubt").

41. Richard A. Clarke & Robert K. Knake, Cyberwar: The Next Threat to National Security and What to do About it 215 (2010).

42. *See infra* Part IV.

43. *See infra* Part V.A.

44. *See, e.g.*, Ellen Nakashima, *Pentagon: Cyber Offense Part of U.S. Strategy*, Wash. Post, Nov. 16, 2011 ("The Pentagon is prepared to launch cyberattacks in response to hostile actions . . . .").

45. *See* William J. Lynn, III, Deputy Sec'y of Def., Remarks at Stratcom Cyber Symposium (May 26, 2010), http://www.defense.gov/speeches/speech.aspx?speechid=1477 (noting role of U.S. Cyber Command in offensive cyber measures and calling the National Security Agency a "core" part of the U.S. government's cyber efforts); *see also Cybersecurity: DHS' Role, Federal Efforts, and National Policy: Hearing Before the H. Com. on Homeland Security*, 111th Cong. 36 (2010) (statement of Rep. Michael T. McCaul, Member, H. Comm. on Homeland Security) ("We have NSA, DOD that are very good at the offensive capability . . . .").

46. *See* David A. Fulghum, *Darpa to Develop Offensive Cyber Weapons*, 242 Aerospace Daily & Def. Rep. 3 (2012), *available at* 2012 WLNR 13092082; David E. Sanger, *U.S. Plans Attack and Defense in Web Warfare*, N.Y. Times, Apr. 28, 2009, at A1.

Other portions of the federal government, e.g., the Department of Homeland Security (DHS) and the Department of Justice (DOJ), have substantial investigative, remediation and other resources, but are generally thought to lack much offensive capability.[47] Likewise, state and local governmental agencies are not believed to possess offensive cyber resources.[48]

Further, while offensive capabilities are the exclusive province of the government, active defense is not. Government contractors, private enterprise, and even individuals are capable of and driven to implementing active defenses in an effort to frustrate, dissuade, deter, and hold responsible cyber attackers.[49]

Defense contractors are, by virtue of their commercial success, proximity to the government, and the value of the information they maintain, frequent targets of cyber espionage.[50] For many of the same reasons, these contractors are uniquely situated to engage in more 'active' defensive measures against attackers.[51] Their close ties to the government and more granular intelligence (including more accurate attribution) likely provide these contractors with a higher level of confidence both as to the efficacy of defense used, and whether domestic authorities are likely to tolerate their more active measures.

The rest of corporate America is not as fortunate as the defense industrial base when it comes to accurate intelligence, cooperative government relationships, or deployable cyber defenses. For most companies, active defense is a theoretical but out of reach capability sought by the overworked CSO rather than a deployable option (even without regard to the legalities). Still, some of the largest enterprises have built security teams competent enough to understand and execute on offensive measures against attackers.[52] When vital corporate intellectual property or

47. Comm. On Offensive Info. Warfare, *supra* note 10, at 137, 213 (discussing the investigative, remedial, and defensive roles of DHS and DOJ in cyberspace).

48. *See* Comm. On Offensive Info. Warfare, *supra* note 10, at 201, 201 n.2 (noting that state and local law enforcement lack authority to, for example, carry out denial-of-service attacks against wireless networks to prevent their use to conduct remote bombings).

49. *See, e.g.*, Joseph Menn, *Hacked Companies Fight Back With Controversial Steps*, Reuters, June 18, 2012, *available at* http://www.reuters.com/article/2012/06/18/us-media-tech-summit-cyber-strikeback-idUSBRE85G07S20120618 ("Companies can also allow intruders to make off with bogus files or 'beacons' that reveal information about the thieves' own machines, experts say.").

50. *See, e.g.*, Siobhan Gorman et al., *Computer Spies Breach Fighter-Jet Project*, Wall St. J., Apr. 21, 2009, at A1 (detailing theft of sensitive information on the F-35 fighter jet from defense contractors Lockheed Martin and BAE by attackers possibly located in China); David Leppard, *Chinese Steal Jet Secrets from BAE*, Sunday Times (London) (Mar. 11, 2012), http://www.thesundaytimes.co.uk/sto/news/uk_news/National/article991581.ece (indicating that British intelligence had confirmed to BAE that China was behind the data breach).

51. *See* David A. Fulgham, *Boeing's Buying Cyber*, Aviation Week Le Bourget Blog (June 11, 2009 3:29 PM), http://www.aviationweek.com/blogs.aspx?plckblogid=blog:dd3390dd-c9af-47ab-8bf5-3405dbe4a111&plckpostid=blog:dd3390dd-c9af-47ab-8bf5-3405dbe4a111post:159ca117-4d83-411a-8943-272bc82f3306 (noting Boeing's use of active defense technologies).

52. *See* Andy Greenberg, *New Grad Looking For a Job?: Pentagon Contractors Post Openings For Black-Hat Hackers,* Forbes (June 15, 2012, 9:22 AM), http://www.forbes.com/sites/andygreenberg/2012/06/15/new-grad-

multibillion dollar deals are on the line, the potential legal exposure arising out of such actions is just another frustration.[53]

III. Hypothetical and Non-Attribution Private Sector Attack Scenarios and Responses

A. Process

Today, a large number of cyberattacks in the commercial sector begin with an initial compromise achieved through phishing.[54] That is, attackers send an employee at the intended victim company an email or other electronic communication pretending to be a trusted entity.[55] These phishing communications sometimes solicit credentials directly, but more often include an attachment consisting of — or a link to — a malware "payload."[56] This malware payload, once executed, establishes a foothold in the corporate IT environment, escalates privileges, moves laterally across systems, and works to maintain its presence.[57] At the same time, the attackers controlling the malware use it to search the corporate networks and provide or plant information or code of their choosing.[58]

Preventing these types of attacks is difficult. If an adversary attempting to penetrate a network is advanced, as is the case with state-sponsored attacks, they will have access to technology and exploits that circumvent the traditional "Maginot Line" layer of traditional network security.[59] To detect these advanced attackers, companies need services or devices with access to up-to-date intelligence about the newest methods in use by advanced attackers.[60] Even then, prevention of

looking-for-a-job-pentagon-contractors-post-openings-for-black-hat-hackers-2/ (describing how large defense contractors are actively seeking job applicants with offensive cyber skills).

53. *See Coca-Cola 'Targeted' by China in Hack Ahead of Acquisition Attempt*, BBC (Nov. 5, 2012, 9:49 PM), http://www.bbc.co.uk/news/technology-20204671.

54. Warwick Ashford, *Phishing Attacks Cast Wider Nets in Businesses*, ComputerWeekly.com (Sept. 28, 2012, 2:29 PM), http://www.computerweekly.com/news/2240164139/Phishing-attacks-cast-wider-nets-in-businesses.

55. *See* Saul Hansell, *Online Swindlers, Called 'Phishers,' Lure the Unwary*, N.Y. Times, Mar. 24, 2004, at A1 (discussing phishing attacks and their mechanics).

56. Sudhir Aggarwal et al., *Trust-Based Internet Accountability: Requirements and Legal Ramifications*, 13 J. Internet L. 3, 11 (2010).

57. *See* Uri Rivner, *Anatomy of an Attack*, Speaking of Security (Apr. 1, 2011), http://blogs.rsa.com/rivner/anatomy-of-an-attack/ (describing the process of a recent successful phishing attack against cybersecurity company RSA).

58. *Id.*

59. *See* Kim Zetter, *Hack of Google, Adobe Conducted Through Zero-Day IE Flaw*, Wired Threat Level (Jan. 14, 2010, 2:27 PM), http://www.wired.com/threatlevel/2010/01/hack-of-adob (describing how advanced infiltration of numerous corporate networks by actors possibly inside China circumvented companies' defensive measures). The Maginot Line was a series of fortifications France built up along its borders before World War II. Merriam-Webster's Collegiate Dictionary 747 (11th ed. 2007).

60. David Salomon, Elements of Computer Security 157–58 (Ian Mackie ed., 2010) (reasoning that anti-virus software should be regularly updated due to the rapid and constant appearance of new malware).

the initial compromise is often impossible.[61] With technology that can detect, assess, and contain the attackers, though, the damage that would otherwise arise out of such an attack — if not the attack itself — can often be prevented.[62]

With the right equipment and personnel, an entity attacked even by one of the advanced, state-sponsored hackers can sometimes locate the command and control (often referred to as "C2") channel used by the attackers to communicate with the malware installed on the network.[63] These C2 channels often communicate through C2 servers controlled exclusively by the attackers.[64]

The temptation to try to access or destroy those C2 servers can be strong since doing so would disrupt the attackers' communication with the malware infecting your network.[65] Such a response would be of questionable legality, though, and would likely be considered an offensive act.[66]

Responses that are more likely to constitute "active defense" include poisoning documents or other files that you know may be exfiltrated by the attackers.[67] These files can either contain malware designed to shut down or slow the attackers, or just web-bugs — HTML links back to a web server you control — so that you can see

61. *See* Clay Wilson, Cong. Research Serv., RL32114, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress 25 (2008) (defining a "Zero-Day exploit" as a cyberattack that occurs when "a computer hacker discovers a new software vulnerability and launches a malicious attack to infect computers before a security patch can be created by the software vendor and distributed to protect users"); *see also* Randal C. Picker, *Cybersecurity: Of Heterogeneity and Autarchy*, *in* The Law and Economics of cybersecurity 115, 118 (Mark Grady & Francesco Parisi eds., 2006) (stating a developing problem that "the time between knowledge of the vulnerability [of attack] and exploitation by a hacker is dropping, as hackers pursue the zero-day exploit" defined as "no gap between knowledge of the vulnerability and malware that exploits it" (citing David Bank, *Computer Worm Is Turning Faster — Installing Security Patches Is Now Constant Rush Job Against Speedier Invaders*, Wall St. J., May 27, 2004, at B3)).

62. *See* Salomon, *supra* note 60, at 156–73 (describing various technologies to combat malware).

63. Nicholas Ianelli & Aaron Hackworth, CERT Coordination Center, Botnets as a Vehicle for Online Crime (2005), *available at* http://www.cert.org/archive/pdf/Botnets.pdf (explaining that by performing runtime analysis on malicious code, users may be able to capture information on the attackers, perhaps including the domain name for the command and control server and a channel name and password). For a thorough discussion of the advanced persistent threat, see Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

64. *See id*. at 16–20 (describing botnet command and control).

65. *But see* Internet Sec. Alliance, Social Contract 2.0: A 21st Century Program for Effective Cyber Security 24 (2010), *available at* http://www.isalliance.org/isa-publications/ ("Perhaps the best way to address this new reality is to recognize that attackers will get into your network and to expand defensive actions to detect, disrupt, and deny an attacker's command and control (C2) communications back out to the network.").

66. Jay P. Kesan & Carol M. Hayes, *Thinking Through Active Defense in Cyberspace*, *in* Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy 327, 328 (The National Academies Press ed., 2010) [hereinafter Kesan & Hayes, *Thinking Through*] (stating that counterstrikes have been going on for the past decade or more despite the fact that "such counterstrikes are of questionable legality under the current regime").

67. Menn, *supra* note 49.

from where your documents are being viewed.[68] Camouflaging systems or creating honeypots designed to misdirect hackers may also be considered active defenses.[69]

B. Policy

Private entities often prepare for the possibility of an attack by employing various security measures. These can include network design, encryption, device- and network-based authentication and verification measures, keeping security up to date and installing patches, and enforcing best practices for the use of technology.[70] An important component of preparation for a cyberattack is the deployment of strong authentication and authorization measures.[71]

During an attack, the primary goal of the targeted entity is to stop or mitigate the attack, rather than to gather evidence that may be used later.[72] How to stop or mitigate an attack is dependent on its nature and scope, requiring data-gathering and assessment. Private companies in the U.S. "generally ha[ve] real-time intrusion detection systems and prevention procedures."[73]

Some companies respond to detected attacks with purely passive, defensive practices. For instance, an entity that knows it is under attack will often seek to identify the vulnerabilities that the attacker is exploiting and patch or rectify them — perhaps by raising security standards or requiring a greater extent of user authentication.[74] The targeted entity may also seek to identify the attacker and determine what techniques the attacker is using; one type of passive defense is a "honeypot," a "decoy site[ ] designed to attract hackers to discover their attack techniques, and potentially their identities."[75]

68. *See* John Gilroy, *Ask The Computer Guy*, Wash. Post, Jan. 27, 2002, at H07 (describing a web bug as "a small, nearly invisible object on a Web page that can . . . relay data about your activity at that page to the outside Web site it's hosted at. This information could include such details as the Internet protocol address of the computer you're using . . . .").

69. *See* Salomon, *supra* note 60, at 295 (stating, "[a] honeypot is a server that acts as a decoy, attracting hackers in order to study their methods and monitor their activities. Security workers use honeypots to collect valuable information about new methods and tricks employed by hackers to break into computers").

70. *See* Peter Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?*, *in* The Law and Economics of Cybersecurity 29, 45–48, 61 (Mark Grady & Francesco Parisi eds., 2006) (discussing encryption and patching); *see also* Joel Trachtman, *Global Cyberterrorism, Jurisdiction, and International Organization*, *in* The Law and Economics of Cybersecurity 259, 265–66 (Mark Grady & Francesco Parisi eds., 2006) (discussing verification and authentication).

71. *See* Clark & Landau, *supra* note 30, at 34 ("[P]utting tools in place to implement good authentication and authorization is [sic] part of good security.").

72. *Id.*

73. Kesan & Hayes, *Mitigative Counterstriking*, *supra* note 28, at 462–63. For more on intrusion detection systems (IDS), see Kesan & Hayes, *Thinking Through*, *supra* note 66, at 330–31 ("IDS works partly by detecting patterns of attack by a particular attacker, so there is a challenge in detecting intrusions when the intrusion is being executed remotely by one person attacking through thousands of compromised computers in a botnet.").

74. *See* Salomon, *supra* note 60, at 209–31 (discussing authentication techniques).

75. Kesan & Hayes, *Mitigative Counterstriking*, *supra* note 28, at 471–72.

Commentators have described sole reliance on passive defenses as akin to a "duck and cover" approach, and suggested that targeted entities must meet force with force in order to repel cyberattacks.[76] Conceptually, active defense techniques can be sorted into three categories: (i) those where the victim redirects the attacker's attack back at the attacker;[77] (ii) those where the victim seeks to destroy, disable, or gain control of the systems of the attacker using their own attacks;[78] and (iii) those that are undertaken by an intended victim, preemptively, akin to the Stuxnet virus.[79] Although details are murky, active defense techniques have reportedly been deployed by governments, targeted entities, and security firms.[80]

An example of an active defense technique not involving attribution problems would be: "In the event of a [distributed denial of service] attack via a botnet, two potential neutralization responses may involve sending a [denial of service] attack at the botnet controller or hacking the botnet controller and thereby taking control of the botnet."[81] Other techniques might include sending a virus to or packet-flooding an attacker.[82]

Active defense encompasses three elements: detection, traceback, and counterstrike.[83] If an entity determines that it is under attack, it will use a type of traceroute called "traceback" to determine the source of the attack.[84] The four major techniques for Internet Protocol (IP) traceback are active probing, Internet Control Message Protocol (ICMP) traceback, packet marking, and log-based traceback.[85] However, attackers often use elusive techniques, such as IP spoofing, to attempt to

76. *Id.* at 417–18 (suggesting that the futile "duck and cover" approach used by American school children in the 1950s to protect against nuclear attacks is comparable to the passive defense approaches used by Internet users in that they both have questionability utility in the face of an attack).

77. *See supra* notes 49, 69, and text accompanying note 75 (detailing the use of bogus files and honeypots as active defense mechanisms).

78. *See* W. Earl Boebert, *A Survey of Challenges in Attribution*, *in* Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Strategy 41, 48 (2010) (contemplating increased use of counterattacks, or "hack backs").

79. *See id.* at 49 ("A further step in active defense is to mount preemptive covert operations against sites that are suspected to be planning or preparing attacks."). The Stuxnet virus, for example, targeted Iranian nuclear enrichment facilities as part of an effort to prevent Iran from obtaining nuclear weapons. Sanger, *supra* note 3.

80. *See, e.g.*, William J. Lynn, III, Deputy Sec'y of Def., Remarks on Cyber at the RSA Conference (Feb. 15, 2011) (confirming the deployment of active defense techniques to protect U.S. military networks); *see also* Kesan & Hayes, *Thinking Through*, *supra* note 66, at 333–34 (discussing that there are advantages to allowing targeted entities and attacked firms to counterattack as well as benefits to giving the government the right to carry out active defense strategies).

81. Kesan & Hayes, *Mitigative Counterstriking*, *supra* note 28, at 475.

82. *Id.* at 476.

83. *Id.* at 475 (showing that active defense includes intrusion detection systems, traceback, and counterstriking).

84. A traceroute is "the most widely used diagnostic tool on the Internet" and allows individuals to identify the source of an attack. *Id.* at 482.

85. *Id.* (citing Youg Guan, *Network Forensics*, *in* Computer and Information Security Handbook 339, 341–42 (John R. Vacca ed., 2009)).

thwart traceback, and although private entities and the government are reported to be actively innovating to improve traceback capabilities, these innovations are understandably shrouded in secrecy at present.[86]

Although the Stuxnet virus was more likely a response to the threat of a kinetic (nuclear) attack rather than a response to a cyberattack perpetrated by Iran,[87] it represents a valuable example of both a technique and a context of active defense that may be relevant for private entity responses. In terms of technique, Stuxnet was a virus designed to move across numerous systems and devices but to target only certain specific systems, therefore limiting the potential for collateral damage.[88] In terms of context, Stuxnet was likely a preemptive strike on systems believed to be in preparation for use in future kinetic attacks.[89] If private entities become aware of credible threats of imminent cyberattacks, they may very well seek to respond preemptively. Particularly when striking preemptively, however, private entities must be confident in their attribution techniques.

IV. Legal Issues Affecting Active Defense and Attribution

A. Self-Defense in Domestic Jurisprudence

Much of our law around self-defense evolved from English common law.[90] The fundamentals, however, date back much further. In the thirteenth century, for example, Thomas Aquinas posited that when an immediate risk arises that does not allow enough time for recourse to a superior (e.g., law enforcement), the use of force in an act of self-defense may be justified.[91] By the sixteenth century, the notion of chance-medley had developed, which was also called "chaud-medley" and

86. *Id.* at 483.

87. The Stuxnet virus "temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium." Sanger, *supra* note 3.

88. *See* Nate Anderson, *Confirmed: US and Israel Created Stuxnet, Lost Control of It*, Ars Technica (June 1, 2012, 6:00 AM), http://www.arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/ (reporting that the goal of Stuxnet "was to break Iranian nuclear centrifuge equipment by issuing specific commands to the industrial control hardware responsible for their spin rate").

89. *See* Sanger, *supra* note 3 (indicating that the Stuxnet virus was "America's most ambitious attempt to slow the progress of Iran's nuclear efforts . . . ."); *see also* Perlroth, *supra* note 4 (noting that security researchers uncovered evidence that Stuxnet was aimed at Iranian industrial control systems in order to weaken Iran's plans to build a nuclear bomb).

90. *See* Cathryn Jo Rosen, *The Excuse of Self-Defense: Correcting a Historical Accident on Behalf of Battered Women Who Kill*, 36 Am. U. L. Rev. 11, 25–33 (1986) (discussing the history of the law of self-defense, stemming from the common law, as it transitioned to the modern definition in the United States).

91. *See* Michael Skopets, Comment, *Battered Nation Syndrome: Relaxing the Imminence Requirement of Self-Defense in International Law*, 55 Am. U. L. Rev. 753, 759 n.23 (2006) ("Saint Thomas Aquinas proposed that the use of force in self-defense was justified in the case of a risk so immediate that it 'does not allow enough time to be able to have recourse to a superior.'" (quoting Thomas Aquinas, Treatise on Law 61 (Richard J. Regan ed. & trans., Hackett Publ'g Co. 2000) (1272))).

eventually became merged with the concept of manslaughter.[92] Chance-medley applied in situations where two people got into an avoidable altercation: an argument escalating into a bar fight, for example.[93] If such a situation was to escalate into violence, one person attacked by another may need to make a split second decision whether to kill or be killed. A claim of self-defense could be made but would only be found justified if the evidence showed that the eventual killer had attempted retreat, if retreat was possible.[94]

Two hundred years later, William Blackstone asserted that defense of oneself or a member of one's family would be acceptable by society if one "be forcibly attacked in his person or property."[95] Moreover, the inability of the "future process of law" to address the immediacy of the situation justifies opposing "one violence with another."[96] Any responsibility for such actions would fall only to the person who began the attack in the first place. Thus, as a "primary law of nature," a person can resort to self-defense as long as the force used does not exceed the defensive purpose of the action.[97] Otherwise, "the defender would himself become an aggressor."[98] Setting an appropriate balance provided a fertile ground for many commentators when analyzing various crimes.

When the common law migrated to America, the notion of chance-medley did not follow.[99] The individual rights espoused in the Bill of Rights were clearly present in the development of the doctrine of "stand your ground."[100] In the 1895 case of *Beard v. United States*, the Supreme Court addressed the following question: "Does the law hold a man who is violently and feloniously assaulted responsible for having brought such necessity upon himself on the sole ground that he failed to fly from

92. Richard Singer, *The Resurgence of Mens Rea: I-Provocation, Emotional Disturbance, and the Model Penal Code*, 27 B.C. L. Rev. 243, 250–51, 250 n.34 (1986). Chance-medley is "accidental homicide not entirely without fault of the killer but without evil intent." Merriam-Webster's Collegiate Dictionary 206 (11th ed. 2007).

93. *Id.* at 250–51; *see also* Jean K. Gilles Phillips & Elizabeth Cateforis, *Self-Defense: What's a Jury Got to Do with It?*, 57 Kan. L. Rev. 1143, 1158 (2009) (describing this historical claim of self-defense in the context of a fight).

94. Garrett Epps, Further Development, *Any Which Way But Loose: Interpretive Strategies and Attitudes Toward Violence in the Evolution of the Anglo-American "Retreat Rule,"* Law & Contemp. Probs. Winter 1992, at 303, 309–10.

95. 3 William Blackstone, Commentaries *3.

96. *Id.* at *4.

97. *Id.*

98. *Id.*

99. Epps, *supra* note 94, at 311.

100. *See* District of Columbia v. Heller, 554 U.S. 570, 592–93 (2008) (finding that "the historical background of the Second Amendment" shows that the English Bill of Rights, which gave Protestants the right to have arms for self-defense purposes, was "the predecessor to our Second Amendment"); *see also* Nicholas J. Johnson, *Self-Defense?*, 2 J.L. Econ. & Pol'y 187, 188 (2006) ("The imbedded self-defense question has been central to the Second Amendment debate of the last few decades. Most legal scholars who have considered the question conclude that the amendment secures an individual right to arms that includes a personal right to self-defense.").

his assailant when he might safely have done so?"[101] The Court found that a victim could legally exercise his or her right of self-defense without having to at least attempt to flee.[102]

Thus, what began as the "castle doctrine," which held that a person attacked by an intruder in the person's home has no duty to retreat and could use deadly force to repel an attack,[103] evolved into the "stand your ground" doctrine that applies to situations other than the home.[104] A little more than 100 years ago, an Oklahoma court ruled:

> *Under the old common law, no man could defend himself until he had retreated, and until his back was to the wall; but this is not the law in free America. Here the wall is to every man's back. It is the wall of his rights; and when he is [assailed] at a place where he has a right to be . . . he may stand and defend himself.*[105]

Much more recently, self-defense law has undergone some very public scrutiny due to the Trayvon Martin case.[106] That case dealt with a change in the Florida law related to self-defense, statutorily establishing the concept of "stand your ground."[107] Thus, the contours of self-defense continue to be tested and refined.

Reaching consensus on applying the concepts of self-defense to the cyber domain has proven to be a difficult task, though not for the lack of trying.[108] Proponents argue that just as a person has a right to defend oneself against imminent harm (whether or not retreat has been attempted, though analogies exist there as well), so does the owner of a cyber asset under attack.[109] In particular, since a computer network cannot "retreat," the notion of stand-your-ground described above becomes even more germane. Critics argue that active defense (a) lacks clear

101. Beard v. United States, 158 U.S. 550, 561 (1895).

102. *Id.* at 563–64.

103. Runyan v. State, 57 Ind. 80, 84 (Ind. 1877).

104. Recent Development, *Florida Legislation—The Controversy Over Florida's New "Stand Your Ground" Law—Fla. Stat. § 776.013 (2005)*, 33 Fla. St. U. L. Rev. 351, 355 (2005).

105. Fowler v. State, 126 P. 831, 833 (Okla. Crim. App. 1912).

106. *See, e.g.*, Rene Stutzman, *Police Say Teen Hit Zimmerman; Man Claims He Was Beaten, Injured*, Sun-Sentinel (Fort Lauderdale, Fla.), Mar. 27, 2012, at 1A ("[George] Zimmerman told police he shot [Trayvon Martin] in self-defense"); *see also* Sari Horwitz & Stephanie McCrummen, *Trayvon Martin Documents Reveal New Details in Shooting*, Wash. Post, May 17, 2012, at A01 (noting that the case was "provoking nationwide debates over . . . self-defense laws").

107. Fla. Stat. § 776.013 (2012).

108. *See, e.g.*, Nakashima, *supra* note 9 ("In the debate over how best to defend the nation against cyberattacks, one of the main points of tension relates to the extent to which the government should be able to deploy 'active defenses.'").

109. *See, e.g.*, Kesan & Hayes, *Thinking Through*, *supra* note 66, at 330.

rules[110] and (b) could easily escalate into a situation beyond the control of the attacked party.[111]

As a further obstacle to the use of active defense, there are international considerations preventing domestic activities. The Neutrality Act provides that no private entity can take action against a nation-state with which the United States is at peace.[112] Thus, if a cyberattack (e.g., along the lines of Stuxnet or Flame) was attributable to a nation-state against whom the U.S. was not at war, a private party would be prohibited from taking action directly against that nation-state.[113] In such a scenario, attribution becomes critically important. The likelihood is high, however, that a nation-state would be incentivized to carefully cover its tracks. In most cases, the nation-state would probably not even directly be involved. Instead, the nation-state would likely utilize an entity that would guarantee that the nation-state could claim plausible deniability that it was the source of the attack.[114]

B. Self-Defense in International Law

Because cyberattacks are commonly carried out by actors and computers outside the United States, it is instructive to consider the international bases for justifiable self-defense as between nation-states. While this article focuses on the private sector, given the interconnected nature of the Internet, it is possible that either (i) systems and networks employed for active defense are State-controlled or regulated; (ii) that active defense is authorized, potentially even carried out through the aid of a nation-state; or (iii) there are many quasi-governmental organizations serving dual roles, sometimes serving in a public capacity of the state, but simultaneously operate privately.[115] Thus, international law is necessarily implicated not only to instruct situations involving State action, but also companies using active defense would want to ensure their measures were not violative of international law, or at least be aware of the implications of their actions.

110. *See* Kesan & Hayes, *Mitigative Counterstriking*, *supra* note 28, at 479 (discussing how it is difficult for the attack victim to determine when an attack is in progress).

111. Graham *supra*, note 24, at 97–98; *see also* Kesan & Hayes, *Mitigative Counterstriking*, *supra* note 28, at 478–79.

112. 18 U.S.C. § 960 (2006).

113. *Id.* (prohibiting a private party from taking any part in a military or naval expedition against a country with which the United States is at peace).

114. *See* Cassandra M. Kirsch, *Science Fiction No More: Cyber Warfare and the United States*, 40 Denv. J. Int'l L. & Pol'y 620, 634 (2012) (observing that the party behind a cyber espionage plot based in China was entitled to plausible deniability because it could not be determined whether an entity other than the Chinese government was responsible); Kelly J. Higgins, *Attackers Engage in 'False Flag' Attack Manipulation*, Security Dark Reading (Oct. 1, 2012, 6:39 PM), http://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240008256/attackers-engage-in-false-flag-attack-manipulation.html (noting that skilled hackers were used as militias-for-hire to attack other nation-states).

115. *See infra* Part IV.B.3 (noting that a coordination between a Russian criminal organization and a Russian intelligence agency may have been responsible for a cyberattack); Part V.A (asserting that there are instances where private organizations are funded by state governments to carry out cyberattacks).

The basis of self-defense in international law is founded upon Article 2(4) of the United Nations Charter, which prohibits the use of force by one state against another, with one exception being when acting in self-defense, responding to an armed attack under Article 51.[116] This exception is relevant to the analysis here, raising the question of whether cyber intrusions are a use of force, an armed attack, or something different altogether. As scholars of *jus ad bellum* have correctly illustrated, there is a difference between what can be considered a use of force under Article 2(4)[117] and what is considered an 'armed attack' for purposes of self-defense under Article 51[118] — a difference that has consequences for the lawfulness of any operative countermeasure, including cyber.

1. Jus Ad Bellum[119] *Background*

The most common analytical approach to determining the difference between an armed attack or use of force involves assessing the gravity of the act, "to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms,"[120] as the International Court of Justice stated in *Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua*).[121] The Court held that sending armed bands (e.g., the contras from El Salvador into Nicaragua), as opposed to a regular army, could constitute an armed attack, whereas providing assistance to rebels in the form of weapons or logistical or other support (i.e., U.S. support to contras in El Salvador) would not constitute an armed attack.[122] Rather, the latter could be regarded as a threat or use of force, or intervention in the affairs of another State.[123] The Court relied on the "scale and effects" of the operation to help differentiate between a use of force and an armed attack, suggesting that mere "frontier incidents" would not rise to the level of an armed attack.[124]

116. U.N. Charter art. 2, para. 4 & art. 51.

117. *See* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 Yale J. Int'l L. 421, 426–29 (2011) (discussing three different interpretations of Article 2(4)).

118. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 195 (June 27) (assessing the meaning of "armed attack" in the context of the international law of self-defense); Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 63–64 (Nov. 6) (same); Tom Ruys, 'Armed Attack' and Article 51 of the UN Charter 139–42 (2010) (observing that the scale and effects of an armed attack distinguish it from less grave forms of the use of force).

119. *Jus ad bellum* translates from Latin to "justice of war" and regulates the pre-hostilities conduct of going to war. Richard P. DiMeglio et al., Law of Armed Conflict Deskbook 8, *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2012.pdf.

120. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 91 (June 27); *see also* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 101 (Nov. 6).

121. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 91 (June 27); *see also* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 101 (Nov. 6).

122. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 103–04 (June 27).

123. *Id.* at 104.

124. *Id.* at 103.

The line between frontier incidents and armed attacks is blurry at best, even within the ICJ's own jurisprudence. The Court has suggested that mining a single warship could constitute an armed attack in certain circumstances,[125] but has generally maintained a conservative approach both to the concept of armed attack and to the genesis of the attack (i.e., that it must reflect State action or be carried out by those operating on its behalf) — relevant to a discussion of attribution.[126] Thus, a right of self-defense can be invoked as an exception to the prohibition of use of force only if an 'armed attack' occurs because the drafters of the U.N. Charter in 1945 recognized only a limited right of self-defense.[127] The basis for this narrow approach is that a use of force "not tantamount to an armed attack is simply not of 'sufficient gravity,'" because an armed attack "presupposes a use of force producing (or liable to produce) serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property."[128] In essence, self-defense is a "remedy of last resort in a situation in which all alternatives for the peaceful vindication of a recognized legal right have been exhausted and the law

125. *See* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 191 (Nov. 6) (holding that the mining of a United States-flagged warship was not an armed attack against the United States because there was no evidence it was laid with the intention of targeting the United States). *But see, e.g.*, Corfu Channel, 1949 I.C.J. Rep. 4, 22–23 (Apr. 9) (holding that Albania was responsible for the explosions of British warships because it failed to warn the vessels of the danger that the vessels were heading towards).

126. *See* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9) (finding Israel's construction of a wall in the Occupied Palestinian Territory was contrary to international law); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 104 (June 27). *Cf.* S.C. Res. 1368, ¶ 3, U.N. Doc. S/RES/1368 (Sept. 12, 2001) (noting that threats to international peace and security were caused by terrorist acts, recognizing the inherent right of individual or collective self-defense in accordance with the U.N. Charter); S.C. Res. 1373, ¶ 2, U.N. Doc. S/RES/1373 (Sept. 28, 2001) (noting that threats to international peace and security were caused by terrorist acts, and reaffirming individual or collective self-defense in resolution 1368); *Statement by the North Atlantic Council*, North Atlantic Treaty Organization (Sept. 11, 2001), http://www.nato.int/cps/en/SID-D22D8FC5-11B5DDD9/natolive/official_texts_18863.htm (regarding authorization of self-defense in the aftermath of the 9/11 attacks).

127. *See, e.g.*, Ian Brownlie, International Law and the Use of Force by States 365–67 (1963) (discussing when the use of force might be necessary in a conflict); Ahmed Riffat, International Aggression: A Study of the Legal Concept 124–26 (1979) (determining that there are limited cases where an armed attach occurs against member states).

128. Yoram Dinstein, War, Aggression and Self-Defence 193 (4th ed. 2005) (quoting G.A. Res. 3314 (XXIX), U.N. GAOR, 20th Sess., 29(1) RGA 143 (1974)(Article 2 Definition of Aggression). An earlier edition of the same title had explained an "armed attack" as "a use of force causing human casualties and/or serious destruction of property," but notably this definition was expanded in the latest version. Yoram Dinstein, War, Aggression and Self-Defence 174 (3d ed. 2001). Dinstein posits that a restrictive interpretation is necessary because "[a]ny other interpretation" of Article 2(4) "would be counter-textual, counter-factual and counter-logical:" counter-textual because the use of the phrase 'armed attack' in Article 51 is not inadvertent and a threat of force was not covered in the General Assembly's Definition of Aggression in 1974; counter-factual because at the time of the drafting international customary law had consolidated its allowance of self-defense, in particular because there were no occurrences of preventive self-defense at the time; and counter-logical because the purpose of Article 51 was to introduce limitations on the exercise of self-defense. *See* Yoram Dinstein, War, Aggression and Self-Defence 183–85 (4th ed. 2005).

and the facts indisputably support a plea of extreme necessity."[129] This latter construction would be particularly useful in the commercial context.

Some argue, in contrast, that the gravity of the act is relevant to the necessity and proportionality of the response, but not to whether the act constituted an armed attack at all.[130] This broader view argues that the 'inherent' right of self-defense encapsulates earlier notions of self-defense existing in customary international law because at the time of its drafting, the U.N. Charter did not limit pre-existing rights of states, at least without explicitly doing so.[131] In analogizing from traditional *jus ad bellum* analysis to cyber issues, policy considerations can also be helpful. First, a narrow reading of armed attack leaves aggrieved parties with few options to protect their interests in the wake of a forcible measure short of an armed attack.[132] Second, some argue that restrictive self-defense options eliminate one avenue for limiting low-level uses of force, thus encouraging low-intensity conflicts and, ultimately, increased violence in international politics.[133] Alternatively, the ICJ's distinction between frontier incidents and armed attacks can serve to limit third-party States' involvement (i.e., the U.S. on behalf of Honduras and Costa Rica), thereby eliminating collective self-defense in the absence of an armed attack, while not necessarily negating the contentions of a particular victim state's own recourse (i.e., Honduras and Costa Rica directly).[134]

The consequence of the narrow reading of Article 2(4) and the Nicaragua decision in this regard is that the options for an aggrieved party to protect its interest in the wake of a forcible measure short of an armed attack are limited.[135] U.N. equanimity towards self-help has been described as a "remedy of last resort in a situation in which all alternatives for the peaceful vindication of a recognized legal

129. Thomas Franck, Recourse to Force: State Action Against Threats and Armed Attacks 131–32 (2002) (asserting that the systemic recognition of a margin of flexibility approximating consensus that facts, evidence, and sensitivity to political context shape responses to self-help claims). *Compare id.* at 133 (noting that in the Corfu Channel case, the ICJ held the British navy's military countermeasures as unlawful, yet it did accept that extreme necessity could mitigate the legal consequences of the illegality of those acts if necessity were demonstrable by clear contextual evidence), *with id.* at 130–31 (noting that Argentina was unable to legitimize its invasion of the Falkland Islands to a majority on the U.N. Security Council based on historic title and anti-colonialism).

130. *See* William H. Taft IV, *Self-Defense and the Oil Platforms Decision*, 29 Yale J. Int'l L. 295, 300 (2004) ("The gravity of an attack may affect the proper scope of the defensive use of force . . . but it is not relevant to determining whether there is a right of self-defense in the first instance.").

131. W. Michael Riesman, Law and Force in the New International Order 39–40 (Damrosch & Scheffer eds., 1991).

132. *See* Thomas Franck, *Some Observations on the ICJ's Procedural and Substantive Innovations*, 81 Am. J. Int'l L. 116, 120 (1987).

133. *See id.* (noting that due to the holding in *Nicaragua*, which limited the scope of an "armed attack," victimized states are left with little recourse against states, who are given a "free ride" and are "legally invulnerable," where minor insurgencies are directed from).

134. *See* Christine Gray, International Law and the Use of Force 130 (2000) (describing how the United States believed that it was justified in its use of force against Nicaragua, but the ICJ disagreed).

135. Franck, *supra* note 132, at 120.

right have been exhausted and the law and the facts indisputably support a plea of extreme necessity."[136] Nonetheless, because a use of force can embrace acts, such as arming or training guerillas, which fall short of an armed attack, it leaves open the possibility that non-physically destructive activities, especially cyber operations would fall into this category as well.

For this reason, assessing the parameters of the use of force and armed attack has particular relevance in the cyber arena. While there may be disagreement as to the particular application, *jus ad bellum* has been accepted by international law experts as being applicable to cyberattacks.[137] The following section is a brief survey of the main analytical approaches to cyber ops and *jus ad bellum,* as they may be relevant to active defense.

2. Cyber Operations as a Use of Force

Certain cyber-related terms, such as "cyberattack" or "active defense," do not appear in any of the formative writings concerning the use of force — naturally, given the vast technological developments of the past several decades.[138] The conventional means of waging war usually referenced in Article 2(4) analyses are typically grouped by the type of instrument used (e.g., gun or missile) to represent

136. Franck, *supra* note 129, at 131–32 (asserting that the systemic recognition of a margin of flexibility approximating consensus that facts, evidence, and sensitivity to political context shape responses to self-help claims). *Compare id.* at 133 (noting that in the Corfu Channel case, the ICJ held the British navy's military countermeasures as unlawful, yet it did accept that extreme necessity could mitigate the legal consequences of the illegality of those acts if necessity were demonstrable by clear contextual evidence), *with id.* at 130–31 (noting Argentina was unable to legitimize its invasion of the Falkland Islands to a majority on the U.N. Security Council based on historic title and anti-colonialism).

137. *See* Int'l Grp. Experts, N. Atlantic Treaty Org. Coop. Cyber Def. Ctr. Excellence, The Tallinn Manual on the International Law Applicable to Cyber Warfare 19 (Michael N. Schmitt ed., forthcoming 2013) [hereinafter Tallinn Manual], *available at* http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft (noting that the International Group of Experts behind the Tallinn Manual unanimously believed that *jus ad bellum* applied to cyber operations).

138. Thomas C. Wingfield, When is a Cyberattack and Armed Attack: Legal Threshold for Distinguishing Military Activities in Cyberspace (2006), which explains that the term "CNA" — also referred to "cyber war" — is a type of Information Warfare (IW), which is itself a subset of Information Operations (IO). He notes that the difference between IO and IW is that IO "may be undertaken at any level of conflict (strategic, operational, or tactical) and at any time during the resort to force (peace, crisis, or war)." However, IW "includes only those operations conducted in crises or wartime," and thus would be applicable only to *jus in bello* analysis. *See* U.S. Dep't of Def., Joint Pub. 1-02, Department of Defense Dictionary of Military and Associated Terms 2 (2012) (defining IO as "the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own"); *see also* Kenneth B. Moss, *Information Warfare and War Powers: Keeping the Constitutional Balance*, 26 Fletcher F. World Aff. 239, 241 (2002) (defining IW as "conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or conflict").

"kinetic impact."[139] It has been well reported that the wide variety of effects caused by "cyberattacks,"[140] spanning from those that cause financial damage to those that manipulate aspects of a national's critical infrastructure, "can influence the course of conflict between governments, between citizens, and between government and civil society."[141] Unsurprisingly in the non-kinetic cyber-context, military operators, policy-makers, and now corporate CIOs and CSOs, can find it to be a difficult process to know whether they have engaged in an activity that is a "threat or use of force," or conversely, whether they are a victim.[142]

While there are no definitive criteria for what constitutes a "threat or use of force,"[143] many commentators generally agree that a use of force may be non-kinetic, such that it encompasses cyber operations.[144] The "Schmitt Analysis" is considered the most widely accepted normative framework for considering whether

139. *See* Jason Barkham, Comment, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. Int'l L. & Pol. 57, 70–72 (2001) (discussing Article 2 and its grouping of the types of force into categories such as kinetic).

140. Note that this memo will primarily refer to "cyberattack," but will occasionally use other references to "cyber operation," "information operation," and "cyber network attack," with a synonymous meaning (as would any citing sources' use of the term "cyberattack"). An interdisciplinary study conducted by the National Research Council (NRC) of the National Academies defines the term as follows:

> Cyberattack refers to the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks. Such effects on adversary systems and networks may also have indirect effects on entities coupled to or reliant on them. A cyberattack seeks to cause adversary computer systems and networks to be unavailable or untrustworthy and therefore less useful to the adversary. Furthermore, because so many different kinds of cyberattack are possible, the term 'cyberattack' should be understood as a statement about a methodology for action—and that alone—rather than as a statement about the scale of the action's effect.

Comm. On Offensive Info. Warfare, *supra* note 10, at 10–11.

141. Kenneth Geers, *Sun Tzu and Cyber War*, N. Atlantic Treaty Org. Coop. Cyber Def. Ctr. Excellence (Feb. 9, 2011), *available at* http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf.

142. *See* Kesan & Hayes, *Mitigative Counterstriking*, *supra* note 28, at 479.

143. *See* Waxman, *supra* note 117, at 427–30 (discussing various approaches about how to categorize threats of force).

144. The threshold for non-kinetic activity as a use of force has been authoritatively discussed three times. The first occurred during the San Francisco drafting conference in 1945, in regards to a proposal by Brazil to include economic coercion, which was decisively rejected after being considered. 6 U.N.C.I.O. Docs. 344 (1945). Next, the topic came up during the U.N. General Assembly's Declaration on Friendly Relations, in which was decided that "[a]ll forms of pressure, including those of a political or economic character, which have the effect of threatening the territorial integrity or political independence of any State" would not all be uses of force. U.N. GAOR Special Comm. on Friendly Relations, U.N. Doc. A/AC.125/SR.114 (1970); *see also* Report of the Special Committee on Friendly Relations, U.N. Doc. A/7619 20, 32–33 (1969). In that respect, purely economic harm or political pressure would not constitute a use of force on its own. Thus, a cyber operation akin to psychological coercion would not qualify as being a prohibited use of force. Lastly, the ICJ held on this issue in the Nicaragua case that whereas arming and training a guerrilla force, a non-kinetic activity, was a use of force, the slight funding of that force was not a use of force. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 118–19 (June 27).

a cyberattack has risen to the level of a "use of force."[145] This seven-prong test addresses both the quantitative aspects of attacks, such as the amount of damage incurred, and the qualitative aspects, such as the nature/quality of the cyber operation in question.[146] To do so, the test applies a quantitative figure (e.g., a one-to-ten scale, whereby averages above a six may be definitely considered a use of force, below a four are definitely not, and in between four and six are debatable) to seven qualitative factors:

1. Severity (e.g., number of casualties, area/scope of attack, damage within area/intensity);

2. Immediacy (e.g., duration of attack, moment effects surfaced, and period of effects);

3. Directness (e.g., actual and proximate causation);

4. Invasiveness (e.g., physical or electronic border crossing, locus of action);

5. Measurability (e.g., quantifiable effects, level of certainty);

6. Presumptive legitimacy (e.g., acceptance within the international community, resemblance to kinetic attack); and

7. Responsibility (e.g., attribution)[147]

145. This framework can be found in Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885, 914–16 (1999) [hereinafter Schmitt, *Normative Framework*]. For support of the framework, see Matthew J. Sklerov, *The Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 Mil. L. Rev. 1, 56–57 (2009) (citing the Schmitt Analysis as the most useful approach to distinguishing uses of force in cyberspace). *See also generally* Stephen J. Cox, *Confronting Threats Through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War*, 42 Hous. L. Rev. 881, 901 (2005) (discussing Schmitt's innovative article); Eric Talbot 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 (2002) (approving Schmitt as the most accurate application of current international law, but proposing a forward-looking view due to the unique cyber environment); Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. Int'l & Comp. L. Rev. 439, 448 (2009) (commenting favorably on Schmitt, but discussing the difficulty of performing a legally sufficient review in the limited time available for a an effective active defensive response in cyberspace).

146. Schmitt, *Normative Framework*, *supra* note 145, at 914–16; *see* Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts*, *in* Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy 155–56 (2010) [hereinafter Schmitt, *Cyber Operations*].

147. Schmitt, *Normative Framework*, *supra* note 145, at 914–16 (listing the substantive points of the Schmitt Analysis); *see also* James B. Michael et al., *Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case*

The final prong assessing responsibility serves as a reminder that attribution is a vital consideration during the initial stages of assessing an attack by a victim state, and when that victim retaliates with its own measures against an identified aggressor state.[148] The Schmitt Analysis allows approximation to techniques used in characterizing traditional operations, so it also accounts for the technical realities that often frustrate cyber analogies to the brick-and-mortar world, for instance the likelihood of spoofed IP addresses.[149] Because of the applicability of the Schmitt factors to actions by private actors, it can be useful to compare and contrast to active defense as applied to corporate or other private entities — the idea being that the assessment is not operator-specific to only public actors.

This broad array of factors facilitates responses to the ever-changing dynamic of cyberattacks. The computer network attack:

> *Spans the spectrum of consequentiality. Its effects freely range from mere inconvenience (e.g., shutting down an academic network temporarily) to physical destruction (e.g., as in creating a hammering phenomenon in oil pipelines so as to cause them to burst) to death (e.g., shutting down power to a hospital with no back-up generators).*[150]

Notably, the Schmitt Analysis rejects the notion that the instrumentality or form of cyber operations be dispositive; instead, it emphasizes Article 2(4)'s purpose, which concerned the consequence or effect that uses of force would pose.[151]

Wide-support has established the Schmitt Analysis as a primary means to construe cyberattacks in a *jus ad bellum* context.[152] As some scholars have suggested, besides being a practical "legal algorithm," the test provides "a principled means" in order to "organize analysis in something other than a quantum cloud of uncertainty."[153] However, a variety of divergent views suggest there still is no bright line rule for determining a use of force for cyber operations. On one end of this spectrum, some experts suggest that the use of force prohibition cannot be

Study of Attack Scenarios for a Software-Intensive System, *in* Proc. 27th Ann. Int'l Computer Software & Applications Conf. 621–27 (2003) (detailing and demonstrating, by way of example, the quantitative and qualitative nature of the Schmitt Analysis).

148. *See* Schmitt, *Cyber Operations*, *supra* note 146, at 156–57 (defining responsibility in the context of the Schmitt Analysis and providing an example).

149. *Id.* at 154–56 (arguing that traditional terminology can fit within the context of cyberattack law, and then using that terminology to explain the different steps of the Schmitt Analysis).

150. Schmitt, *Normative Framework*, *supra* note 145, at 912.

151. Erik M. Mudrinch, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F. L. Rev. 167, 191 (2012); Schmitt, *Normative Framework*, *supra* note 145, at 914–15.

152. *See, e.g.*, Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 Naval L. Rev. 132, 168–72 (2005) (citing the Schmitt Analysis as an authoritative source on what constitutes "use of force" in a cyber context); Waxman, *supra* note 117, at 432 (calling the Schmitt Analysis "influential" in this regard); *see also supra* note 145 and accompanying text.

153. Michael, *supra* note 147, at 622–23.

adequately addressed by the Schmitt Analysis or through any existing regimes in current international law.[154] Rather, they argue that the particular challenges of cyber require an entirely new international framework.[155] Although its critics raise salient points, the Schmitt Analysis will likely remain the standard by nation-states for determining when cyber operations amount to uses of force, especially given its ease of use for military advisors.[156] Moreover, it serves as a model that can be adopted by private operators (e.g., CIOs and CSOs) to characterize the cyberattack their organizations have suffered. In particular, it can allow those private operators to incorporate a non-binary analysis of attribution into the broader calculus related to a cyberattack.

3. Cyberattack Example: DDoS in Estonia

The massive distributed denial of service (DDoS) attack on Estonia in 2007 offers a prime example for applying this analysis.[157] The DDoS occurred following the Estonian government's decision to move a Soviet war memorial from the center of its capital, Tallinn, to a military cemetery outside the city.[158] A series of cyberattacks were then undertaken against Estonia's government and commercial information systems, including those of the President and Parliament, banks, news agencies, and Internet service providers (ISPs).[159] The culprit behind the attack, according to news reports, was either Russian Nashi hackers (a pro-Kremlin youth group), or the Russian government itself, or possibly a coordination between them; however, absolute attribution has yet to be established, or at least announced.[160]

154. *See, e.g.*, Martin C. Libicki, Cyberdeterrence and Cyberwar iii (2009) ("Cyberspace is its own medium with its own rules. . . . [D]eterrence and warfighting tenets established in other media do not necessarily translate reliably into cyberspace."); Duncan B. Hollis, *Why States Need an International Law For Information Operations*, 11 Lewis & Clark L. Rev. 1023, 1040–42 (2007) ("The use of force prohibition encounters real difficulty . . . when translated into the [information operations] context.").

155. *See* Hollis, *supra* note 154, at 1040–42 (2007) (explaining "the novelty of [information operation] methods generates confusion regardless of the standard chosen," and seeks a system of international law for information operations, which could "rectify many of the deficiencies of the current legal system and provide states with additional functional benefits that do not currently exist").

156. *See* Tallinn Manual, *supra* note 137, at 47–49; Sklerov, *supra* note 145, at 56–57 (calling the Schmitt Analysis "the most useful analytical framework for evaluating cyberattacks); *see also* Thomas C. Wingfield, The Law of Information Conflict: National Security Law in Cyberspace 101 (2000).

157. Schmitt himself has used Estonia as a point of reference for the Schmitt Analysis. Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 Vill. L. Rev. 569, 577 (2011).

158. *Estonia and Russia: A Cyber-Riot*, Economist, May 2007, at 55, *available at* http://www.economist.com/node/9163598.

159. Schmitt, *Cyber Operations*, *supra* note 146, at 151; *see also* Eneken Tikk et al., International Cyber Incidents: Legal Considerations 14–33 (2010) (providing an in-depth look at the attacks, their background, their effects, and lessons learned).

160. *See, e.g.*, Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 Calif. L. Rev. 817, 837–38, 854 (2012) (noting that despite reports of Nashi involvement and suspicion of Russian government involvement, "authorities never officially attributed the attack to a state"); Schmitt, *Cyber Operations*, *supra* note 146, at 151 (noting that experts have tracked the Estonia attacks to a number of Russian government institutions, but also that the attacks had been "traced to at least 177 countries"); Charles Clover, *Kremlin-Backed Group Behind*

The DDoS had the immediate effect of severely disrupting the operations of all of Estonian society.[161] The consequences went beyond inconvenience; they were long-term and widespread, undermining confidence in the government and halting economic activity for several days.[162] They directly affected important individual and state functions, preventing the access to funds and interfering with the distribution of government benefits.[163] The DDoS targeted systems that were designed to be secure, and thus, necessarily operated highly invasively.[164] The consequences, albeit serious, were difficult to measure because the DDoS attacks had the effect of stymieing activity, not destroying data.[165] Although political and economic attacks are presumptively legitimate under international law because they are not considered uses of force, these cyberattacks did more than merely pressure Estonia.[166] The attacks intentionally frustrated civic functions.[167]

Forensic reports after the attacks have presented highly suggestive evidence of Russian involvement.[168] Additionally, the fact that Russian authorities refused to cooperate with later Estonian investigative efforts, transferred geopolitical tensions to presumptive guilt.[169] Under the Schmitt Analysis the quantitative value corresponding to attributing these attacks may be ranked as a six; albeit, not irrefutable, such a value range provides a reasonable basis for implicating Russian criminal groups and/or a rebuttable presumption of Russian-state involvement.[170] This level of attribution could be viewed as "good enough" for carrying out a countermeasure.

For the above reasons, many commentators find that the DDoS attack on Estonia reached the use of force threshold.[171] Under the Schmitt Analysis the

Estonian Cyber Blitz, Fin. Times (London), Mar. 11, 2009, at 8 (noting responsibility for the attack claimed by Kremlin-backed Nashi hackers); Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, Guardian (London) (May 17, 2008), http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (noting that the attacks in some instances appeared to originate from IP addresses belonging to Russian government).

161. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 Berkeley J. Int'l L. 192, 193–94 (2009).

162. *Id.*

163. *Id.*

164. Schmitt, *Cyber Operations*, *supra* note 146, at 157.

165. *Id.*

166. *Id.*

167. *Id.*

168. Traynor, *supra* note 160.

169. *See* Tikk, *supra* note 159, at 23.

170. *See* Schmitt, *Normative Framework*, *supra* note 145, at 915 n.81 (discussing "responsibility" as one criterion in the Schmitt Analysis).

171. *See* Schmitt, *Cyber Operations*, *supra* note 146, at 156–57 (noting that the attacks "arguably reached the use of force threshold"); Tikk, *supra* note 159, at 25 (noting that, in the wake of the attacks, "[p]arallels to conventional warfare and terrorism were drawn"); Eneken Tikk, *Global Cybersecurity — Thinking About the Niche for NATO*, 30 SAIS Review of Int'l Affairs 105, 114 (2010) ("[T]he 2007 Estonian incidents can be seen as beyond the threshold of an 'average' cyber crime…."); Mark Landler & John Markoff, *After Computer Siege*

majority of the seven-prongs would have been met.[172] Due to the rising frequency and severity of cyber operations, a future trend may presumptively regard similar cyberattacks as being a use of force, with evolving practice as being the force to "clarify the norm and its attendant threshold."[173] Had an alternative scenario occurred, whereby the only entities attacked in Estonia were strictly private organizations (and who had suffered attacks rising to the level of a use of force under the Schmitt Analysis), it behooves policy makers and victim corporations to consider how to assess the effects of their attack and their available recourse.

4. Cyber Operations as an "Armed Attack"

Similar to Article 2(4), so too Article 51 of the U.N. Charter was drafted before the advent of the Internet.[174] Article 51, establishing that an aggrieved State may resort to an individual or collective use of force in response to being the victim of an "armed attack,"[175] remains the central feature of *jus ad bellum*, and has been previously applied to non-kinetic challenges posed by biological and chemical warfare.[176] Likewise, Article 51 can be instructive for determining when a cyber operation amounts to an armed attack, and three approaches have been recognized to deal with this application: an effects-based approach, a target-based approach, and an instrument-based approach.[177]

---

in Estonia, War Fears Turn to Cyberspace, N.Y. Times, May 29, 2007, at A1 (noting that Estonia's defense minister called the attacks a "national security situation"); *cf.* Ulf Haeussler, *Cyber Security and Defense from the Perspective of Articles 4 and 5 of the NATO Treaty*, *in* International Cyber Security Legal & Policy Proceedings 105 (Eneken Tikk & Anna-Maria Taliharm eds., CCD COE Publications 2010) (discussing the Estonian cyberattacks in the context of thresholds for NATO action and analogizing NATO thresholds to U.N. thresholds).

172. *See* Schmitt, *Normative Framework*, *supra* note 145, at 914–15 (listing the prongs of the Schmitt Analysis).

173. Schmitt, *Cyber Operations*, *supra* note 146, at 157.

174. Articles 2(4) and 51 of the United Nations Charter were enacted in 1945. *See* U.N. Charter art. 2, para. 4 (discussing how U.N. members should retain in their use of force against other territories); *see also* U.N. Charter art. 51 (articulating that a state may act in self-defense to an armed attack against it). While the precursor to the Internet was discovered in 1965 when a computer in Massachusetts was connected to a computer in California over a telephone line – twenty years after Articles 2(4) and 51 of the United Nations charter were enacted. *See* Barry M. Leiner et al., *Brief History of the Internet*, Internet Society, http://www.internetsociety.org/internet/internet-51/history-internet/brief-history-internet#Origins (last visited Nov. 1, 2012) (noting that the Internet can be traced only to the 1960s).

175. U.N. Charter art. 51.

176. *See* Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Jan. 13, 1993, 1974 U.N.T.S. 45 (providing that a signatory may request assistance from other signatories to respond to the use of chemical weapons against it). *But see* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 Harv. Int'l L.J. 179, 179–80 (arguing that states have struggled in their attempt to promulgate rules of engagement in a timely manner when faced with advancements in warfare techniques and weaponry).

177. U.N. Charter art. 51; Hollis, *supra* note 154, at 1041; *see* Tallinn Manual, *supra* note 137, at 19 (the International Group of Experts behind the Tallinn Manual unanimously believed that *jus ad bellum* applied to cyber operations).

The predominant approach for assessing when a use of force in the cyber context crosses the threshold of an armed attack is an effects-based approach, premised on the idea that cyber warfare produces effects that can equate to kinetic force, namely the effects of death and destruction that flow from cyberattacks.[178] This view focuses on the consequences that result in the aftermath. Under the effects-based approach, a cyber operation is an armed attack if it either (i) causes actual physical damage or injury to persons,[179] or (ii) was specifically intended to cause physical damage or injury to persons.[180]

This approach to cyberattack is the most akin to traditional *jus ad bellum* regarding nontraditional kinetic warfare, and currently remains the favored approach by a number of states, including the United States, and even Russia, along with inter-governmental organizations, such as the North Atlantic Treaty Organization (NATO).[181] However, this emerging consensus is called into question, as some detractors object to a proposed normative framework based on Article 51 altogether. Critics to this effects-based approach find a daunting translational problem in applying existing international law to cyberattacks, largely because cyber operations represent an entirely different dynamic than traditional military operations, exhibiting everything from a diverse set of objectives in their usage (e.g., cyber hacking pranks and social protest) and varied results (e.g., cyber crimes of identity theft or harmless practical jokes) than traditional military operations.[182] However, even the most critical of objectors recognize the current framework of *jus ad bellum* will remain, at least until state practice and *opinio juris* would suggest otherwise.[183] Thus, the effects-based approach still stands as a robust approach for determining armed-attack.

178. Schmitt, *Normative Framework*, *supra* note 145, at 913 ("Armed coercion is not defined by whether or not kinetic energy is employed or released, but rather by the nature of the direct results caused, specifically physical damage and human injury."); *see* Hollis, *supra* note 154, at 1041–42.

179. Schmitt, *Normative Framework*, *supra* note 145, at 934; Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 Int'l L. Stud. Ser. U.S. Naval War Col. 99, 100 (2002).

180. Schmitt, *Normative Framework*, *supra* note 145, at 913.

181. Comm. On Offensive Info. Warfare, *supra* note 10, at 251–52 (citing Schmitt, *Normative Framework*, *supra* note 145, at 913) (recognizing that cyberattack assessment should be an effects-based analysis); Barkham, *supra* note 139, at 79 (same); Dep't of Def., Office of the Gen. Counsel, An Assessment of International Legal Issues in Information Operations 8 (2d ed. 1999) (detailing effects of cyberattacks that may constitute armed conflict); Karl Rausscher & Andrey Korotkov, The Russia-U.S. Bilateral on Critical Infrastructure Project: Working Towards Rules for Governing Cyber Conflict Rendering the Geneva and Hague Conventions in Cyberspace 25 (EastWest Institute 2011), *available at* http://www.ewi.info/working-towards-rules-governing-cyber-conflict (in introducing joint recommendations from Russian and American government and private sector officials, noting that a cyberattack that causes damage could be considered warfare); *see also* Brownlie, *supra* note 127, at 265–69 (discussing a results-oriented approach to the law of war); Haeussler, *supra* note 171, at 115, 120–21 (discussing an effects-based approach before urging revisiting the prohibition of the use of force in the cyber context); Tallinn Manual, *supra* note 137, at 19.

182. *See* Hollis, *supra* note 154, at 1040–42.

183. *Id.* at 1040–42.

It is possible to envision the applicability of the effects-based analysis in the private sector when dealing with certain critical infrastructure operators, such as power plants, hospitals, or water treatment plants. In these situations, theoretically a framework could be proposed whereby the company or its regulatory authority would have a means to establish physical damage in fact or that life or limb were lost, and thus invoke the right to self-defense. In these cases, the critical infrastructure that would affect the "right" effects because they are inherently the sorts that could cause physical damages, versus simply virtual, economic, or social; however, to exhibit the kind of effects that could take down networks in life-critical industries, the situations are few and far between.

The reality is that most private sector entities would not exhibit the "right effects" (i.e., physical damage or death), even if they were considered industries operating as critical infrastructure (e.g., banking or information technology).[184] The fact that their effects are not of the right kind, should not preclude them from trying to protect themselves; certainly, substantial economic harm can be debilitating on a wide-scale, as evidenced by the Global Recession of 2008.[185] It is imperative for policy makers to take a nuanced and flexible approach, albeit still based on the foundations of the various *jus ad bellum* theories, enabling private companies to have adequate methods of recourse, when they are substantially disrupted or disabled. This requires policy makers, as this paper will attempt to prove, to envision the other critical aspects of a company which are (a) affected in ways manifestly different from simply physical effects (e.g., to prevent a population from accessing bank accounts online); and (b) likely to the target of attack against a private organization (e.g., stealing trade secrets as part of corporate espionage) — both of which are evolving technological and cultural notions.[186]

V. Adequate Attribution for Active Defense

Attribution in the cyber context is defined as being "the identity or location of an attacker or an attacker's intermediary."[187] Attributing cyber operations is a critical determination in the assessment of the types of recourse a victim network operator has available to respond to an attack. As Hunker et al. have described, "[o]ur legal and policy frameworks for responding to cyberattacks cannot work unless we have adequate attribution; these frameworks remain incomplete because we lack the

184. *See* Schmitt, *Cyber Operations*, *supra* note 146, at 163 (noting that the "essence" of an armed attack is the causation or risk of death, injury, or tangible damage).

185. Phillip Swagel, The Cost of the Financial Crisis: The Impact of the September 2008 Economic Collapse 15 (Pew Fin. Reform Project, Briefing Paper No. 18, 2009), *available at* http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Economic_Mobility/Cost-of-the-Crisis-final.pdf (finding that American families' lost $3.4 trillion form the values of their homes between July 2008 and March 2009 and the value of their stocks fell by $7.4 trillion over the same period).

186. *See infra* Part V.A.

187. Hunker, *supra* note 26, at 5.

basis (sufficient attribution) to actually use them."[188] Such adequate attribution would be beneficial in three primary ways: (i) improving deterrence if there is a prospect that an attacker can be identified, (ii) strengthening security postures with defensive measures against identified sources, and (iii) promoting the active defense of networks to interrupt and neutralize incoming attacks.[189]

Various theories exist about how to determine the source of a cyberattack. For example, a technical approach can focus on the specific technical characteristics of the attack mechanism, such as identifying portions of attack code or programming techniques.[190] A list of nine technical approaches is summarized in Figure 1. Despite the fact that a technical approach helps to provide a framework for collecting digital forensics, it is widely held that even perfect technical proof is an inadequate measure for assigning responsibility to a cyberattack.[191] This is largely because of the ability of hackers to develop methods to overlay or confuse channels and the prevalence of IP spoofing.[192]

Figure 1: Some Current Technical Approaches to Attribution[193]

Technique	Description
Hash based IP traceback	Routers store a hash (relatively unique, compressed representation created by a one-way function) of each packet across the network; attribution is done by tracing back the hash across network routers
Ingress filtering	Require that all messages entering a network have a source address in a valid range for that network entry point. This limits the range of possible attack sources.
Internet Control Message Protocol (ICMP) return to sender	Reject all packets destined for the victim; return rejected packets to their senders (e.g., "destination unreachable" error message packet is sent back to the source IP address listed in the rejected packets).
Overlay network for IP traceback	An overlay network links all ISP edge

188. *Id.*

189. *Id.*

190. Irving Lachow, *The Stuxnet Enigma: Implications for the Future of Cybersecurity*, 11 Geo.J. Int'l Aff. (Special Issue) 118, 119 (2011).

191. Hunker, *supra* note 26, at 10–11.

192. *See id.* at 16–17 (discussing that technical approaches to attribution can be circumvented by spoofing — i.e., a user hiding his identity — and that it cannot be practically stopped).

193. This table has been reproduced in its entirety from *id.* at 16.

	routers to a central tracking router; hop-by-hop approaches are used to find the source; especially useful for large packet flows associated with DDOS attacks.
Generating trace packets using control messages (e.g., iTrace)	Periodically (e.g., 1 in 20,000 packets) a router sends an ICMP traceback message to the same destination address as the sample packet. The destination (or designated monitor) collects and correlates the tracking information.
Probabilistic packet marking	A router randomly determines whether it should embed information about the message's route into a given message. The defender can then use a set of messages to determine the route.
Hackback/countermeasure	Insert querying functionality into a host, specifically without the permission of the owner. If an attacker controls the host, this may alert the attacker and make the information less reliable.
Honeypots	Decoy systems that are only accessed by attackers capture information for attribution.
Watermarking	A passive technique that brands a file as belonging to a rightful owner.

Taking a more operational approach, one could observe the "tactics, techniques, and procedures (TTPs)" of the adversary.[194] In contrast to either a technical or operational approach, a focus on the "strategic context surrounding the event" could be employed.[195] Dmitri Alpertrov, a notable security expert, has posited that:

> *The threshold is not proof beyond reasonable doubt in the court of law but sufficient mix of suspicion and evidence to justify the retaliatory strike to the plurality of domestic and international audiences. For instance, strategic*

194. Lachow, *supra* note 190, at 119.
195. *Id.*

> *context of international relations at the time at which a cyber attack may take place can offer strong clues as to its origins.*[196]

Regardless of the approach used, the ultimate goal is to adequately identify the adversary so that a response can be deployed.

A. Framework for 'Good Enough' Attribution: A Roadmap

Defining "good enough" or adequate attribution as it pertains to our discussion of private-actors requires a framework that incorporates commonly practiced cyberattack analysis and threat assessments. Additionally, there must be a bifurcation of international versus domestic attacks, and different legal, strategic, and tactical considerations when dealing with a private actor that may be government-backed (e.g., government contractors). Contending with the technical and political realities requires that applicable standards are flexible and not so rigid as to be impractical or abused.

To this end, applying traditional standards of proof — the evidentiary levels required in U.S. criminal and civil jurisprudence — would be unwise. As U.S. Air Force Lt. Col. Forrest Hare recently attested to at an international conference, attribution represents more of a political concept rather than legal.[197] He warns that the traditional standards of proof — i.e., beyond a reasonable doubt, clear and compelling, and preponderance of the evidence — are inapplicable in cyber operations, let alone most military or intelligence activities.[198] Nonetheless, Bret Michael, a professor at the U.S. Naval Post-Graduate School, contends that the challenges of attributing the source of an attack can be overcome by weaving what he terms, "a clear mosaic of responsibility."[199]As such, Michael believes that showings of who provided monetary funding or material technical instruction may be adequate.[200] In light of the state of the cyber world, both in a nation-state and private-context, we find Michael's assessment as highly instructive.

The goal of our "good enough" standard will, therefore, be premised upon trying to paint a "mosaic of responsibility," based upon the multitude of factors (e.g., political, economic, social, technical, etc.) that reasonably point to the source of an attack. While it has been duly noted that the concept of "spoofing," is regarded by security experts as being more of a rule than an exception;[201] the basic

196. Dmitri Alperovitch, Towards Establishment of Cyberspace Deterrence Strategy 91 (C. Czosseck et al. eds., CCD COE Publications 2011) (citing Eric Sterner, *Retaliatory Deterrence in Cyberspace*, 5 Strategic Studies Quarterly 62, 71, 73 (2011)).

197. Jones, *supra* note 40.

198. *See, e.g.*, *id.*

199. *Id.*

200. Jones, *supra* note 40.

201. Sharon Nelson & John Simek, *Smoke and Mirrors: Fabrication and Alteration of Electronic Evidence*, Law Practice, Mar. 2007, at 22–23 (discussing the practice and prevalence of email spoofing).

premise in building a prima facie case against an aggressor, and thus, justification for employing active defense, remains that the "good enough" standard allows for a rebuttable presumption against an alleged aggressor. The burden of proof for the prima facie case for employing active defense measures lies with the victim-plaintiff's rendition of a responsibility mosaic; whereas the rebuttal or any other complete or partial defense must be reasonably established by an alleged attacker-defendant.[202]

The framework envisioned considers the grave danger that inaction presents to private organizations, while also pairing together the advances in attribution technology, the risks presented of a misattributed counterstrike, and the overall interests of the principal stakeholders (i.e., the victim, the alleged attacker, nation-state interests, and users of the Internet, at large). The explanation of the framework will first begin by applying a "good enough" standard in a domestic context, as between domestic companies and according to common law civil and criminal jurisprudence.[203] Second, the international context will be explored as between purely private organizations located in different countries, in light of prevailing international law standards.[204] Third, another dynamic will be explored as between private organizations located in different countries, but where one or both of the actors are either funded or in some form commissioned by a nation-state actor.[205] Naturally, this will invite a discussion of the applicability of the Laws of Armed Conflict.[206] An examination of these different scenarios and legal issues will reveal a roadmap that both companies and governments can use in assessing whether to engage in active defense and the policy recommendations to be crafted for resolving private-sector cyber conflicts. Ultimately, the "good enough" standard will enable attribution to adequately ascertain the identity of an attack source — promoting systemic cyber deterrence — while still being able to serve as a limiting principle for justifying active defense only when appropriate — preventing the unnecessary escalation of cyber aggression.

1. Domestic Private-Sector Attacks

The contours of an entirely domestic conflict require that one non-governmental organization (the "aggressor-company"), based in Country A, takes action against another non-governmental organization (the "victim-company") in Country A, using only commercial cyber infrastructure, means, and engineering to launch the

202. *Compare* Schmitt, *Cyber Operations*, *supra* note 146, at 169 (discussing that a state acting in self-defense bears the burden of proof), *and* Jones, *supra* note 40 (discussing that a state may collect sources to meet its burden of proof), *with* Schmitt, *Cyber Operations*, *supra* note 146, at 169 (stating that a state acting in anticipation of an attack also bears a burden of proof).

203. *See infra* Parts V.A.1–3.

204. *See infra* Part V.A.4.

205. *See infra* Part V.A.5.

206. *See infra* Part V.A.5.

attacks. This model presupposes that the purpose for engaging in such attacks is limited either (i) to facilitate the acquisition or espionage of corporate intellectual property (IP), sensitive information, or other physical corporate assets — acts which could be actionable under civil tort liability or per se illegal under criminal statutes; or (ii) to damage, disrupt, or neutralize corporate IP, sensitive information, or other physical corporate assets — implying criminality, either per se under Country A's criminal statutes or common law crime where mens rea (specific or general) is established, along with the potential for civil tort liability. In either case, the normative framework requires that there be an attack made to serve primarily economic ends — e.g., to diminish or dilute victim-company's competitive edge, and in turn improve or maintain aggressor-company's footing.

Additionally, assumptions need to be drawn for analogizing between physical and the Internet world. Torts and crimes against one's property do not allow for any self-help, physical self-defense measures to be taken, except in narrower circumstances for when there is "hot pursuit," as against an alleged tortfeasor or criminal assailant.[207] Where torts and crimes are committed against a person, self-defense measures are allowed against the attacker.[208] For instance, under common law assault, self-defense is allowed by a victim or third party when there is a reasonable apprehension of immediate harm against the victim's person or another person.[209]

2. Attacking the Victim-Company's Property

Cyberattacks of a primarily economic motivation, would be mostly considered as either a tort or crime against a company's property, thereby restricting the ability to pursue any active defense-counter measure except for alerting legal authorities to help them, unless there is arguably a "hot pursuit" against the aggressor.[210] While immediacy is an important factor in weighing whether "hot pursuit" to retake physical stolen property, perhaps the standard may be relaxed or redefined as to cyber detections and intrusions, which may occur simultaneously in real-time if a victim-company monitors leaked information being stolen or potentially after some reasonable amount of time after-the-fact that a victim-company realizes that

207. Adam B. Badawi, *Self-Help and the Rules of Engagement*, 29 Yale J. on Reg. 1, 30–33 (2012) (self-help); Gregory A. Diamond, Note, *To Have but Not to Hold: Can "Resistance Against Kidnapping" Justify Lethal Self-Defense Against Incapacitated Batterers?*, 102 Colum. L. Rev. 729, 749 n.109 (2002) (citing 2 Paul Robinson, Criminal Law Defenses § 131(c)(1), at 78 (1984)) (theft and hot pursuit).

208. Crawford v. State, 190 A.2d 538, 541 (Md. 1963) (citing State v. Middleham, 170 N.W. 446 (Iowa 1883); State v. Patterson, 45 Vt. 308 (1873); People v. Coughlin, 35 N.W. 72 (Mich. 1887)) (discussing the generally accepted rule that man has a right to self-defense).

209. *Crawford*, 190 A.2d at 541 (citing Oscar L. Warren, Warren on Homicide 805–06 (1938); *Homicide or Assault in Defense of Habitation or Property*, 25 A.L.R. 508 (1923), People v. Osborne, 115 N.E. 890 (Ill. 1917); Carroll v. State, 23 Ala. 28, 36 (1853); Parrish v. Commonwealth, 81 Va. 1 (1884), People v. Tomlins, 107 N.E. 496 (N.Y. 1914); Pond v. People, 8 Mich. 150 (1860)).

210. *See supra* Part V.A.1.

company assets have been stolen.[211] Nonetheless, this context is one that would be guided by familiar duty, breach, causation (actual and proximate), and harm jurisprudence.[212] Because active defense would only be justified in "hot pursuit," it will be the only attention given as per strictly stolen corporate assets.

3. Attacking the Victim-Company's "Person"

The more difficult issue to grapple with is when dealing with primarily criminal acts, intended to damage or substantially injure a victim's person or third party, and the justification for self-defense in such context in the corporate, cyber-realm. Here the analogy of corporate cyber infrastructure damage requires that we define the "personhood" of a corporate entity, such that a victim company could respond back with active defense countermeasures.[213] Instructive to such a conversation, wherein graver dangers are involved with corporate assets, is the concept of a country's critical infrastructure.[214] Just as an attack against a country's critical infrastructure (i.e., where it threatened the stability and physical safety of a country's citizens) would likely enable a countermeasure to be deployed by a country, here too a company's core corporate assets, which give it economic viability, could be defined as its own critical infrastructure, which if purposefully attacked, could justify a countermeasure — i.e., placing into jeopardy a company's "personhood."

Defining the specific parameters of what would be included as vital corporate assets or critical corporate infrastructure is the topic of future inquires, but at least for purposes of our framework they represent graver forms of attack beyond corporate espionage, which seek to damage the lifeblood of a corporation, and thereby could allow for a proportional countermeasure, self-help.[215] Although critical corporate assets may include possessions directly or indirectly related to the preservation of physical life and limb (e.g., a formula for an important medicine or code to run a power facility for a hospital), they might also include assets that substantially endanger the company's competitiveness (e.g., someone stealing or

211. *Compare* Andrea Shalal-Esa, *Decision on Expanding Cyber Defense Pilot Due in March*, Reuters, Jan. 13, 2012, *available at* http://www.reuters.com/article/2012/01/14/us-cyber-defense-idUSTRE80D02L20120114 (discussing Lockheed Martin Corp.'s recent success in detecting and thwarting a virus), *with* Justin Balthrop et al., *Technological Networks and the Spread of Computer Viruses*, 304 Science, 527, 527–28 (2004) (discussing the effects of viruses that were not immediately detected, notably that the Sobig virus alone caused over $30 billion in damages).

212. Restatement (Second) of Torts § 282 (2005).

213. *See* Pembina Consol. Silver Mining & Milling Co. v. Pennsylvania, 125 U.S. 181, 189 (1888) (stating that there is no doubt that a private corporation is included under the designation of "person").

214. Rausscher & Korotkov, *supra* note 181, at 11–12.

215. *See* Hathaway, *supra* note 160, at 824–30 (differentiating cyberattacks from cyber espionage).

manipulating the Coca-Cola formula) to the point where it may spell a corporation's demise.[216]

a. First-Prong: Assessing the Attack and Determining the Attack Source

Irrespective of the criminal or tort charge, the proposed framework for adequate attribution in the event of recourse is the same. The first prong of analysis requires both an intensive investigation of the attack source and a determination of whether there was a substantial harm caused by the attack and an understanding of the nature of the attack.[217] This requires collecting digital forensics at a technical level to determine how an attack took place, and to define the target of the theft or damage.[218] Understanding the nature of the attack is a key step for a victim company, insofar as it determines the severity of the attack employed and clues as to the intent of the cyber weapon that was employed by an aggressor-company. However, the harm may not be limited to the actual taking or destruction of a vital corporate asset, but may also include the economic or physical effects that might be the foreseeable consequence as well. Once these factors and the sophistication and intent of the cyber weapon used against it have been assessed, it will be the task of the victim-company's operators to determine the source.

In light of painting a "mosaic of responsibility" in this scenario, a technical approach to identifying the source of the attack must include analysis of both the motive of potential corporate competitors and the strategic context for why an attack was triggered in the first place. Herein, the market landscape of industries plays an important role in the determination of attribution. While it is entirely possible that non-economic forces (e.g., reckless hackers) were at work to bring down a victim's company's viability, the probability of such an occurrence needs to be balanced with the probable intent and sophistication involved in the attack.[219] If evidence of an attack source is too mixed and intent indeterminable, then a "good enough" threshold has certainly not been reached and discussion of active defense should be tabled. If, however, evidence can reveal strong indicators of a source, as

216. *See generally* Kenneth M. Siegel, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 Penn St. L. Rev. 779 (2007) (arguing that since technology changes have shifted many aspects of a business from a brick and mortar operation onto the Internet, information is a company's most important asset).

217. See *infra* Parts VI.B.2, IV.B, V for reasons why attribution and determination of harm take primary importance.

218. For commentary in broad agreement with this point, see Kesan & Hayes, *Thinking Through*, *supra* note 66, at 330–33.

219. *See* David P. Leonard, *Character and Motive in Evidence Law*, 34 Loy. L.A. L. Rev. 439, 469 (2001) (discussing motive and reaction in general by stating, "[a] person who has a motive to act is somewhat more likely to have acted than is a person without a motive"); Press Release, Kaspersky Lab, Kaspersky Lab Provides Its Insights on Stuxnet Worm (Sept. 24, 2010), http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm (arguing — prior to later reporting that would clarify the matter — that the worm's sophistication alone helped to indicate that it had a very specific target).

used against a vital corporate asset or where there is a "hot pursuit" scenario of stolen property, then the second prong of inquiry needs to be considered in terms of the type of countermeasure allowed, along with an assessment of the risks and consequences of their use.

b. Second-Prong: Justifying a Counterattack and Interest-Based Analysis

The second prong of the inquiry addresses the other goal of attribution, which is to establish a limiting principle of whether active defense is at all advisable. Assuming, again, that a non-governmental actor is suspected with a strong degree of confidence under the first prong, the analysis of whether to strike back needs to weigh several factors before a counterstrike is made: the ability to make a proportional counterattack, the interests at stake for (i) the victim-company in striking back, (ii) striking back at the alleged aggressor-company, and (iii) the risk level posed by wrongly attributing the strike as against an innocent third party ("innocent-company") or the strain it places on the overall users of the Internet (i.e., system wide effects). Under the totality of the circumstances in this interest-based analysis, if a majority of the factors weighs in favor of a countermeasure, then a victim-company can utilize active defense; if not, then the victim-company must pursue other mechanisms to resolve the issue, including a call to authorities, a lawsuit, or its own corporate diplomacy with its adversaries (i.e., their competitors).

i. Victim-Company Interests

Realizing the substantial nuance involved, in light of ambiguous forensic data or the likely red-herrings of would-be competitors, the balance of interests requires considerable attention. For the interests of the victim-company to allow a countermeasure to be carried out, the corporate asset stolen or damaged would, again, have to be something of critical value to that company (i.e., viewed holistically to include its employees, shareholders, and customers). The victim-company would also need to determine if its interests would be best served by striking back in the first place — a commonsensical restraint — revealing whether it truly had confidence in its own cyber armory to attack back effectively and whether it would achieve an efficacious result to either retake stolen or prevent the (further) damage of stolen corporate assets. Cost and time assessments of attribution analysis or forensic data would also help determine whether countering back makes rational business sense.

ii. Aggressor-Company Interests

In regards to the interests of the alleged aggressor-company, a victim-company must determine whether the value of a countermeasure would send the message of deterrence or desistence to the original attacker. Such interest would also include an

assessment for the market damage that would be caused if a rival were impugned, and the damage it could serve to consumers, overall, when more than one member of an industry is now weakened (e.g., Coca-Cola hacking back at Pepsi to the point where both are unable to serve a thirsty populace). Additionally, interests would need to account for whether an aggressor-company could itself attribute the victim-company's counterattack, and the cost-benefit of risking further escalation of a protracted cyber conflict (i.e., going back and forth).[220]

iii. Innocent-Company Interests

Acknowledging the fact that imperfect certainty will guide attribution decisions, the second prong of the framework requires a serious consideration of the risks, costs, and disruption caused by a countermeasure attack.[221] Naturally, the equation of an innocent-company's involvement in a cyber conflict, represents a grave reality of active defense; however, when approached with the same level of diligence and reasonable apprehension, vis-à-vis, a "mosaic of responsibility," as represented in the first-prong, risks will be minimized to the furthest extent possible. One policy recommendation is that a system of carrying cyber insurance may help alleviate the pressures and worries of misattributed countermeasure activities, helping to make whole innocent-company victims or to repair collateral damage caused by a countermeasure. Such coverage may spark and incentivize victim-companies to make optimal decisions, lest they face steep rises in their coverage premiums. Discrete effects upon third-party Internet users may also be taken into account, where possible, if a countermeasure serves to overwhelm their use of the overall cyber infrastructure as part of their daily activities, i.e., spillover effects that foreseeably disrupt both other innocent-companies and Internet users. Again, the specific penalties or monies to be paid are not the topic of this paper, but simply can be used as guidance.

If an assessment of the second prong weighs in favor of the victim-company's interests, then a company will have established a prima facie justification under the adequate attribution standard to carry through with an active defense operation. This is an important feature of this framework as a signal not only of a well-reasoned technical decision by the victim-company, but also one that has a legal justification if ever brought to court. More importantly, it is an element that makes sense if demanded by a victim-company's shareholders. All things considered, our normative framework is much more of a caution against the use of indiscriminate active defense than it is a boon for its proliferation.

220. Michael Schmitt, *Classification of Cyber Conflict*, 17 J. Conflict & Sec. L. 245, 258 (2012) (describing a protracted conflict as a certain level of intensity and continuity, as opposed to sporadic or isolated incidents).

221. *See* Kesan & Hayes, *Mitigative Counterstriking*, *supra* note 28, at 477–79, 532–33 (describing a few of the risks associated with counterstrikes).

4. Private International Attacks

The next area of inquiry expands the normative framework beyond the confines of a single jurisdiction to highlight the legal and policy implications at work in a strictly private international context. Here, a conflict requires that one non-governmental organization (the "aggressor-company"), based in Country A, takes action against another non-governmental organization (the "victim-company") based in Country B, using only commercial cyber infrastructure, means, and engineering to launch the attacks. As in the domestic context,[222] the model assumes the reason for such an attack in a purely private conflict is primarily economic either: (i) to facilitate the acquisition or espionage of foreign corporate intellectual property (IP), sensitive information, or other physical corporate assets — actionable under civil tort liability or per se illegal under criminal statutes in either country; or (ii) to damage, disrupt, or neutralize "vital corporate assets," that would threaten victim-company's economic viability — implying criminality, either per se under Country A and/or Country B's criminal statutes or common law crime where a mens rea can be established, in addition to civil liability.

Despite the international setting, our framework in this context is largely the same as for a purely domestic attack, as has been explained in the detail above, with two notable additions. Unlike in a domestic conflict, here transmission lines and data over the Internet will cross jurisdictional lines and may further obscure the private versus public infrastructure used to launch a cyberattack. Therefore, one of the critical differences requires that, under the first prong attack and attribution analyses,[223] a victim-company in Country B determine, to its best ability, whether the attack against it from a foreign aggressor-company in Country A was motivated by a purely private reason using primarily commercial cyber infrastructure to launch the attack. Assuming that a rough bifurcation of attack source (i.e., public vs. private) is technically feasible, a further inquiry would be needed to ensure that the reason for the attack was not one to perturb national security or materially affect Country B's public interests.

Similarly, an interest-based analysis as occurs in the second prong would need to be expanded to include not only the interests of the victim-company and aggressor-company, but also the nation-state interests of Country B (i.e., where victim-company is based), the nation-state interests of Country A (i.e., where aggressor-company is based, and the nation-state interests of Country C (i.e., where innocent-company is based). A non-exhaustive list of Country A's concerns would include the protection of domestic private organizations (i.e., victim-company), its enforcement of any domestic legal regimes related to cyberattack, and, specifically, the regulation of the self-help means used in active defense countermeasures by the

222. *See supra* Part V.A.1.
223. *See supra* Part V.A.3.a.

victim-company. Country B's concern would certainly include the protection of its domestic private organizations (i.e., alleged aggressor-company), the enforcement of domestic cyber laws, along with the need to govern the cyber activities of its domestic private organizations, such that they do not affect the public interests or defensive posture of any other country (i.e., Country A or Country C). Country C, on the other hand, represents the interests of a misattributed cyberattack against an innocent-company based in its jurisdiction. As such, it is important that Country C's interests are weighed to both repair and mitigate the innocent-company's damage, as well as in the interest of spurning reckless cyber countermeasures. Country C's interests may additionally represent some of the collateral damage concerns needed to be taken into account when victim-company decides to employ its active defense.

Thus, a review of the attribution framework begins with the first-prong of assessing the international attack and determining the possible sources of the attack. Assuming, as here, that it is of a purely commercial, albeit international, the critical features will need to do the following: (i) satisfy a severity-effects test, such that the attack causes substantial harm to a victim-company's vital corporate assets, in addition to satisfying a determination that the attack was for purely commercial ends, affecting primarily commercial interests; and (ii) be based on a context-based assessment of the attack source, i.e., painting the "mosaic of responsibility," that reflects world geo-political, economic, and cultural issues. The second prong of this framework would again concentrate on justifying a proportionate response based on the type and severity of the attack made and the confidence of the traceback trail to a source. However, added to the interest-based analysis, is an emphasis on weighing the legal implications and interests of the nation-states involved, i.e., of the victim-company (Country B), the alleged aggressor-company (Country A), along with those of a misattributed innocent-company (Country C).

Realizing the practical and technical issues of employing such a comprehensive assessment (and the time-sensitive nature of making a countermeasure determination), our framework recommends a case-by-case analysis of the salient issues be used as between the nation-states and companies involved. With respect to policy considerations, we believe three emerging trends, in particular, will help guide public-private practice related to active cyber defense and attribution: (i) domestic-level cyber laws, i.e., the increased role of cyber statutory regimes in different countries;[224] (ii) international-level cyber law, the rise in cyber-related bilateral/multilateral agreements (e.g., the European Union Convention on Cybercrime) and rule regimes (e.g., NATO's Cooperative Cyber Defence Centre of

224. *See* Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 10 Ox. Int'l. J. Law & Info. Tech. 139, 189 (2012) (mentioning several different action plans and organizations developed in Europe to combat cyberattacks).

Excellence);[225] and (iii) the growing practice of using international commercial arbitration and contractual arrangements to handle disputes between private companies operating under divergent domestic laws.[226]

5. Public-Private International Attacks

The third area of the normative framework's inquiry is perhaps the most complicated, involving both private and public international actors. The reason for the complication is primarily due to the dual-use scenario where private companies are employed or sponsored by nation-states to carry out cyberattacks for non-purely economic goal, and the resulting maelstrom of trying to parse domestic jurisprudence with the long-held rules guiding international laws or armed conflict. Despite the obvious shortcomings of clear, international guidance,[227] we believe there is a suggested path for practitioners and operators to follow, which at the least will be better than without a viable alternative. Fortunately, the private actors involved may relax otherwise more rigid parameters as pronounced in traditional international law as between nation-states. Moreover, a word of caution before applying this normative framework: The authors do not in any way condone vigilante cyber actions to cause cyber conflict between nation-states; however, we wish to acknowledge the growing trend of nation-states contracting with private organizations to carry out their cyber operations, and the resulting abuse that comes with rigid standards of assessing "state responsibility."[228]

Whereas the previous guiding motivations for cyberattacks in the private contexts were premised on purely economic gains, here the motivations expand to consider national-economic interests (i.e., modern mercantilism), political, cultural, and military strategy.[229] Thus, the harm to be inflicted reflects not only on the concepts of "vital corporate assets," such as intellectual property, but can also

225. Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 70 (2009); TALLINN MANUAL, *supra* note 137, at 17.

226. James W. Constable, *International Commercial Arbitration*, MD. B.J., July/August 2010, at 14.

227. *See* Hathaway, *supra* note 160, at 822 (noting that "the law of war regulates only a small subset of cyber-attacks").

228. James A. Lewis, *Thresholds for Cyberwar*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Sept. 2010), http://csis.org/publication/thresholds-cyberwar (highlighting nation-states hiring cyber mercenaries to conduct their operations); *see* TALLINN MANUAL, *supra* note 137, at 46 (finding that a 'use of force' could be attributable to a nation-state if it contracted with a third party under the law of State responsibility); SEE U.S.-CHINA ECON. & SEC. REV. COMM'N, 2012 REPORT TO CONGRESS 9 (2012), *available at* http://www.uscc.gov/annual_report/2012/2012-Report-to-Congress.pdf (reporting that "corporate actors, such as Chinese information technology or telecommunications firms, may . . . operate in cyberspace on the state's behalf"); *see, e.g.*, Stacy Curtin, *Michael Chertoff: Cyberattacks Are The Biggest Risk Facing America*, DAILY TICKER (May 4, 2012, 12:58 PM), http://finance.yahoo.com/blogs/daily-ticker/michael-chertoff-cyberattacks-biggest-risk-facing-america-165803529.html (stating that, in carrying out cyberattacks, "many nations . . . use their intelligence agencies as a way to enable their companies . . . to compete in the marketplace").

229. *See, e.g.*, Gorman, *supra* note 50 (attributing theft of sensitive information on the F-35 fighter jet to China); Leppard, *supra* note 50 (indicating British intelligence confirmation of Chinese involvement).

include matters pertaining to military maneuvering, along with objective and subjective notions of a nation-state's "critical infrastructure," commonly comprised of supervisory control and data acquisition (SCADA) systems over power supplies, facilities vital for the sustenance of a population, and the banking system.[230] Besides, the elevation of harm and public interests involved, the stakes become ever higher as self-defense as allowed by jurisprudence, must adapt a standard at least comprehendible to the U.N. Charter and traditional *jus ad bellum*.

As mentioned previously in the background regarding *jus ad bellum*, this becomes increasingly difficult to accomplish when conflicting views on what brings a cyberattack to the level of an "armed attack," given little practical guidance.[231] We propose instead, a non-exclusive "hybrid approach," combining each of the three prevailing views (i.e., "effects-based," "target-based," and "instrument-based") to arrive at how substantial a cyberattack used by or against a nation-state could be. Considering the relative strengths of these analytical frameworks, none of these, let alone the widely-accepted, effects-based approach of the Schmitt Analysis, can be disregarded. Rather, an effort utilizing a hybrid approach, taking the best from each, does seem workable. This is because none of the approaches actually sets out to be mutually exclusive of the other,[232] and so combining them does not frustrate the purpose or the realities of *jus ad bellum* as observed in each of them. This feature of inclusiveness, despite divergent viewpoints on the meaning and interpretation of Article 51,[233] highlights the ability for each to be combined in a framework together and the validity of a hybrid approach, at least as it pertains to evaluate attribution concerns, and whether a counter cyberattack using active defenses would be allowed.

Under the hybrid approach, any technical operator of a victim-company or victim-country (e.g., CSO/CIO in a private context; U.S. Cyber Command (CYBERCOM)[234] in a public context) would determine if they suffered an "armed attack" if: first, the attack used rose to the level of a use of force under the Schmitt Analysis for its effects;[235] second, if the attack both damaged or substantially

230. *See* Spencer Kelly, *Hackers Outwit Online Banking Identity Security Systems*, BBC News (10 Feb. 2012, 12:54 PM), http://www.bbc.co.uk/news/technology-16812064 (detailing threats to banks); David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times, June 1, 2012, at A1 (describing an attack on SCADA systems).

231. *See* Hathaway, *supra* note 160, at 845 (noting the three different approaches to determining when a cyberattack becomes an armed attack).

232. *Id.* at 845, 848 (giving no indication that the three approaches are mutually exclusive).

233. Tom Ruys, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice 58 (2010).

234. Jeremy Hsu, *U.S. Cyber Command Now Fully Online, and Seeking a Few Good Geeks*, POPSCI (Oct. 10, 2009, 2:29 PM), http://www.popsci.com/military-aviation-amp-space/article/2009-10/us-cyber-command-now-online-and-seeking-few-good-geeks (describing the purposes and functions of CYBERCOM); *U.S. Cyber Command*, U.S. Strategic Command, http://www.stratcom.mil/factsheets/Cyber_Command/ (last updated Dec. 2011).

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

disrupted a victim-country's critical national infrastructure and a victim-company's "vital corporate assets";[236] and third, analogize to the functional characteristics of the cyber weapon employed to surmise if its intended use were to cause the resulting harm (e.g., Stuxnet causing turbines to spin out of control).[237] While the hybrid approach is not without flaws, it presents a manner of approach to the subject, and can help initiate a public-private dialog to inspect how to steer a consequence of attack-value for attribution-sake. Additionally, the hybrid approach allows a counter response; self-help measures to be used where there is something less substantial (i.e., not death or physical destruction) than a traditional "armed attack" but where there is an indication of a coordinated attack taken against certain public-private cyber infrastructure of a victim-company and/or victim-country that suggests that it wants to cause national security disruptions.[238]

Setting up the parameters as we did in the other examples, here again we have victim-company, based in Country B, who is attacked by the aggressor-company, in Country A, with the authorization or support (e.g., technical know-how and/or monetary funding) of Country A, with the intent to damage or substantially disrupt some public interest (i.e., military, economic, political, or cultural) of Country B, as it may be manifest or reflected in victim-company. For instance, if the Chinese government contracted with a private company to take action against the U.S.'s Lockheed Martin to manipulate or prevent the aerospace design and production specifications, it could provide China with an important military and economic advantage.

Given the public-private nuance, additional criteria to the aforementioned framework would need to be added: the first prong would establish (i) whether a cyberattack rose to the level of an "armed attack" under the hybrid approach and (ii) whether there was a strong indication of the attack source, i.e., painting the "mosaic of responsibility" against an aggressor-company and aggressor-country; the second prong would also include (i) a justification for using active defense against an alleged aggressor-company and aggressor-country, balanced against (ii) the interest-based analysis of the important stakeholders, including those of each of the host company countries, along with any innocent-company and/or innocent-country.

Applying the hybrid approach to the analysis: if (i) an attack against a victim-company and/or victim-country has substantial consequences (as measured under a Schmitt Analysis or similar test); (ii) targeted against a company's vital corporate assets and a nation-state's critical infrastructure; (iii) by an cyberattack 'weapon'

236. *See supra* Part V.A.4.

237. *See supra* Part III.B.

238. *See, e.g.*, Harold K. Koh, Legal Advisor to the U.S. State Dept., Remarks at US CYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm [hereinafter Koh Remarks] (arguing that the right of self-defense applies to cyberattack as between nation-states and where private actors act upon the State's instructions or under its direction or control).

that was created/used with that specific intent, then the victim-company in conjunction with a victim-country can rightfully respond back with a proportional counterattack. However, attribution serves as a limiting factor; thus victim-companies must (iv) assess both the confidence of their evidence painting a mosaic of responsibility, and the interests served in a counterattack, as to themselves, as against the aggressor-company and aggressor-country, and any possible considerations for an innocent-company or innocent-country. If in the event that traceback and the "mosaic of responsibility" reveal that a nation-state was indeed involved, we recommend that information-sharing with a third-party international operator or an appropriate authority within the victim-country (e.g., U.S. CYBERCOM) be conducted to determine recourse and the use of a counterattack.

Naturally, technical realities of cyber infrastructure, strategic public-private dealings, and a growing number of domestic cyber legal regimes around the world will begin to cloud what constitutes state action/responsibility versus privately-motivated action.[239] As commentators, such as Shackleford and Andres, observe, there is indeed room for more flexible standards to guide countries, and as we believe that such guidance can be instructive to any operator, including those at private companies.[240] Our framework, therefore, can provide some prediction of how companies can tackle the challenges of operating in an uncertain cyber world and evaluating what their recourse may be, based on attributing a source. Even as cyber regimes and state practice will come to further define this field, certainly our "good enough" standard for adequate attribution reflects the complications and interests involved in making a decision to use active defense countermeasures.

B. Consequences of Incorrect Attribution

As mentioned, a victim-company that deploys active defense measures against an incorrectly attributed target, neutral-company or neutral-country, could face significant legal consequences.[241] The counter-attacking company could be subject to criminal or civil liability under federal and state statutes, international law, or state common law.[242]

Numerous federal statutes make it unlawful to disable or gain unauthorized access to computer systems. For example, the Computer Fraud and Abuse Act (CFAA) makes it unlawful to produce a transmission causing damage to a computer, or to access a computer without authorization to obtain information,

239. *See Cyberwar: War in the Fifth Domain*, Economist, July 2010, at 25, *available at* http://www.economist.com/node/16478792 (noting that it remains unclear whether the cyberattacks against Estonia and Georgia were carried out by state or non-state actors).

240. Scott Shackelford & Richard Andres, *State Responsibility for Cyberattacks: Competing Standard for a Growing Problem*, 42 Geo. J. Int'l L. 972, 999–1000 (2011).

241. *See supra* Part IV.B.

242. *See infra* notes 243–59 and accompanying text.

obtain anything of value by fraud, or cause damage.[243] CFAA violations could subject a company engaging in active defense against the wrong actor to either criminal or civil liability.[244] In addition, the Wiretap Act makes it unlawful to intercept or attempt to intercept wire, oral, or electronic communications.[245] Violators are subject to both criminal and civil liability, and information obtained through violations is not admissible in any U.S. court proceeding.[246] The Stored Communications Act makes it unlawful to access a facility through which an electronic communication service is provided without authorization and thereby obtain, alter, or prevent authorized access to a communication in electronic storage, giving rise to both criminal and civil liability.[247] Each of the above could be implicated in cases of incorrect attribution.

Responses based on mistaken attribution may also violate federal intellectual property law. For example, the Economic Espionage Act makes it a federal crime to knowingly steal or destroy a trade secret.[248] The Digital Millennium Copyright Act makes it unlawful to "circumvent a technological measure that effectively controls access" to a copyrighted work.[249]

If active defense mistakenly targets a foreign nation, the persons responsible may have violated the Neutrality Act.[250] The Neutrality Act makes it unlawful to bring "any military or naval expedition or enterprise" against a foreign state or government with which the United States is at peace.[251] While no court has yet considered whether a cyberattack can constitute a military enterprise, at least some commentators have suggested that the statute ought to be interpreted in such a way.[252]

Misattributed responses could also run afoul of international law. Under the Council of Europe's Convention on Cybercrime, signatory states are obligated to adopt criminal laws making it unlawful to gain unauthorized access to a computer, to intercept electronic transmissions without authorization, to damage or delete computer data without authorization, to sabotage computer systems without

243. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2000); *see* Stewart Baker, *The Hackback Debate*, STEPTOE CYBER L. BLOG (Nov. 2, 2012), http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate (discussing the legality of hacking back under the CFAA with a full account of the dueling views of Stewart Baker and Professor Orin Kerr).

244. *Id.*

245. 18 U.S.C. § 2511 (2006).

246. 18 U.S.C. § 2515 (2006).

247. 18 U.S.C. §§ 2701, 2707 (2006).

248. 18 U.S.C. § 1832 (2006).

249. 17 U.S.C. § 1201 (2006).

250. 18 U.S.C. § 960 (2006).

251. *Id.*

252. Paul Rosenzweig, *The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 245, 261 (2010) (asserting that whether a cyberattack from the private sector constitutes a military expedition is an important question).

authorization, and to use or distribute a device or program for the purpose of committing any of the foregoing crimes.[253] Numerous countries have executed their obligations under the Convention on Cybercrime by enacting compliant laws.[254]

Misattributed countermeasures could also run afoul of U.S. state law. These include laws prohibiting unauthorized access to computers,[255] transmission of malicious code,[256] and installation of spyware.[257] In addition, such tactics could violate state trade secret laws. Furthermore, victims of such countermeasures could prevail under tort causes of action including trespass to chattels[258] and conversion.[259] Curtis Karnow has suggested applying the law of nuisance to cyberattacks, which might permit companies to take some self-help measures against correctly attributed attackers, but courts have not yet adopted this theory.[260]

Another important consideration, even when accurate attribution is made, is how precise of a response is appropriate. For example, should active defense measures be targeted at the attacker's machine, network, enterprise, or ISP? The precision of the response is inversely proportional to the potential for collateral damage. As Curtis Karnow has noted, "intermediate machines, or zombies in a DDoS attack, may be operated by hospitals, governmental units, and telecommunications entities such as Internet service providers that provide connectivity to millions of people."[261] An active defense tactic employed by a U.S.-based accounting firm in 1997 reportedly "took down 75% of the Internet."[262] One commentator argues that active defense measures should not be taken against companies just because single employees have been attributed as attackers.[263]

253. Convention on Cybercrime, Nov. 23, 2001, Eur. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Oct. 26, 2012).

254. *See, e.g.*, The Computer Misuse Act, 1990, c. 18 (U.K.), *available at* http://www.legislation.gov.uk/ukpga/1990/18/contents (last visited Nov. 1, 2012); Lorenzo Picotti & Ivan Salvadori, National Legislation Implementing the Convention on Cybercrime – Comparative Analysis and Good Practices (2008), *available at* http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20%282008%29%20DOC%20National%20legislation%20implementing%20E.PDF.

255. *See, e.g.*, Cal. Penal Code § 502 (West 2011); N.Y. Penal Law §§ 156.00–156.50 (McKinney 2006).

256. *See, e.g.*, Cal. Penal Code § 502(c)(8) (West 2011).

257. *See, e.g.*, Cal. Bus. & Prof. Code §§ 22947–22947.6 (West 2005); 720 ILCS 5/17-52.5. (West 2012).

258. *See, e.g.*, Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996); America Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998) (allowing a victim of cybercrime to make a claim for trespass to chattel).

259. *See* Margae, Inc. v. Clear Link Technologies, LLC, 620 F. Supp. 2d 1284, 1288 (D. Utah 2009) (holding that a the plaintiff had a cognizable claim of conversion after being locked out of its own Internet pages by defendant).

260. Curtis E.A. Karnow, *Launch on Warning: Aggressive Defense of Computer Systems*, 7 Yale J.L. & Tech. 87, 98–102 (2005). Karnow has also argued that such self-help should give rise to "authorization" to take active defense measures under CFAA. *Id.* at 101–02.

261. *Id.* at 93.

262. Winn Schwartau, *Cyber-Vigilantes Hunt Down Hackers*, CNN.com (Jan. 12, 1999 12:19 AM), http://www.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/.

263. Kesan & Hayes, *Thinking Through*, *supra* note 66, at 339.

Because of the potential for harm due to certain active defense measures, which could provoke retaliation and in some cases international conflict, some commentators have suggested requiring companies to seek government approval before initiating them.[264]

VI. Conclusion

Neither active defense nor attribution presents novel policy or technical issues. The security community has been discussing both for quite some time. While a dialog has started to take shape with recent pronouncements by policymakers acknowledging the need to apply traditional notions of self-defense in cyber operations,[265] meaningful guidance has not yet developed that would allow a stakeholder in the commercial community to freely take action that might be necessary to protect itself.[266] In October 2012, then Secretary of Defense Leon Panetta made the bold pronouncement that "[p]otential aggressors should be aware that the United States has the capacity to locate them and hold them accountable for their actions that may try to harm America."[267] Panetta, also commented that traditional self-defense concepts would be part of the "rules of engagement" being finalized by the Department of Defense.[268] However, little has been talked about how the private sector would be impacted, both in helping the government and in terms of helping itself confront attackers.

A part of any such dialog necessarily must include legislative considerations and the effect of the legal landscape on active defense. Although the recent session of Congress was unable to pass any kind of cybersecurity legislation, the underlying principles of some of the bills can provide some guidance as to how Congress might approach the issue of active defense. For example, the so-called "safe harbors" that existed in the SECURE IT Act and provided limited liability for information sharing could be used as a model for providing limited liability in cases where an entity might be under cyberattack.[269] If the victim of such a cyberattack reasonably believed that offensive cyber actions were necessary and such reasonable belief was based on attribution under a framework such as the one described herein, that victim might be afforded some kind of liability protection, particularly if the victim

264. Kesan & Hayes, *Mitigative Counterstriking*, *supra* note 28, at 519.

265. *See* Koh Remark, *supra* note 238; Leon Panetta, Secretary of Defense, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

266. *See* Kenneth Corbin, *Cybersecurity Stalls in Senate, Obama Could Issue Executive Order*, CIO Magazine (Nov. 16, 2012), http://www.cio.com/article/721824/Cybersecurity_Stalls_in_Senate_Obama_Could_Issue_Executive_Order.

267. Panetta, *supra* note 265.

268. Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack*, N.Y. Times, Oct. 12, 2012, at A1.

269. SECURE IT Act of 2012, H.R. 4263, 112th Cong., § 102(g) (2012).

took cyber action against the wrong party. Obviously, any such liability protection would be premised on not only adequate attribution but also appropriate attention to any whitelisting mandates and compliance with conventional rules of engagement (e.g., avoid any kinds of attacks that would harm any kind of critical infrastructure or civilian facilities like hospitals, churches, or schools).

Ultimately, attribution remains a challenging policy issue in the broader context of active defense.[270] Provided that a national policy develops that explicitly permits active defense, an adequate or "good enough" approach to attribution will allow active defenses to be used in a meaningful way instead of remaining in a murky area where fear and uncertainty exist. While risks exist (e.g., using an adequate attribution approach could marginally increase the chances of the wrong party being counterattacked), the resulting protections and clarity of policy make it worthwhile.

270. *See supra* Part IV.