# AN UNSATISFACTORY STATE OF THE LAW: THE LIMITED OPTIONS FOR A CORPORATION DEALING WITH CYBER HOSTILITIES BY STATE ACTORS

*Daniel Garrie*† *& Shane R. Reeves*†

*[F]oreign governments, criminal syndicates and lone individuals are probing our financial, energy and public safety systems every day. Last year, a water plant in Texas disconnected its control system from the Internet after a hacker posted pictures of the facility's internal controls. More recently, hackers penetrated the networks of companies that operate our natural-gas pipelines. Computer systems in critical sectors of our economy—including the nuclear and chemical industries—are being increasingly targeted.*

—President Barack Obama[1]

*We will clearly show it to you at the very time and places* The Interview *be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to. Soon all the world will see what an awful movie Sony Pictures Entertainment has made. The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time.*

—Sony Hackers[2]

---

† Daniel B. Garrie is the Executive Managing Partner for Law & Forensics, a legal consulting firm that works with clients across industries on software, cybersecurity, e-discovery, and digital forensic issues. He is also an accomplished electronic discovery Special Master, hearing disputes throughout the United States. In addition, he is a Partner at Zeichner Ellman & Krause LLP, responsible for the firm's cybersecurity and privacy practice, and an Adjunct Professor of Law at Benjamin N. Cardozo School of Law, specializing in Information Governance.

† Shane R. Reeves is a Lieutenant Colonel in the United States Army. He is an Associate Professor and the Deputy Head, Department of Law, at the United States Military Academy, West Point, New York (shane.reeves@usma.edu). The views expressed here are his personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government. The analysis presented here stems from his academic research of publicly available sources, not from protected operational information.

1 Barack Obama, Opinion, *Taking the Cyberattack Threat Seriously*, WALL ST. J. (July 19, 2012, 7:15 PM), http://www.wsj.com/articles/SB10000872396390444330904577535492693044650.

TABLE OF CONTENTS



[2] David Robb, *Sony Hack: A Timeline*, DEADLINE HOLLYWOOD (Dec. 22, 2014, 1:25 PM), http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/# (quoting the Sony hackers). This is the threat made by the Sony hackers to those theaters willing to show the movie *The Interview*. *Id.*

## INTRODUCTION

On November 24, 2014, a stylized skull with long skeletal fingers flashed on the computer of every employee at Sony Pictures Entertainment.[3] Accompanying the skull was a message stating that a group known as the "Guardians of Peace," or "GOP," had obtained all of Sony's internal data and would release the information unless the studio cancelled a soon-to-be released comedy titled *The Interview*.[4] Within a few days it became apparent that North Korea, angered by the movie's far-fetched plot to assassinate dictator Kim Jong-un, was responsible for the cyber hostility.[5] As Sony continued with plans to release the movie, embarrassing emails, sensitive financial information, and valuable intellectual property began to be widely disseminated on the Internet.[6] The incident significantly escalated on December 16, 2014 when North Korea threatened violence against theaters screening the movie.[7] In response, and in a rare move, the United States publically attributed both the hacking of Sony and the threats to North Korea.[8] On February 19, 2015, the head of the National Security Agency (NSA) removed any doubts about North Korean involvement and openly identified the state as the source of the cyber hostilities.[9]

State-sponsored cyber hostilities against corporations are not a new occurrence. Recent examples include the August 2014 Russian hack of JPMorgan Chase,[10] and the continuous cyber activities against corporate targets conducted by Unit 61398 of China's People's Liberation Army.[11]

---

3 *Id.*

4 *Id.*

5 *See, e.g.*, David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES (Dec. 17, 2014), http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=1.

6 Robb, *supra* note 2.

7 *Id.*

8 Sanger & Perlroth, *supra* note 5.

9 Mike De Souza, *NSA Chief Says Sony Attack Traced to North Korea After Software Analysis*, REUTERS (Feb. 19, 2015, 4:26 PM), http://www.reuters.com/article/2015/02/19/us-nsa-northkorea-sony-idUSKBN0LN27Y20150219.

10 *See, e.g.*, Michael Riley & Jordan Robertson, *FBI Said to Examine Whether Russia Tied to JPMorgan Hacking*, BLOOMBERG (Aug. 27, 2014, 5:04 PM), http://www.bloomberg.com/news/articles/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking ("Russian hackers attacked the U.S. financial system in mid-August, infiltrating and stealing data from JPMorgan Chase & Co. . . . .").

11 *See, e.g.*, Frank Langfitt, *U.S. Security Company Tracks Hacking to Chinese Army Unit*, NPR (Feb. 19, 2013, 4:00 AM), http://www.npr.org/2013/02/19/172373133/report-links-cyber-attacks-on-u-s-to-chinas-military (discussing the link between Unit 61398 and cyberattacks on dozens of American companies). Hackers affiliated with the Chinese government are considered the most energetic and aggressive international actors. *See, e.g.*, Craig Timberg, *Vast Majority of Global Cyber-Espionage Emanates from China, Report Finds*, WASH. POST (Apr. 22, 2013), http://www.washingtonpost.com/business/technology/vast-majority-of-global-cyber-

However, North Korea's actions against Sony are considered by many to be a "game changer" and a significant escalation of the cyber hostilities targeting corporations.[12] Rather than hacking Sony to steal corporate secrets or disrupt its business activity, North Korea attempted to devastate the company and chill its activities for a perceived nationalist slight. This targeting of a corporation for ideological reasons by a state actor should not be viewed as an anomaly; rather, it is best seen as the harbinger of a new era of particularly pernicious cyber hostilities targeting businesses.[13]

The rapidly increasing willingness of state actors to conduct hostile cyber operations against corporations has not gone unnoticed by governments, and, in particular, the United States.[14] Corporations, for their part, overwhelmingly support government involvement in cyber issues.[15] This mutual desire for a corporate-government partnership provides an opportunity to build an effective response to the cyber threat posed by state actors. Yet, corporations also must be cognizant that the present environment is woefully inadequate at providing the necessary cyber defense mechanisms needed to protect their businesses.[16] This short-term need for protection coupled with the interest in a corporate-government partnership raises two questions. First, what can a corporation do to protect itself from state-sponsored cyber hostilities? Second, what are some possible models for a corporate-government partnership to address the threat in the future?

---

espionage-emanates-from-china-report-finds/2013/04/22/61f52486-ab5f-11e2-b6fd-ba6f5f26d70e_story.html (reporting that of 120 incidents of government cyber espionage, ninety-six percent came from China).

12 Kenneth Corbin, *Sony Hack Is a Corporate Cyberwar Game Changer*, CIO (Jan. 19, 2015, 11:01 AM), http://www.cio.com.au/article/564154/sony-hack-corporate-cyberwar-game-changer ("North Korea's state-sponsored attack against Sony is a dramatic escalation in cyber hostilities.").

13 *See, e.g.*, DANIEL GARRIE & MITCHELL SILBER, CYBER WARFARE: UNDERSTANDING THE LAW, POLICY, AND TECHNOLOGY 5–6 (2014) (discussing various cyber hostilities against corporations by state actors).

14 *See, e.g.*, *The White House Summit on Cybersecurity and Consumer Protection*, WHITEHOUSE.GOV (Feb. 13, 2015), http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit (discussing the 2015 cybersecurity summit to "bring together leaders from across the country who have a stake in this issue—industry, tech companies, law enforcement, consumer and privacy advocates, law professors who specialize in this field, and students—to collaborate and explore partnerships that will help develop the best ways to bolster our cybersecurity").

15 GARRIE & SILBER, *supra* note 13, at 5–6 (noting that in a survey given by the Journal of Law and Cyber Warfare to hundreds of businesses across nearly eighty industries that corporations desperately want government involvement and protection from cyber hostilities).

16 A common complaint by private industry is the lack of government response to cyber hostilities. *See, e.g.*, Paul Rosenzweig, *The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government*, HERITAGE FOUND. (May 24, 2012), http://www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government.

This Article addresses both of these questions by first outlining why it is difficult for a corporation to respond to state-sponsored cyber hostilities. Understanding this difficulty allows for the development of appropriate corporate responses to hostile state actors. An explanation of what the law allows a corporation to do in defense of its business interests will follow. As self-protection for business is only a partial solution, recommendations for enhancing the corporate-government partnership to blunt state actor cyber hostilities will also be offered. The Article concludes by reiterating the criticality of developing a comprehensive and coherent strategy for responding to this ever-growing threat.

## I. CORPORATE DIFFICULTIES IN RESPONDING TO A CYBER THREAT: A BRIEF OVERVIEW

### A. *Cyber Crime or Cyber War?*

To understand the difficulties in developing a corporate response to state-sponsored cyber hostilities,[17] it is important to first provide some background and context. The ambiguity of cyberspace makes the demarcation between cyber war and cyber crime unclear.[18] States, nonstate actors, and criminal groups regularly engage in malicious cyber activities which eschew easy classification,[19] as subtle differences are often all that separate cyber crime, espionage, terrorism, and "hacktivism" from cyber war.[20] Cyber crime, in its most simple distillation, is characterized as a crime which involves "the use of a computer-based means to commit an illegal act."[21] Cyber criminals develop and use various tools that "delve deeply and covertly into

17 There are different types of cyber hostilities that target corporations, and two of the most common types of malware are viruses and worms. *See generally What Is the Difference: Viruses, Worms, Trojans, and Bots?*, CISCO, http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html (last visited Mar. 3, 2016). Within malware there is a range of threats, including: honeypots, spyware, Trojan horses, and zero-day exploits and backdoors. *See generally id.*; *see also* GARRIE & SILBER, *supra* note 13, at 311–17 (defining these various threats). It is outside the scope of this Article to discuss the technical aspects of each of these cyber threats.

18 *See* CLAY WILSON, CONG. RESEARCH SERV., RL32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 1 (2008).

19 *See* Scott J. Shackelford, Essay, *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012*, 64 STAN. L. REV. ONLINE 106, 107 (2012).

20 *See* Tony Bradley, *When Is a Cybercrime an Act of Cyberwar?*, PCWORLD (Feb. 20, 2012, 6:32 AM), http://www.pcworld.com/article/250308/when_is_a_cybercrime_an_act_of_cyberwar_.html.

21 Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 834 (2012); Gary D. Solis, *Cyber Warfare*, 219 MIL. L. REV. 1, 2–3 (2014).

public, commercial, and private networks,"[22] and are motivated, for the most part, by financial gain. According to Interpol, "[c]ybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide."[23] Interpol goes on to note that though "there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of Internet-related crime."[24] These are "advanced cyber crime (or high-tech crime)"—defined as "sophisticated attacks against computer hardware and software"—and "cyber-enabled crime"—defined as "'traditional' crimes," such as "crimes against children, financial crimes and even terrorism."[25]

In contrast, the sine qua non of cyber espionage is gathering intelligence—governmental, corporate, or individual[26]—and generally involves stealing trade secrets, intellectual property, and confidential government information. Despite a military nexus, and the "real and serious threat[]" that cyber espionage poses to states, cyber espionage by and large does not trigger "application of the international law on uses of force," but rather requires a domestic or international criminal legal response.[27]

Cyber terrorism and "hacktivism," two closely related terms, are also commonly used in describing hostile cyber practices. Cyber terrorism is "the intimidation of civilian enterprise through the use of high technology to bring about political, religious, or ideological aims, actions that result in disabling or deleting critical infrastructure data or

---

22 *See* CHRIS C. DEMCHAK, WARS OF DISRUPTION AND RESILIENCE: CYBERED CONFLICT, POWER, AND NATIONAL SECURITY 8 (2011).

23 *Cybercrime*, INTERPOL, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (last visited Mar. 3, 2016).

24 *Id.*

25 *Id.*

26 The Tallinn Manual defines cyber espionage narrowly as "any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather . . . information." TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 193 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]. The Tallinn Manual was developed to provide a framework to governments for understanding how cyber operations and cyber warfare may affect their nations. *See, e.g.*, Jeremy Kirk, *Manual Examines How International Law Applies to Cyberwarfare*, ITWORLD (Sept. 3, 2012), http://www.itworld.com/article/2720628/it-management/manual-examines-how-international-law-applies-to-cyberwarfare.html (noting that the Cooperative Cyber Defense Center of Excellence, which "assists NATO with technical and legal issues associated with cyberwarfare-related issues," created the Tallinn Manual to address a variety of cyber legal issues). "The *Tallinn Manual* examines the international law governing 'cyber warfare'" and "encompasses both the *jus ad bellum* . . . and the *jus in bello*." TALLINN MANUAL, *supra*, at 4.

27 TALLINN MANUAL, *supra* note 26, at 4.

information."[28] A "hacktivist," on the other hand, is a "private citizen who on his or her own initiative engages in hacking for, inter alia, ideological, political, religious, or patriotic reasons."[29] Both of these activities can cause significant damage to a state.[30] Whether cyber terrorism or "hacktivism" constitute a cyber attack—described as "a cyber operation, . . . offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[31]—or are more akin to cyber criminality, is far from certain.[32]

The boundaries between cyber crime, cyber espionage, cyber terrorism, and "hacktivism," whether compared individually or as a group to cyber warfare, are nebulous and amorphous. The "lack of agreed-upon definitions, criteria, and thresholds for application," coupled with "the rapidly changing realities of cyber operations,"[33] make it very difficult to determine who should respond to cyber hostilities and how that response should be tailored. In most cases, if it is determined that a hostile cyber activity occurs "below the level of a 'use of force' (as this term is understood in the *jus ad bellum*),"[34] law enforcement will respond and rely upon domestic law to guide their actions.[35] In contrast, when it is clear that military operations are conducted to deny an enemy force the effective use of cyberspace systems in an armed conflict, and when those operations include cyber attacks, cyber defenses, or cyber enabling actions, the malicious activities are properly considered acts of

---

28 William L. Tafoya, *Cyber Terror*, FED. BUREAU INVESTIGATION (Nov. 2011), https://leb.fbi.gov/2011/november/cyber-terror.

29 TALLINN MANUAL, *supra* note 26, at 259.

30 *See, e.g.*, Nicole Perlroth, *Anonymous Attacks Israeli Web Sites*, N.Y. TIMES: BITS (Nov. 15, 2012, 12:51 PM), http://bits.blogs.nytimes.com/2012/11/15/anonymous-attacks-israeli-web-sites; Michael Rundle, *'Anonymous' Hackers Declare Cyber War On North Korea, Claim Internal Mail System Hacked*, HUFFINGTON POST U.K. (Apr. 4, 2013, 9:24 AM), http://www.huffingtonpost.co.uk/2013/04/04/anonymous-hackers-declare-war-north-korea_n_3012451.html.

31 TALLINN MANUAL, *supra* note 26, at 106. A cyber attack may also include "defending and attacking information and computer networks, as well as denying an adversary's ability to do the same," as well as offensive information operations mounted against an adversary in order to dominate cyberspace. STEVEN A. HILDRETH, CONG. RESEARCH SERV., RL30735, CYBERWARFARE 1 n.3 (2001).

32 *See* TALLINN MANUAL, *supra* note 26, at 4–5.

33 *Id.* at 42.

34 *Id.* at 4. See *infra* text accompanying note 141 for a definition of *jus ad bellum*.

35 The Tallinn Manual notes that such threats "have not been addressed in any detail." TALLINN MANUAL, *supra* note 26, at 4. However, it is generally accepted that in situations where an armed disturbance does not reach the level of a conflict, or is not considered a "use of force," domestic law applies. *See* ADVISORY SERV. ON INT'L HUMANITARIAN LAW, INT'L COMM. OF THE RED CROSS, WHAT IS INTERNATIONAL HUMANITARIAN LAW? (2004), http://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf ("International humanitarian law applies only to [international or noninternational] armed conflict; it does not cover internal tensions or disturbances such as isolated acts of violence. The law applies only once a conflict has begun, and then equally to all sides regardless of who started the fighting.").

cyber warfare.[36] Cyber warfare triggers "the international law governing the resort to force by States as an instrument of their national policy," the Law of Armed Conflict,[37] and the associated risks of traditional hostilities.[38]

### B. *Other Problems for Corporations in Cyberspace: Attribution and Hostile State Actors*

Deciding on how best to respond to cyber hostilities is further complicated by the extreme difficulty of attributing an action in cyberspace to a particular actor. In situations where cyber hostilities target corporations it is impossible to know the complete extent to which these cyber hostilities are affiliated with state actors.[39] Cyber hostilities executed for the benefit of a state are often put into action by citizens, and it can be difficult to determine the state's role in the attack. The problem of attribution is, therefore, a pervasive issue throughout all kinds of cyber hostilities, but can be especially troublesome in the context of state actors.[40] While it is undoubtedly challenging to definitively identify the nefarious in cyberspace, what is certain is that state actors are increasingly developing cyber capabilities to use in their conflicts.[41] For example, in the last ten years interstate cyber hostilities

---

36 *DOD Cyberspace Glossary*, PC MAG. ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia/term/62535/dod-cyberspace-glossary (last visited May 21, 2015).

37 TALLINN MANUAL, *supra* note 26, at 4.

38 *See* Philippa Trevorrow et al., *Defining the Issues*, *in* CYBERWAR, NETWAR AND THE REVOLUTION IN MILITARY AFFAIRS 3 (Edward Halpin et al. eds., 2006) (discussing how modern societies are, for the most part, highly dependent on the continuous flow of information); Michael McCaul, *Hardening Our Defenses Against Cyberwarfare*, WALL ST. J., Mar. 6, 2013, at A19 ("Digital networks could be used as a conduit to gas lines, power grids and transportation systems to silently deliver a devastating cyberattack to the U.S.").

39 *See, e.g.*, U.S. CYBER CONSEQUENCES UNIT, OVERVIEW BY THE US-CCU OF THE CYBER CAMPAIGN AGAINST GEORGIA IN AUGUST OF 2008, at 3 (2009), http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf (discussing the Russia-Georgia conflict and noting "[t]he cyber attacks included many different actions in many different locations by many different people").

40 *See generally* GARRIE & SILBER, *supra* note 13, at 19–40.

41 *See, e.g.*, *Hearing Before the S. Armed Servs. Comm.*, 113th Cong. 7 (2014) (statement of Michael T. Flynn, Director, U.S. Defense Intelligence Agency) ("Annual Threat Assessment"), http://www.armed-services.senate.gov/imo/media/doc/Flynn_02-11-14.pdf ("As other nations develop military cyber warfare doctrine and cyber forces, we know they will cultivate tactics, techniques, tools, capabilities, and procedures to threaten our technological superiority. It is imperative that we understand the adversaries' intent and capabilities."); Ron Kelson et al., *The 'Cyber War' Era Began Long Ago*, SECURITY AFF. (June 25, 2012), http://securityaffairs.co/wordpress/6776/security/the-cyber-war-era-began-long-ago.html (stating that more than 140 countries have cyber weapon development programs).

have occurred in Estonia,[42] Georgia,[43] Iran,[44] and the Ukraine.[45] This escalation in state-sponsored cyber hostilities has not gone unnoticed by international actors, including the United States. In 2010, in recognition of this new threat, William J. Lynn, U.S. Deputy Secretary of Defense, stated: "as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare . . . [which] has become just as critical to military operations as land, sea, air, and space."[46]

Even more disconcerting for corporations is the growing willingness of state actors to use their cyber capabilities against private companies. States such as China,[47] Iran,[48] and North Korea[49] have

42 *See, e.g.*, Kertu Ruus, *Cyber War I: Estonia Attacked from Russia*, EUR. INST. (2008), http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia (providing an overview of the conflict some consider to be the first instance of cyberwar); *see also* Scheherazade Rehman, *Estonia's Lessons in Cyberwarfare*, U.S. NEWS & WORLD REP. (Jan. 14, 2013, 3:34 PM), http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare ("[Estonia] had a hard time getting anyone to believe that this was a 'real war' and not a cybernuisance. In the end no one came to help the Estonians but what that alarm did do was to put global cyberattacks on the warfare discussion table for . . . NATO.").

43 *See, e.g.*, David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS J. (Jan. 6, 2011), http://www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf; *see also* Gregg Keizer, *Russian Hacker 'Militia' Mobilizes to Attack Georgia*, NETWORK WORLD (Aug. 12, 2008, 1:00 AM), http://www.networkworld.com/news/2008/081208-russian-hacker-militia-mobilizes-to.html ("Anyone picking a political fight with Russia today can now expect to deal with multiple forms and sources of electronic attack; not only from the Russian military, but also from the Russian government's unofficial civilian hacker assets." (quoting iDefense director of intelligence Rick Howard)).

44 A virus known as Stuxnet was used to damage Iranian nuclear facilities. *See* David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM (Feb. 26, 2013, 2:00 PM), http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet; *see also* Mark Clayton, *Stuxnet Malware Is "Weapon" Out to Destroy . . . Iran's Bushehr Nuclear Plant?*, CHRISTIAN SCI. MONITOR (Sept. 21, 2010), http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant (noting that German cybersecurity researcher Ralph Langner describes Stuxnet as a "military-grade cyber missile").

45 Ukraine has been involved in two major conflicts involving cyber hostilities as of this writing. In December 2015, a Ukrainian power plant was the target of a cyberattack that caused a massive blackout. *See* Evan Perez, *U.S. Investigators Find Proof of Cyberattack on Ukraine Power Grid*, CNN (Feb. 3, 2016, 8:00 PM), http://www.cnn.com/2016/02/03/politics/cyberattack-ukraine-power-grid. Cyber hostilities also played a large role in the 2014 conflict between Russia and Ukraine. *See, e.g.*, Mark Clayton, *Massive Cyberattacks Slam Official Sites in Russia, Ukraine*, CHRISTIAN SCI. MONITOR (Mar. 18, 2014), http://www.csmonitor.com/World/Passcode/2014/0318/Massive-cyberattacks-slam-official-sites-in-Russia-Ukraine.

46 Pierluigi Paganini, *Nation State Sponsored Attacks: The Offensive of Governments in Cyberspace*, SECURITY AFF. (Nov. 12, 2012) (alteration in original), http://securityaffairs.co/wordpress/10203/security/nation-state-sponsored-attacks-the-offensive-of-governments-in-cyberspace.html (quoting William J. Lynn, U.S. Deputy Secretary of Defense).

47 In 2011, China was found to be responsible for cyber hostilities against seventy-two organizations around the world, including: the Association of Southeast Asian Nations (ASEAN); the International Olympic Committee (IOC); the World Anti-Doping Agency; NASA; the New York Times; Coca-Cola; Google; Intel; several multinational oil companies; various defense contractors; and an array of other private companies. *See* Jim Finkle, *"State*

demonstrated a complete disregard for corporate rights and repeatedly target the digital assets of private businesses. The motivation for these state-sponsored hostile cyber activities run the gamut from attempting to gain economic advantages through theft of intellectual property to intimidating corporations through acts of terrorism.[50] To be sure, state actors are not the only perpetrators of cyber hostilities against corporations, and the damage to a company by hostile cyber activities, regardless of origin, can be devastating.[51] However, the cyber exploitation of corporations by state actors is particularly troubling as this is quickly becoming the new normal in international relations.

### C. *Foundations for a Legal Response*

Categorizing a particular cyber hostile act and attributing it to an identifiable source are immense obstacles for a corporation attempting to craft an appropriate legal response. One of the traditional characteristics of cyber hostilities is anonymity.[52] This fact alone makes hostile cyber activities an exceedingly attractive option for those actors seeking to do anonymous damage to a state or private entity.[53] However,

*Actor" Behind Slew of Cyber Attacks*, REUTERS (Aug. 3, 2011, 7:17 PM), http://www.reuters.com/article/us-cyberattacks-idUSTRE7720HU20110803. Additionally, in 2014, the Chinese military was found to be responsible for hacking several American companies. *See* Ashley Fantz, *Chinese Hackers Infiltrated U.S. Companies, Attorney General Says*, CNN (May 19, 2014, 6:31 PM), http://www.cnn.com/2014/05/19/justice/china-hacking-charges.

48 *See, e.g.*, Thom Shanker & David E. Sanger, *U.S. Suspects Iran Was Behind a Wave of Cyberattacks*, N.Y. TIMES (Oct. 13, 2012), http://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html?_r=0; *see also* Benjamin Elgin & Michael Riley, *Now at the Sands Casino: An Iranian Hacker in Every Server*, BLOOMBERG (Dec. 12, 2014, 3:48 PM), http://www.bloomberg.com/bw/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.

49 *See* Sanger & Perlroth, *supra* note 5.

50 *See generally* CATHERINE A. THEOHARY & JOHN W. ROLLINS, CONG. RESEARCH SERV., R43955, CYBERWARFARE AND CYBERTERRORISM: IN BRIEF (2015), http://fas.org/sgp/crs/natsec/R43955.pdf (describing cyber terrorism and noting that there are currently no legally binding instruments that explicitly regulate interstate relations in cyberspace).

51 This Article examines the issues companies confront when dealing with state-sponsored cyber hostilities. However, the damage to corporations by cyber criminals and nonstate cyber groups can be significant, as illustrated by the February 2015 hack of Anthem Incorporated Insurance Company. *See, e.g.*, Susanna Kim, *Anthem Cyber Attack: 5 Things that Could Happen to Your Personal Information*, ABC NEWS (Feb. 5, 2015, 11:37 AM), http://abcnews.go.com/Business/anthem-cyber-attack-things-happen-personal-information/story?id=28747729 (noting that over eighty million personal records were exposed, including those of children and noncustomers).

52 *See* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1014 (2010).

53 *See* David Wallace & Shane R. Reeves, *The Law of Armed Conflict's "Wicked" Problem: Levée en Masse in Cyber Warfare*, 89 INT'L L. STUD. 646, 666–67 (2013) (discussing the attractive traits of cyber warfare for actors looking for anonymity).

as demonstrated by North Korea, attribution is less of a problem when a state conducts hostile cyber operations against a corporation for ideological purposes. As these hostile acts are intent on "punishing" the corporation for its behavior, they are often poorly veiled or even openly advertised by the offending state.[54]

Attribution, when verbally declared, is therefore not the difficulty in these philosophically-driven state-actor cyber hostilities against a corporation. Further, even in circumstances where a state desires to remain anonymous, its hostile cyber acts are often exposed.[55] Complications arise instead in determining the appropriate legal response to the state actor's cyber tactic. While, as explained above, differentiation between various cyber activities is often difficult, it is imperative for an appropriate response.[56] In practice, labeling a cyber act may be possible only by discerning the goals and motives underlying the activity. However this determination is made, understanding whether the hostile state's cyber activity is a criminal act, an act of war, or somewhere in between may trigger different responses from both the victimized corporation and its host state. It is therefore important to understand what domestic and international law allows a corporation to do, and not do, in response to a state actor's hostile cyber activities.

---

54 While North Korea publicly denies hacking into Sony, it consistently praises the action and implicitly takes credit for the damage. *See, e.g.*, Jon Fingas, *North Korea Denies Hacking Sony Pictures, but Likes that Someone Did*, ENGADGET (Dec. 7, 2014), http://www.engadget.com/2014/12/07/north-korea-denies-hacking-sony-pictures.

55 *See, e.g.*, Charles Arthur, *Chinese Cyber-Attacks 'Pinned to Users'*, GUARDIAN (Dec. 12, 2011, 2:38 AM), http://www.theguardian.com/technology/2011/dec/12/china-us-hacking-tensions.

> The aggressive, but stealthy attacks, which steal billions of dollars' worth of intellectual property and data, often carry distinct signatures allowing US officials to link them to certain hacker teams. Analysts say the US often also gives the attackers unique names or numbers, and at times can tell where the hackers are and even who they may be.

*Id.* However, this is not to say that attribution is easy. It is important to keep in mind the difficulties of finding certainty as to the source of cyber hostilities and to avoid jumping to conclusions that could have dangerous consequences. For more discussion on the consequences of misattribution, see Shane McGee et al., *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1, 43–46 (2013) (describing the various domestic and international legal consequences that can result from responding to cyber hostilities that have been misattributed).

56 *See supra* notes 17–38 and accompanying text.

## II. DOMESTIC LAW: U.S. LEGAL DOCTRINE AVAILABLE TO CORPORATIONS FACING CYBER HOSTILITIES

### A. *Overview*

The federal government's role in tackling cybersecurity involves securing both public and private systems. While there is no overarching legal doctrine available to inform private corporations, there are a litany of federal statutes addressing different aspects of cybersecurity.[57] In fact, companies contending with hostilities perpetrated by state actors cannot look to a comprehensive domestic framework for a remedy, but rather must be familiar with the myriad of statutes that touch on cybersecurity.[58]

Currently, federal computer crime statutes criminalize, inter alia: accessing computers without authorization; causing damage via a program or code (such as a virus); stealing electronically stored trade secret information; and unauthorized use of an electronic means of identification.[59] The language of these statutes, for the most part, is broad and a point of debate as to interpretation.[60] Moreover, "it is

---

57 *See generally* ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBER SECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS (2013), http://fas.org/sgp/crs/natsec/R42114.pdf. Over the last decade there has been a great deal of discussion within the legislature about reforming federal cybersecurity statutes. Many bills have been proposed but few have been enacted. *See, e.g.*, Cybersecurity Enhancement Act of 2013, H.R. 756, 113th Cong. (2013) (unenacted); Cybersecurity Act of 2012, S. 3414, 112th Cong. (2012) (same); Cybersecurity Act of 2010, S. 773, 111th Cong. (2009) (same). Only recently has there been any substantial movement with federal cyber statutes with the enactment of the Cybersecurity Enhancement Act of 2014, the most significant cybersecurity statute to be enacted since 2002. Pub. L. No. 113-274, 128 Stat. 2971 (codified as amended in scattered sections of 15 U.S.C.); *see infra* Section II.C.6.

58 The Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848, for example, was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute) that extended government restrictions on wiretaps from telephone calls to include transmissions of electronic data by computer, 18 U.S.C. §§ 2510–2522 (2012), and added new provisions prohibiting access to stored electronic communications, such as the Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2712 (2012). The ECPA has since been amended by the Communications Assistance for Law Enforcement Act (CALEA) of 1994, 47 U.S.C. §§ 1001–1010 (2012), the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006), and the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436. Rather than address the cyber-related aspects of wiretap statutes separately, Congress decided to integrate these provisions into the existing statutes. This is perhaps due to the particular importance Congress saw in striking a balance between privacy rights and the needs of law enforcement with respect to data shared or stored by electronic and telecommunications services. *See* FISCHER, supra note 57, at 33–35.

59 18 U.S.C. §§ 1028, 1030, 1831–1839 (2012).

60 *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); Orin S. Kerr, *Cybercrime's Scope:*

difficult—if at all possible—to predict a priori the ways in which criminals will attempt to misuse computers and the Internet."[61]

In the private sector, federal statutes relating to cybersecurity are typically industry-specific and create general standards. In addition, the majority of these cybersecurity statutes are directed at health care entities and financial institutions.[62] Again, while statutes were recently passed to facilitate private-public cooperation in establishing cybersecurity standards across critical infrastructure industries,[63] they do not establish a comprehensive regulatory framework. The following is a summary of some of the notable federal cyber crime and cybersecurity provisions.

## B. *Cyber Crime Provisions*

### 1. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA), enacted in 1986, is the federal statute under which computer crimes are prosecuted. It expanded the scope of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, which had established criminal penalties for unauthorized access and use of computers and networks.[64] Since

*Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003); Charlotte Decker, Note, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959 (2008); Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81 (2013).

61 David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 948 (2013).

62 Federal statute permits various regulatory agencies to issue cybersecurity regulations over private sector entities, but some agency officials feel that issuing regulations could be counterproductive. *See, e.g.*, PAUL W. PARFOMAK, CONG. RESEARCH SERV., R42660, PIPELINE CYBERSECURITY: FEDERAL POLICY 7–8 (2012).

> TSA officials assert that security regulations could be counterproductive because they could establish a general standard below the level of security already in place at many pipeline companies based on their company-specific security assessments. Because TSA believes the most critical U.S. pipeline systems generally meet or exceed industry security guidance, the agency believes it achieves better security with voluntary guidelines, and maintains a more cooperative and collaborative relationship with its industry partners as well.

*Id.*

63 15 U.S.C. § 272(c)(15) (2012); *see also infra* Section II.C.6 (discussing the 2014 Cybersecurity Enhancement Act).

64 *See generally* Shawn E. Tuma, "*What Does CFAA Mean and Why Should I Care?*"*—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141 (2011) (tracing the evolution of the statute from the narrow scope of its infancy to the catchall provisions of today and the complications that can arise).

1986, the CFAA has been amended multiple times and it now criminalizes a broad range of computer-related activities including: obtaining information by accessing a protected computer without authorization;[65] causing damage to a protected computer or its data by the transmission of a program or code;[66] and trafficking in stolen computer passwords.[67] However, the CFAA does not define "without authorization," causing a circuit split on how to interpret this key aspect of the statutory provision.[68] Moreover, the CFAA extends to any machine connected to the Internet, as it defines "protected computer" broadly to include any device "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[69] As to "damage," the CFAA is also broadly interpreted to include "any

---

65 The CFAA punishes anyone who:

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (A) information contained in a financial record of a financial institution, or of a card issuer . . . , or contained in a file of a consumer reporting agency on a consumer . . . . ;
>
> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer . . . .

18 U.S.C. § 1030(a) (2012).

66 The CFAA punishes anyone who:

> (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

*Id.*

67 The CFAA punishes anyone who:

> (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—
>
> (A) such trafficking affects interstate or foreign commerce; or
>
> (B) such computer is used by or for the Government of the United States . . . .

*Id.*

68 *See generally* Warren Thomas, Note, *Lenity on Me:* LVRC Holdings LLC v. Brekka *Points the Way Toward Defining Authorization and Solving the Split Over the Computer Fraud and Abuse Act*, 27 GA. ST. U. L. REV. 379 (2011).

69 18 U.S.C. § 1030(e)(2)(B).

impairment to the integrity or availability of data, a program, a system, or information."[70]

### 2. The Economic Espionage Act of 1996

The Economic Espionage Act of 1996 criminalizes the theft of trade secret information, including electronically stored information, provided that "reasonable measures" have been taken to keep it secret.[71] The statute treats the theft of trade secrets by or for foreign entities separately from domestic entities, labeling as "economic espionage" the theft of trade secrets that "will benefit any foreign government, foreign instrumentality, or foreign agent," and assigning it more severe penalties.[72] It also authorizes civil proceedings by the Department of Justice to enjoin violations of the Act.[73]

### 3. The Identity Theft and Assumption Deterrence Act of 1998

The Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime, provided penalties, and directed the Federal Trade Commission to document and refer complaints.[74] Inter alia, the Act criminalizes unauthorized productions, transfers, possessions, and unlawful uses of identification documents or any means of identification. The Act defines identification broadly to encompass various data elements such as social security numbers, dates of birth, and "unique biometric data" and any "unique electronic identification number, address, or routing code."[75]

### 4. The Stored Communications Act

The Stored Communications Act (SCA) 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.[76] For the most part, the SCA does not allow Internet Service Providers (ISPs) to

---

70 *Id.* § 1030(e)(8).
71 18 U.S.C. § 1839(3) (2012).
72 *Id.* § 1831(a).
73 *Id.* § 1836.
74 18 U.S.C. § 1028.
75 *Id.* § 1028(d)(7).
76 18 U.S.C. §§ 2701, 2707 (2012).

"divulge to any person or entity the contents of any communication which is carried or maintained on that service."[77] The SCA targets two types of online service: "electronic communication service[s]," which it defines as "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[78] and "remote computing service[s]," which is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[79]

### C. *Notable Federal Statutes with Cybersecurity Language*

#### 1. The Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the Secretary of Health and Human Services (HHS) to establish security standards and regulations for protecting the privacy of individually protected health information, and obligates healthcare entities to protect the security of such information.[80] Protected health

---

77 *Id.* § 2702(a)(2).

78 *Id.* § 2510(15).

79 *Id.* § 2711(2).

80 The regulation provides:

> (a) General requirements. Covered entities . . . must do the following:
>
> > (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
> >
> > (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
> >
> > (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
> >
> > (4) Ensure compliance with this subpart by its workforce.
>
> (b) Flexibility of approach.
>
> > (1) Covered entities . . . may use any security measures that allow the covered entity . . . to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
> >
> > (2) In deciding which security measures to use, a covered entity . . . must take into account the following factors:
> >
> > > (i) The size, complexity, and capabilities of the covered entity . . . .
> > >
> > > (ii) The covered entity's . . . technical infrastructure, hardware, and software security capabilities.
> > >
> > > (iii) The costs of security measures.

information is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual.[81] These rules apply to "covered entities" as defined by HIPAA and the HHS.[82] Covered entities include: health plans; health care clearinghouses, such as billing services and community health information systems; and health care providers that transmit health care data in a way that is regulated by HIPAA.[83]

### 2. The Gramm-Leach-Bliley Act of 1999

The Gramm-Leach-Bliley Act requires financial institutions to protect the security and confidentiality of customers' personal information and authorizes the creation of regulations for that purpose.[84] The Act contains a Financial Privacy Rule that obligates financial institutions to provide consumers with a privacy notice when the consumer relationship is established and every year thereafter.[85] The privacy notice must detail the information collected about the consumer, where it is shared, how it is used, and how it is protected.[86]

### 3. The Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act requires annual reporting to the Securities and Exchange Commission (SEC) on the internal financial controls of covered firms, which includes information security.[87] Section 302 of the Act demands that a set of procedures designed to ensure accurate financial disclosure exist.[88] It also requires the signing officers to certify that they are "responsible for establishing and maintaining internal controls" and "have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those

---

(iv) The probability and criticality of potential risks to electronic protected health information.

45 C.F.R. § 164.306 (2013).

81 45 C.F.R. § 160.103 (2014).

82 *Id.*

83 *Id.* (defining covered entities as a "health plan," "health care clearinghouse," or "health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter").

84 *Id.*

85 15 U.S.C. §§ 6801–6809 (2012).

86 *Id.*

87 15 U.S.C. § 7262 (2012).

88 *Id.*

entities, particularly during the period in which the periodic reports are being prepared."[89] The Act also requires officers to "have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report" and "have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date."[90] The nexus to cybersecurity beyond the aforesaid points is that the Sarbanes-Oxley Act defines "internal controls" very broadly to include everything that controls risks to the organization, including cybersecurity measures and, by extension, cyber risks.[91]

### 4. The Homeland Security Act of 2002

The Homeland Security Act of 2002 (HSA) created the Department of Homeland Security (DHS) and empowered it with functions relating to the protection of information infrastructure for both public and private entities.[92] The HSA also strengthened some criminal penalties relating to cyber crime.[93] Included in the HSA was the Cyber Security Enhancement Act of 2002.[94] This Act established various entities, headed by the Under Secretary, that focus on receiving, gathering, and analyzing information from federal, state, and local government agencies, with the intent of preventing terrorist acts.[95]

The HSA also sought to improve information security under Title X, which consisted of eight sections regarding the establishment of several divisions of information security.[96] This Title and its subchapter provided tactics and mechanisms for protecting federal information and preserving information security.[97] In addition, it established standards, responsibilities, authorities and functions, the various definitions in information security, and an annual independent evaluation.[98] It is

89 *Id.* § 7241(a)(4).

90 *Id.*

91 1 INST. OF INTERNAL AUDITORS RESEARCH FOUND., SAWYER'S GUIDE FOR INTERNAL AUDITORS 36 (6th ed. 2012).

92 6 U.S.C. §§ 121–195(c), 441–444, 481–486 (2012).

93 *See* U.S. SENTENCING COMM'N, INCREASED PENALTIES FOR CYBER SECURITY OFFENSES (2003).

94 6 U.S.C. § 145.

95 *Id.*

96 *See* 44 U.S.C. §§ 3531–3538 (2012) (repealed by Pub. L. 113-283, § 2(a), 128 Stat. 3073 (2014)).

97 *See id.*

98 *See id.*

important to note that Title X was repealed in December 2014, but other pieces of the HSA still remain in effect today.[99]

### 5. The Federal Information Security Management Act of 2002

The Federal Information Security Management Act of 2002 (FISMA) created a cybersecurity framework for federal information systems, with an emphasis on risk management, and required implementation of agency-wide information security programs.[100] Under FISMA, the National Institute of Standards and Technology (NIST) is responsible for developing security standards for federal computer systems (aside from national security systems).[101] Each federal agency is responsible for complying with those standards and they report annually on the status of their information security to the Office of Management and Budget (OMB), which then reports to Congress.[102] However, in December 2014, President Obama signed reforms to FISMA, including designating DHS as the lead enforcement agency in the federal government's internal fight against data breaches.[103]

### 6. The Cybersecurity Enhancement Act of 2014

The Cybersecurity Enhancement Act of 2014 obligated NIST to coordinate with industry leaders and critical infrastructure owners to facilitate and support the development of an industry-led set of standards and procedures to reduce cyber risks to critical infrastructure.[104] Part of the Act requires NIST to consult with government agencies in an attempt to coordinate the cybersecurity efforts between public and private sectors.[105] The Act further requires NIST to work with industry leaders to "identify a prioritized, flexible, repeatable, performance-based, and cost-effective" set of standards that "owners and operators of critical infrastructure" can adopt to help "identify, assess, and manage cyber risks."[106] The Act necessitates that the Comptroller General (GAO) submit biennial reports to Congress

99 *See id.* §§ 3551–3558.

100 *See* 40 U.S.C. § 11331 (2012); *see also* 15 U.S.C. §§ 278g-3 to 278g-4 (2012).

101 40 U.S.C. § 11331(a)(1).

102 44 U.S.C. §§ 3544–3545.

103 *See* Eric Chabrow, *DHS Big Winner in Congressional CyberSec Vote*, BANK INFO SECURITY (Dec. 12, 2014), http://www.bankinfosecurity.com/dhs-big-winner-in-congressional-cybersec-vote-a-7672 [http://perma.cc/6L22-VLZ2].

104 15 U.S.C. § 272(c)(15) (2012).

105 *Id.* § 272(e)(1)(A)(ii).

106 *Id.* § 272(e)(1)(A)(iii).

concerning NIST's progress in facilitating the development of such standards and procedures.[107]

### D. *What Are a Corporation's Options Under Domestic Law?*

Corporations that are victims of cyber hostilities perpetrated by a state actor have essentially one option under domestic law: rely on law enforcement to enforce one of the above-mentioned statutes.[108] Depending on the industry of the corporation and the severity of the attack, a variety of government agencies can be involved in assisting a company in mitigating and responding to a breach. However, as a general rule, the agency coordinating the response will be DHS.[109]

Once a breach is reported, the FBI will typically lead the investigation, including in situations involving cyber-based terrorism, espionage, computer intrusions, and major cyber fraud. Victims of cyber crimes can report to the FBI's Internet Crime Complaint Center, which was established as a partnership between the FBI and the National White Collar Crime Center.[110] Through the FBI-led National Cyber Investigative Joint Task Force, the FBI coordinates its efforts with more than seventeen law enforcement and intelligence community entities, including: the Central Intelligence Agency; Department of Defense; Department of Homeland Security; and the National Security Agency.[111] Recently, the FBI has enhanced its partnership "with DHS, forming joint FBI-DHS teams to conduct voluntary assessments for critical infrastructure owners and operators who are concerned about the network security of their industrial control systems."[112]

---

107 *See Summaries for the Cybersecurity Enhancement Act of 2014*, GOVTRACK, https://www.govtrack.us/congress/bills/113/s1353/summary (last visited Apr. 26, 2016); *see also* Cybersecurity Enhancement Act of 2014, S. 1353, 113th Cong. (2014), https://www.govtrack.us/congress/bills/113/s1353.

108 For a discussion about why corporations are restricted from using active cyber defense measures, see *infra* Part III.

109 *See* Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,743 (Feb. 12, 2013) (discussing the establishment of the critical infrastructure partnership advisory council which is run by DHS to "facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments").

110 *See Internet Crime Complaint Center (IC3)*, FED. BUREAU INVESTIGATION, http://www.ic3.gov/default.aspx (last visited Mar. 8, 2016).

111 *See* Ed Finkel, *Cyberspace Under Siege*, ABA J. (Nov. 1, 2010, 9:58 AM), http://www.abajournal.com/magazine/article/cyberspace_under_siege.

112 *Hearing Before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 112th Cong. (2011) (statement of Gordon M. Snow, Assistant Dir., Cyber Div., Fed. Bureau of Investigation), https://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.

The Department of Homeland Security is responsible for coordinating with the appropriate government and private sector organizations to respond to cyber hostilities that threaten national security.[113] It does this mainly through the National Cybersecurity and Communications Integration Center (NCCIC), a division of DHS that "combines two of DHS' operational organizations: the U.S. Computer Emergency Readiness Team (US-CERT), which leads a public-private partnership to protect and defend the nation's cyber infrastructure; and the National Coordinating Center for Telecommunications (NCC), the operational arm of the National Communications System."[114] The NCCIC shares information among the public and private sectors to provide greater understanding of cybersecurity and situation awareness of communication vulnerabilities, intrusions, incidents, mitigation, and recovery actions.[115]

DHS is currently drafting a National Cyber Incident Response Plan (NCIRP) that sets the strategic direction for how the nation should respond to cyber incidents.[116] This draft plan states that "[a]lthough steady-state activities and the development of a common operational picture are key components of the NCIRP, the plan focuses primarily on building the mechanisms" needed to respond to what it defines as a Significant Cyber Incident within its National Cyber Risk Alert Level system.[117] The system takes "into account the threats, vulnerabilities,

---

113 *See generally* Chabrow, *supra* note 103; s*ee also* DEP'T OF DEF., THE DOD CYBER STRATEGY 22, 25 (2015) (discussing how DoD supports DHS in cyber incidents).

114 Press Release, Dep't of Homeland Sec., Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center (Oct. 30, 2009), https://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened; *see also* Isabel Skierka, Mirko Hohmann, Robert Morgus & Tim Maurer, *National CSIRTs and Their Role in Computer Security Incident Response*, CYBERSECURITY INITIATIVE (Nov. 19, 2015), https://www.newamerica.org/cybersecurity-initiative/national-csirts-and-their-role-in-computer-security-incident-response.

115 *Protecting Critical Infrastructure*, DEP'T HOMELAND SECURITY, https://www.dhs.gov/topic/protecting-critical-infrastructure (last updated Jan. 19, 2016); *see also Assessing DHS's Performance—Watchdog Recommendations to Improve Homeland Security: Hearing Before the Subcomm. on Oversight & Mgmt. Efficiency of the H. Comm. on Homeland Security*, 113th Cong. 2 (2014) (statement of Daniel M. Gerstein, RAND Corp.), http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT424/RAND_CT424.pdf ("Close collaboration between the private sector and the National Cybersecurity and Communications Integration Center (NCCIC) on emerging cybersecurity issues in several critical infrastructure areas—including in the financial and energy sectors—also demonstrates how far the department has come.").

116 DEP'T OF HOMELAND SECURITY, NATIONAL CYBER INCIDENT RESPONSE PLAN (2010), http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf; *see also* Kyoung-Sik Min, Seung-Woan Chai & Mijeong Han, *An International Comparative Study on Cyber Security Strategy*, INT'L J. SECURITY & ITS APPLICATIONS, at 13, 16–17 (Feb. 2015), http://www.sersc.org/journals/IJSIA/vol9_no2_2015/2.pdf.

117 DEP'T OF HOMELAND SECURITY, *supra* note 116, at 2–3. DHS considers a cyber incident to be a Significant Cyber Incident when it raises the threat level to "substantial" in which there are "observed or imminent degradation of critical functions with a moderate to significant level

and potential consequences across the cyber infrastructure" and, in assessing the severity of a cyber incident, takes into account the impact of the incident on national security, public safety, public confidence, and the national economy (including any individual sectors that may affect the national economy).[118]

Local law enforcement agencies are also able to receive support from the Department of Defense (DoD) in the event of severe cyber incidents.[119] Written requests for law enforcement support are granted at the discretion of the Executive Secretary of the Department of Defense and are evaluated according to the factors set out in DoD Directive 3025.18.[120] DoD support in the event of a cyber incident comes from the Defense Cyber Crime Center.[121] The Cyber Crime Center provides digital and multimedia forensics, cyber investigative training, research, development, test and evaluation, and cyber analytics for a number of DoD mission areas.[122]

---

of consequences, possibly coupled with indicators of higher levels of consequences impending." *Id.* at 3.

118 *Id.* at 2; *see also* Min, Chai & Han, *supra* note 116, at 16 (noting that the NCIRP was created in order to provide a strategic framework for responding to a "critical cyber infringement accident").

119 *See* DEP'T OF DEF., INSTRUCTION NO. 3025.21, DEFENSE SUPPORT OF CIVILIAN LAW ENFORCEMENT AGENCIES 15 enclosure 3 (Feb. 27, 2013) (Participation of DoD Personnel in Civilian Law Enforcement Activities), https://info.publicintelligence.net/DoD-CivilianLaw Enforcement.pdf. Though this Instruction does not discuss cyber directly, it broadly discusses the Department of Defense's ability to provide support in situations involving a severe, domestic incident. *See* DEP'T OF DEF., *supra* note 113, at 22–25.

120 *See* DEP'T OF DEF., DIRECTIVE NO. 3025.18, DEFENSE SUPPORT OF CIVIL AUTHORITIES ¶ 4(e) (Sept. 21, 2012), http://www.dtic.mil/whs/directives/corres/pdf/302518p.pdf. This directive states:

> All requests from civil authorities and qualifying entities for assistance shall be evaluated for:
>
> (1) Legality (compliance with laws).
>
> (2) Lethality (potential use of lethal force by or against DoD Forces).
>
> (3) Risk (safety of DoD Forces).
>
> (4) Cost (including the source of funding and the effect on the DoD budget).
>
> (5) Appropriateness (whether providing the requested support is in the interest of the Department).
>
> (6) Readiness (impact on the Department of Defense's ability to perform its other primary missions).

*Id.*

121 *See* DOD CYBER CRIME CTR., http://www.dc3.mil/index#dc3 (last visited Mar. 8, 2016).

122 *See id.* This mission areas includes: "information assurance (IA) and critical infrastructure protection (CIP), law enforcement and counterintelligence (LE/CI), document and media exploitation (DOMEX), and counterterrorism (CT)." *Id.* For a greater discussion on why and how the United States military has responded to the cyber threat, see generally William T. Lord, *USAF Cyberspace Command: To Fly and Fight in Cyberspace*, STRATEGIC STUD. Q., Fall 2008, at 5.

In summary, it is usually best for corporations responding to a cyber incident to initially refer their complaint to the DHS or the FBI, who will then coordinate with appropriate additional agencies as necessary. Cyber events directed at critical infrastructure or those severe enough to threaten national security are referred to the DHS, and they may even call for assistance from the DoD. However, law enforcement's ability to effectively remediate the breach and identify the perpetrators can be quite limited, not to mention their ability to prosecute foreign state actors.[123] These limitations obviously cause frustration and may lead corporations to believe that relying solely on law enforcement will not provide them adequate protection. As a result, corporations may consider active defense measures in their cybersecurity systems. However, a corporation's attempt at invoking a right of self-defense is problematic under international law as discussed in the next Part.

## III. INTERNATIONAL LAW AND THE NONEXISTENT RIGHT OF CORPORATE SELF-DEFENSE

A state actor conducting hostile cyber operations against a corporation unquestionably violates the sovereignty of the host nation.[124] It is irrelevant whether these activities were physically destructive or injurious, as long as they were unlawful and detrimental.[125] A host state has a variety of options to respond to the aggressor state[126] depending on whether the activity is an armed attack

123 *See, e.g.*, Devlin Barrett & Danny Yadron, *Sony, U.S. Agencies Fumbled After Hacking*, WALL ST. J., Feb. 23, 2015, at B1 (discussing how there are major shortcomings in how the government and companies work together to respond to cyber hostilities, particularly in the hack of Sony Entertainment).

124 Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 274–75 (2014) [hereinafter Schmitt, *Cyber Warfare*] ("[H]ostile cyber operations directed against cyber infrastructure located on another state's territory, whether government owned or not, constitute, *inter alia*, a violation of that state's sovereignty . . . ."); *see also* Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014, 9:29 AM) [hereinafter Schmitt, *International Law*], http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea. For example, North Korea's cyber hostilities directed at Sony violated the sovereignty of the United States.

125 Schmitt, *International Law*, *supra* note 124 ("[I]t would seem reasonable to characterize a cyber operation involving a State's manipulation of cyber infrastructure in another State's territory, or the emplacement of malware within systems located there, as a violation of the latter's sovereignty. This being so, . . . it violated U.S. sovereignty.").

126 *See* Schmitt, *Cyber* Warfare, *supra* note 124, at 284. Professor Schmitt notes that "[a]s a practical matter, characterization of a cyber operation as a wrongful use of force merely serves to label the state involved as a violator of international law." *Id.* State responses to uses of force are capped "at the non-forceful countermeasures level, an armed attack gives the targeted state the right to respond with its own use of force." *Id.* (footnote omitted).

or something less significant.[127] Yet, what about the corporation? Can it do anything?

The short answer is yes—a corporation has a right to some self-help by using protective measures. But the legal justification and the parameters of the corporate response are significantly different than that of a state. A state reacting to cyber hostilities will look to international law to regulate their response. In contrast, a corporation can only rely upon domestic law to justify its actions.[128] While international law allows a state acting in self-defense to use force against another state if attacked or in anticipation of an attack,[129] domestic law will limit a corporation to stopping the hostile act.[130] In addressing the immediate hostilities, a corporation may only use protective measures that do not cause destruction[131] or death to a hostile state actor's cyber agents or

127 Cyber intrusions can range from a violation of sovereignty, to an unlawful intervention, to a use of force, to an armed attack. What rises to the level of an armed attack is debatable, but most agree that there is a difference between a "use of force," and an "armed attack." *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 101 (June 27) [hereinafter Nicaragua v. United States] ("[I]t [is] necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."). *But see* Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, International Law in Cyberspace, Address at the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *in* 54 HARV. INT'L L.J. ONLINE 1, 7 (2012) (stating that the United States position is that the "inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response"). The U.N. Charter does not define a "use of force," leaving some discretion to individual states. The International Criminal Tribunal for the Former Yugoslavia somewhat addressed this issue by stating "an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State." Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995). Though not addressing the definition directly, this statement infers "that activities that directly lead to an armed conflict may be a use of force." *See* GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 15 (2012).

128 The international legal definition of self-defense only applies to states, as it is one of the two legal justifications for using force against another state. *See* U.N. Charter art. 51. Consequently, the right of self-defense in international law exclusively addresses when states may use force in response to other states—including when it involves cyber operations. *See* Schmitt, *Cyber Warfare*, *supra* note 124, at 281.

129 *See infra* Section III.A (discussing an international law interpretation of self-defense); *see also* Schmitt, *Cyber Warfare*, *supra* note 124, at 285 ("[T]he great weight of informed opinion supports the existence of a right of anticipatory self-defense in the face of an 'imminent' armed attack.").

130 *See infra* Section III.A (discussing domestic self-defense).

131 It is unclear what qualifies as a "use of force" in cyber operations. This is, of course, an important question as the use of force is prohibited but for two exceptions in the U.N. Charter. *See* U.N. Charter art. 2, ¶ 4. While there is no bright-line test, the Tallinn Manual provides a nonexclusive list of factors that helps clarify whether a cyber activity is a "use of force." *See* TALLINN MANUAL, *supra* note 26, at 48–51.

infrastructure.[132] Further, the corporation must be careful to not pierce the sovereignty of the hostile state, which is quite complicated due to the borderless nature of cyberspace,[133] since this would also be a violation of international law.[134] Put differently, a state has latitude to preemptively counter a cyber attack, and may broadly engage the hostile state in self-defense.[135] In contrast, a corporation's defensive actions must have a temporal proximity to the hostilities, and the response is limited to stopping the offending state's cyber operations without violating international law.[136]

The following hypothetical scenarios help provide some clarity. Consider a situation where a corporation in State A is cyber attacked[137] by a unit of cyber soldiers[138] located in State B. State A may respond by using force against State B. The corporation, for its part, may use

---

132 The irrelevance of borders in cyberspace could lead to the theoretical situation where a corporation acts in self-defense against a hostile state actor's agents in cyberspace and the result is death or destruction in the host nation. As the use of force in self-defense is an exclusive right of state actors, the corporation would be in violation of the U.N. Charter's general prohibition on the use of force. *See* U.N. Charter art 2, ¶ 4. As a perverse result, under the law of state responsibility, the United States would be responsible for the corporation's violation of the hostile state's sovereignty. *See* G.A. Res. 56/83 (Jan. 28, 2002) (Responsibility of States for Internationally Wrongful Acts) [hereinafter Articles on State Responsibility]. This is the same result if a corporation is acting in self-defense and their response damages a third nation's cyber infrastructure or personnel.

133 *See* U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT, at iv (2010) (discussing the difficulties of cyberspace); Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, Winter 2008–09, at 60, 70 ("[I]nternational laws of war are . . . fundamentally weak in addressing borderless, nonstate actor participation in cyber conflict where individuals organize their own cyber campaigns.").

134 *See* Articles on State Responsibility, *supra* note 132, art. 2 (discussing attribution to a state for nonstate activities).

135 *See* Schmitt, *Cyber Warfare*, *supra* note 124, at 286 (noting that the practical and operational realities of cyber operations allow a state greater latitude in employing anticipatory self-defense).

136 For a discussion on the limitations on a corporation's right of self-defense, see *infra* Section III.A. However, it is important to note that an unresolved issue with respect to sovereign rights and obligations "is whether cyber operations that neither cause physical damage nor amount to an intervention" violate state sovereignty. *See* Schmitt, *Cyber Warfare*, *supra* note 124, at 275. Unclear examples include: monitoring certain cyber activities in a state, sending malware into a network remotely, or remotely conducting denial of service attacks. *Id.*

137 A cyber attack is defined as "any use of force that injures or kills persons or damages or destroys property." TALLINN MANUAL, *supra* note 26, at 55. The "requisite degree of damage or injury remains . . . the subject of some disagreement." Schmitt, *Cyber Warfare*, *supra* note 124, at 282. How much damage is necessary to qualify as an armed attack and the nonmilitary measures available to a state under international law are outside the scope of this Article. For a more in-depth discussion about state self-defense in cyberspace, see Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99 (2002), and Matthew C. Waxman, *Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions*, 89 INT'L L. STUD. 109 (2013).

138 For an excellent discussion on combatant status in cyber warfare, see generally Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 391 (2010).

protective measures to stop the hostile cyber activities, but these actions cannot cross into the realm of violating the sovereignty of State B. Another example is also helpful: Consider a situation where a corporation in State A is under imminent cyber attack by State B. State A may again respond with force against State B, as a cyber attack triggers the international legal interpretation of self-defense, and particularly State A's authority to act in anticipation of an attack.[139] In contrast, the corporation can defend its business interests from the impending attack, but must be careful not to take any active measures against State B.

International law categorically prohibits a nonstate actor—in this case a corporation—from actively engaging a hostile state, even if victimized by a cyber attack. The right of action against a state actor is exclusively within the purview of states, as articulated in the United Nations Charter and the Articles on State Responsibility.[140] Though this is unsettling for a corporation constantly victimized by hostile cyber activity, international law intentionally mandates a nonstate actor to rely upon its nation for a self-defense response. This bright-line rule is perhaps the primary reason for a robust private-government partnership. Yet, it is also impractical and unreasonable to expect a corporation to passively stand by and not defend its interests. Some self-help protective measures must be allowed. The prohibitive use-of-force paradigm established in international law, and a corporation's right to use defensive protective measures, intersect when confronted with state-sponsored cyber hostilities. How this intersection works is discussed below.

### A. *Why the Inherent Right of Self-Defense Does Not Apply*

The use of force under international law is strictly regulated by the part of the laws of war known as *jus ad bellum*, which "refers to the conditions under which one may resort to war or to force in general."[141] *Jus ad bellum* is "governed by an important, but distinct, part of the international law set out in the United Nations Charter."[142] The U.N.

---

139 *See infra* Section III.A (discussing anticipatory self-defense in international law).

140 *See generally* Articles on State Responsibility, *supra* note 132.

141 Robert Kolb, *Origin of the Twin Terms* Jus Ad Bellum/Jus In Bello, 320 INT'L REV. RED CROSS 553, 553 n.1 (1997). In contrast, *jus in bello* "governs the conduct of belligerents during a war, and in a broader sense comprises the rights and obligations of neutral parties as well." *Id.* *Jus ad bellum* and *jus in bello* together are the law of armed conflict. *See* Shane R. Reeves & David Lai, *A Broad Overview of the Law of Armed Conflict in the Age of Terror*, *in* THE FUNDAMENTALS OF COUNTERTERRORISM LAW 140, 140–42 (Lynne Zusman ed., 2014).

142 ADVISORY SERV. ON INT'L HUMANITARIAN LAW, *supra* note 35, at 1.

Charter prohibits the threat or use of force by any state.[143] This prohibition is absolute, with only two generally recognized exceptions.[144] The first exception reserves to the Security Council the right to "determine the existence of any threat to the peace, breach of the peace, or act of aggression," and the power to "decide what measures shall be taken . . . to maintain or restore international peace and security."[145] The second exception ensures that states retain the "inherent" right of individual or collective self-defense if they are the victim of an armed attack.[146]

The U.N. Charter's first exception to the general prohibition on the use of force is clearly inapplicable to corporations responding to a state-sponsored cyber attack. It is important, however, to note that the nations which formulated the U.N. Charter envisioned a system where the United Nations, through the Security Council, would control the use of force in international law.[147] There is no doubt that this vision is now reality and the use of force regulatory framework established in the U.N. Charter is binding on all states whether through membership[148] or customary international law.[149] The Security Council, empowered by the

143 U.N. Charter art. 2, ¶ 4 ("All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state . . . ."). The U.N. Charter's general prohibition on the use of force echoes the ban on wars of aggression, or "the renunciation of war as an instrument of national policy," agreed to in the Kellogg-Briand Pact of 1928. *See* Treaty Between the United States and Other Powers Providing for the Renunciation of War as an Instrument of National Policy, Aug. 27, 1928, 46 Stat. 2343.

144 "Consent" is considered by some as a third exception to the general prohibition on the use of force. The U.N. Charter allows nations to deal with internal domestic matters. *See* U.N. Charter art. 2, ¶ 7. "If a nation requests the aid of a fellow nation or ally, that fellow nation or ally is free to use force within the boundaries of the requesting nation." CORN ET AL., *supra* note 127, at 17. *But see* INT'L & OPERATIONAL LAW DEP'T, U.S. JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., LAW OF ARMED CONFLICT DESKBOOK 31 n.7 (William J. Johnson & Andrew D. Gillman eds., 2012) [hereinafter DESKBOOK] ("[C]onsent is sometimes stated as a separate exception. However, if a State is using force with the consent of a host State, then there is no violation of the host State's territorial integrity or political independence; thus, there is no need for an exception to the rule as it is not being violated.").

145 U.N. Charter art. 39.

146 *Id.* art. 51.

147 *See* CORN ET AL., *supra* note 127, at 12.

148 There are currently 193 member states to the United Nations. *U.N. Member States: On the Record*, UNITED NATIONS, http://www.un.org/depts/dhl/unms/whatisms.shtml (last visited May 26, 2015). Each member agrees to "accept and carry out the decisions of the Security Council." U.N. Charter art. 25.

149 *See* Nicaragua v. United States, *supra* note 127, at 98–101 (finding that the U.N. Charter is customary international law). Customary international law results from the general and consistent practice of states followed from a sense of legal obligation. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 102(2), 102 cmt. c (AM. LAW INST. 1987); 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW xxxviii (2009), https://www.icrc.org/eng/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf ("[C]ustomary international law requires the presence of two elements, namely State practice (*usus*) and a belief that such

rest of the international community, is the final arbiter of these decisions and the only source of authority allowing for the use of force.[150] Individual nations therefore do not have legal discretion to unilaterally use force, as the U.N. Charter makes clear that all states are disallowed from the aggressive use of force—including acts of cyber war.[151] For those states that decide to ignore the U.N. framework, those cyber activities construed as an armed attack may trigger a self-defense response from a victimized state.[152]

The U.N. Charter expressly allows a victimized state to make an individual use-of-force determination if exercising its inherent right of self-defense.[153] This right was a well-established international norm prior to the drafting of the U.N. Charter and is generally recognized as customary international law.[154] The customary definition, most famously outlined in the Caroline Doctrine,[155] allows a state to use force if it "show[s] a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation."[156] But, even if

practice is required, prohibited or allowed, depending on the nature of the rule, as a matter of law (*opinio juris sive necessitatis*).").

150 *See* U.N. Charter art. 24, ¶ 1 ("Members confer on the Security Council primary responsibility for the maintenance of international peace and security, and agree that in carrying out its duties under this responsibility the Security Council acts on their behalf.").

151 *See 1944–1945: Dumbarton Oaks and Yalta*, UNITED NATIONS, http://www.un.org/en/sections/history-united-nations-charter/1944-1945-dumbarton-oaks-and-yalta/index.html (last visited May 26, 2015) ("The essence of the plan was that responsibility for preventing future war should be conferred upon the Security Council."); *see also* CORN ET AL., *supra* note 127, at 4 ("One of the key goals of the Charter was to establish a presumptive prohibition on the use of force by States.").

152 States also have response options if the hostile state uses cyber tactics that fall below the "armed attack" threshold. *See* Schmitt, *Cyber Warfare*, *supra* note 124, at 274–75.

153 U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.").

154 *See* Nicaragua v. United States, *supra* note 127, at 103 ("This resolution demonstrates that the States represented in the General Assembly regard the exception to the prohibition of force constituted by the right of individual or collective self-defence as already a matter of customary international law."); YORAM DINSTEIN, WAR, AGGRESSION, AND SELF-DEFENCE 181 (4th ed. 2005).

155 An 1837 incident on Lake Erie between the United States and the British concerning the *Caroline*, a U.S. flagged ship, led to correspondence between Secretary of State Daniel Webster and the British Foreign Officer Lord Ashburton concerning a state's right to assert self-defense. *See generally* John J. Merriam, *Natural Law and Self-Defense*, 206 MIL. L. REV. 43, 59–61 (2010); *see also* John Dever & James Dever, *Cyberwarfare: Attribution, Preemption, and National Self Defense*, 2 J.L. & CYBER WARFARE 25, 37–63 (2013).

156 Letter from Daniel Webster, U.S. Sec'y of State, to Lord Ashburton (July 27, 1842), *in* 11 THE WRITINGS AND SPEECHES OF DANIEL WEBSTER 292 (1903) [hereinafter Webster Letter] (quoting Letter from Daniel Webster, U.S. Sec'y of State, to H.S. Fox (Apr. 24, 1841)). In this correspondence, Webster posited that a state does have an inherent right to self-defense but can only exercise that right if it "show[s] a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation." *Id.*

force is necessary, it cannot be "unreasonable or excessive[,] since the act, justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it."[157] Using force in self-defense, according to this customary definition, is therefore allowed if it is necessary and used in a proportionate manner.[158]

Customary international law thus imparts upon the state independent authority to determine when it is necessary to exercise this inherent right to self-defense. According to the language expressed in the Caroline Doctrine, this authority is broad and may include using force in an anticipatory manner to stymie an imminent armed attack.[159] Some disagree vehemently with this idea, arguing that a plain reading of the U.N. Charter's Article 51 supplants the expansive customary definition of self-defense and any independent right asserted by a state.[160] Noting that the language of Article 51 only allows for self-defense after an armed attack, and even then only until the Security Council takes action, these "strict constructionists" believe the Charter has preempted the customary understandings.[161] Yet this argument is incomplete as it does not account for the Charter's express recognition that it cannot "impair the inherent right" of self-defense, nor does it address what constitutes an "armed attack."[162] Further, even under the most restrictive interpretation of Article 51, the document recognizes

157 *Id.* at 261 (quoting Letter from Daniel Webster, U.S. Sec'y of State, to H.S. Fox (Apr. 24, 1841)).

158 Necessity is generally understood to mean that force should be used as a last resort. DESKBOOK, *supra* note 144, at 35. To comply with proportionality, "[s]tates must limit the magnitude, scope, and duration of any use of force to that level of force which is reasonably necessary to counter a threat or attack." *Id.* Some argue for a third defining criteria, which is immediacy. CORN ET AL., *supra* note 127, at 19–22 ("Three major principles are generally accepted as governing self-defense actions under Article 51: necessity, proportionality, and timeliness."); DINSTEIN, *supra* note 154, at 242 ("War may not be undertaken in self-defence long after an isolated armed attack.").

159 *See* DESKBOOK, *supra* note 144, at 37 ("Secretary Webster posited that a State need not suffer an actual armed attack before taking defensive action, but may engage in anticipatory self-defense . . . ."); Webster Letter, *supra* note 156.

160 *See* DINSTEIN, *supra* note 154, at 183. However, Professor Dinstein does allow for anticipatory action if an armed attack has been launched in an "irrevocable way." *Id.* at 191.

161 This group believes that "the right [to self-defense] is no more than as granted in the Charter and must, therefore, be understood in conjunction with other Charter provisions limiting the resort to force." CORN ET AL., *supra* note 127, at 22. Under this restrictive view, a state acting in self-defense would need to gain authority from the Security Council prior to responding with force. *Id.*; *see also* Merriam, *supra* note 155, at 62–68; Sean D. Murphy, *The Doctrine of Preemptive Self-Defense,* 50 VILL. L. REV. 699, 706–17 (addressing to what extent a customary international law right to self-defense exists and coining the term U.N. "strict constructionists").

162 U.N. Charter art. 51.

that an actual armed attack authorizes a proportionate self-defense response.[163]

While "[t]here is clearly no common understanding of the application" of Article 51 to state action, it is apparent that some authority exists for a state to act in self-defense.[164] But can a corporation assert the same "inherent" right of self-defense as a state under international law?[165] The answer is a clear and resounding "no." International law is broadly conceived as regulating the interactions between states.[166] In these interactions, states have developed the highly restrictive use of force regulatory framework outlined in the U.N. Charter. Article 2(4) of the Charter "and its customary analog apply only to actions conducted by states or otherwise attributable to them pursuant to the law of state responsibility; it has no bearing on the actions of non-state actors."[167] As the inherent right of self-defense is a legal justification for using force in international law, there is simply no room for a corporation to invoke that right. This is not by accident. Chief among the responsibilities of the United Nations is an obligation to suppress "acts of aggression or other breaches of the peace."[168] Allowing nonstate actors, such as corporations, to use force in self-defense against a state actor would open the door for arbitrary acts of armed violence.[169]

---

163 There is a general consensus on the principles that apply to a use of force in self-defense. *See* CORN ET AL., *supra* note 127, at 19.

164 *Id.*; *see also* TALLINN MANUAL, *supra* note 26, at 63 ("Textually, Article 51 of the United Nations Charter refers to a situation in which 'an armed attack occurs.' Clearly, this covers incidents in which the effects of the armed attack have already materialized . . . ." (quoting U.N. Charter art. 51)).

165 Without question, a state may respond to cyber aggression by another state under its inherent right of self-defense. At minimum, the intrusion will be a violation of a state's sovereignty and, if significantly severe, can be considered an act of war triggering a proportionate response. For an excellent discussion on this graduated scale of state response to a cyber intrusion, see Schmitt, *Cyber Warfare*, *supra* note 124.

166 *See id.* at 272. International law is defined as "rules and principles of general application dealing with the conduct of states and of international organizations and with their relations *inter se*, as well as with some of their relations with persons, whether natural or juridical." RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 101 (AM. LAW. INST. 1987).

167 Schmitt, *Cyber Warfare*, *supra* note 124, at 279.

168 U.N. Charter art. 1, ¶ 1.

169 *See generally* Shane Reeves, *To Russia with Love: How Moral Arguments for a Humanitarian Intervention in Syria Opened the Door for an Invasion of the Ukraine*, 23 MICH. ST. INT'L L. REV. 199 (2014) (explaining the associated problems when states or others operate outside the U.N. Charter's well-established use of force regulatory framework).

### B. *What About Actions Falling Below a Use of Force?*

Of course, there are a number of measures a corporation could use in response to state-sponsored cyber hostilities that fall below the use-of-force threshold. However, the Articles of State Responsibility make clear that violations of a state's sovereignty by nonstate actors are not permitted. Article 2 expresses that "[t]here is an internationally wrongful act of a State when conduct consisting of an action or omission" is attributable to the State.[170] Inclusion of "omission" as a form of attribution is important as a nonstate actor—in this case, a corporation—could respond in such a way that the government becomes responsible. For this reason, a corporation is not authorized to participate in "countermeasures," as outlined in Articles 49 through 54, against a state participating in hostile cyber activities.[171]

In discussing specifically the attack on Sony by North Korea, Professor Michael Schmitt notes:

> Countermeasures are actions by an injured State that breach obligations owed to the "responsible" State (the one initially violating its legal obligations) in order to persuade the latter to return to a state of lawfulness. Thus, if the cyber operation against Sony is attributable to North Korea and breached U.S. sovereignty, the United States could have responded with countermeasures, such as a "hack back" against North Korean cyber assets. . . . Countermeasures may only be taken by States. Thus, Sony could not have, on its own accord, responded against North Korea with its own cyber operations.[172]

A corporation is therefore responsible for ensuring that any cyber protective measures do not pierce the sovereignty of the hostile state, or it risks the consequences of violating international law.[173] So what cyber activities would violate the territorial sovereignty of a state? Clearly cyber operations that cause physical damage or injury, assuming there is no legal justification, would cross the threshold.[174] Even operations that result in no damage or injury may qualify if they are attempts to unlawfully intervene in a targeted state's governmental matters.[175] While

---

170 *See* Articles on State Responsibility, *supra* note 132, art. 2.

171 *See id.* art. 49–54.

172 Schmitt, *International Law*, *supra* note 124.

173 Respect for territorial sovereignty between independent states is "an essential foundation of international relations." Nicaragua v. United States, *supra* note 127, § 202 (quoting Corfu Channel, Merits, 1949 I.C.J. 171 (Apr. 9)).

174 These would obviously violate the prohibition on using force, discussed *supra* Section III.A.

175 *See* Schmitt, *Cyber Warfare*, *supra* note 124, at 275 (examples include using cyber means to interfere with election results).

it is unclear whether cyber operations "that neither cause physical damage nor amount to an intervention" violate territorial sovereignty, even these may be problematic, as the threshold seems to be moving lower.[176] "With states and their citizens becoming ever more reliant on cyber activities, a strengthening of the normative firewalls that safeguard cyber activities against external interference is to be expected."[177] This trend increases the likelihood that a robust definition of sovereignty will be asserted by states trying to rebuff cyber intrusions. What becomes apparent when applying the law on state responsibility to the practical realities of cyber operations is that any corporate response to state-sponsored cyber hostilities must be physically harmless, noncoercive, and perhaps even nondetrimental. These restrictive limitations thus only allow a corporation to implement protective measures, but not active defense measures.

Using active defense measures in corporate computer systems raises many other issues as well. Attribution never completely ceases to be a concern even when a state openly takes responsibility for an attack. It is nearly impossible to attribute cyber attacks with complete certainty, which is one of the key distinctions between active defense in the cyber realm and self-defense in the kinetic realm.[178] The issue of attribution complicates the legal and policy concerns involved in active cyber defense, as well as the effectiveness of the mechanisms themselves, as hacking back strategies can often be shots in the dark against unknown perpetrators.[179]

Active defense also opens the door for disproportionate retaliatory attacks that can cause collateral damage to innocent parties, especially when it is not clear who the target is.[180] Hackers often deploy their attacks from "hijacked computers belonging to innocent bystanders," meaning that a corporate retaliation might end up targeting people who have done nothing wrong.[181] Additionally, widespread hacking back on the part of U.S. companies could create a kind of digital wild west in

---

176 *Id.*

177 *Id.* at 276.

178 *Id.* at 278.

179 JEFFREY HUNKER ET AL., INST. FOR INFO. INFRASTRUCTURE PROTECTION, ROLE AND CHALLENGES FOR SUFFICIENT CYBER-ATTACK ATTRIBUTION 5 (2008) ("Our legal and policy frameworks for responding to cyber attacks cannot work unless we have adequate attribution; these frameworks remain incomplete because we lack the basis (sufficient attribution) to actually use them.").

180 *Id.*

181 Max Fisher, *Should the U.S. Allow Companies to 'Hack Back' Against Foreign Cyber Spies?*, WASH. POST (May 23, 2013), http://www.washingtonpost.com/blogs/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies (quoting John Reed, *The Cyber Security Recommendations of Blair and Huntsman's Report on Chinese IP Theft*, FOREIGN POL'Y (May 22, 2013)).

which companies and criminals would compete in a cyber arms race that only encourages cyber attacks on a larger scale and makes cyberspace less safe overall.[182] This would in turn undermine U.S. efforts to "establish durable international norms that hacking is bad, implicitly endorsing the idea of all-out cyberwarfare among corporations and criminals in a way that would make it tough to hold anyone accountable."[183]

However, quite interestingly, there may be a possibility that a corporation could go beyond simple protective measures when responding to state-sponsored cyber hostilities if empowered by their state. Article 5 notes that an "entity which is not an organ of the State" may be empowered to exercise elements of governmental authority.[184] If empowered, the corporation's actions would be "considered an act of the State under international law, provided [they are] acting in that capacity in the particular instance."[185] A state may therefore "outsource the taking of lawful cyber actions to private entities" but when they do so, "the States shoulder legal responsibility for the actions."[186] As states retain responsibility for the consequences of any corporate actions, it seems unlikely they would allow for active measures. It is important to note that states may "not knowingly allow the cyber infrastructure located in [their] territory or under [their] exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[187] Yet, despite the barriers to a state "deputizing" a private entity to respond to a state-sponsored cyber attack, this is an intriguing possibility that could be an option in a greater corporate-government partnership.[188]

---

182 McGee et al., *supra* note 55 (describing the various domestic and international legal consequences that can result from responding to cyber hostilities that have been misattributed).

183 Fisher, *supra* note 181.

184 *See* Articles on State Responsibility, *supra* note 132, art. 5.

185 *Id.*

186 Schmitt, *International Law*, *supra* note 124.

187 TALLINN MANUAL, *supra* note 26, at 26.

188 For a more detailed discussion on empowering corporations under the Articles of State Responsibility to actively respond to a cyber hostility, see generally Daniel Garrie & Shane R. Reeves, *So You're Telling Me There's a Chance: How the Articles on State Responsibility Could Empower Corporate Responses to State-Sponsored Cyber Attacks,* HARV. NAT'L SECURITY J. ONLINE FEATURES. (Dec. 17, 2015), http://harvardnsj.org/2015/12/so-youre-telling-me-theres-a-chance-how-the-articles-on-state-responsibility-could-empower-corporate-responses-to-state-sponsored-cyber-attacks.

Active cyber defense invites trouble under domestic law as well since counter-attackers could be found to violate any number of cyber crime statutes, such as unauthorized computer access under the CFAA, regardless of the fact that the attack is part of the defense of their systems. *See* 18 U.S.C. § 1030(a)(2)–(5) (2012). The CFAA contains no "self-defense-type" exceptions to any of its provisions. It broadly criminalizes, inter alia, unauthorized access of protected computers and damaging protected computers by means of malicious code, which

### C. *The Red Herring: International Human Rights Law*

Despite this intriguing possibility, the current state of international law clearly prohibits any right to corporate self-defense. However, some argue international law provides an alternative for an individual, and perhaps a corporation, to use force.

> The U.N. Charter, while primarily a *jus ad bellum* instrument, also recognizes the need for human rights [and] [a]ccordingly, "promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion" was included among the Purposes and Principles of the Charter.[189]

This statement laid the foundation for international human rights law which "protects persons as individuals rather than as subjects of sovereign States" and imposes certain legal obligations on state actors.[190] International human rights law is composed of both treaty and customary obligations. While the conventional aspects of this body of law apply to signatory states,[191] certain customary legal obligations are considered binding upon all nations. These customary obligations are interpreted as requiring all states to recognize and protect certain fundamental, or non-derogable, human rights. Though no definitive list of these universal human rights exists, some examples include a

---

are likely to include most kinds of active defense. *Id.* In the context of hacking back, both the attacker and the counter attacker could be found to be equally violating the law.

Additionally, advocates of applying self-defense law in the cyber context claim that, similar to the individual right to protect oneself from imminent harm in the physical realm, a private entity should be able to protect its digital assets in the cyber realm. *See, e.g.*, Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 415 (2012); *Active Self-Defense Strategy Best Deterrent Against Cyber-Attacks*, UNIV. OF ILL. URBANA-CHAMPAIGN (June 27, 2011, 9:00 AM), https://news.illinois.edu/blog/view/6367/205294 ("The principles of mitigative counterstriking are legally justifiable under several areas of domestic and international law, and can be made consistent with other areas of law by amending or reinterpreting the law." (quoting law professor Jay P. Kesan)). While the principle may make sense in theory, notions of retreat and stand your ground that are the basis for determining when the use of force is permitted in the physical realm are difficult to fit into the context of computer networks that cannot retreat or stand their ground in a literal sense. *See* McGee et al., *supra* note 55, at 15. Given these legal barriers, active defense is an ill-advised option under both domestic and international law.

189 Brian J. Bill, *Human Rights: Time for Greater Judge Advocate Understanding*, ARMY LAW., June 2010, at 54, 55 (footnote omitted) (quoting U.N. Charter art. 1, ¶ 3).

190 DESKBOOK, *supra* note 144, at 195.

191 *See, e.g.*, International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

prohibition on slavery, a prohibition on torture, and equality before the law.[192]

As international human rights law is a dynamic and rapidly expanding regulatory regime,[193] there are many who argue for new or previously unrecognized human rights to be declared fundamental.[194] One such group has advocated for self-defense to be recognized as a fundamental human right.[195] Claiming all have an inherent, or natural, right to self-defense, these proponents believe "[n]o government has the legitimate authority to forbid a person from exercising her human right to defend herself against a violent attack or to forbid her from taking the steps and acquiring the tools necessary to exercise that right."[196] Assuming there is a fundamental human right of self-defense, is it possible to interpret this right as applying to corporations who want to actively defend their assets?

While it is hotly debated whether there is an international human right of self-defense,[197] this argument is completely irrelevant to a corporation. International human rights law is focused on protecting the dignity and life of citizens from the state. Designed "to induce states to remedy the inadequacies of their national laws and institutions so that human rights will be respected and vindicated,"[198] a theoretical human right of self-defense is not applicable extraterritorially but is more akin to a domestic protection. Further, and perhaps most obvious, a "human right" does not equate to a "corporate right." Though it is well-established under United States law that a corporation has some of the same rights and responsibilities as an individual,[199] this does not

192 *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) [hereinafter UDHR]. For a discussion on whether the Universal Declaration has ripened into customary international law, see Hurst Hannum, *The Status of the Universal Declaration of Human Rights in National and International Law*, 25 GA. J. INT'L & COMP. L. 287, 317 (1996).

193 *See, e.g.*, Bill, *supra* note 189, at 59 (noting that the international community is constantly expanding human rights law).

194 *See id.* at 59–60.

195 *See generally* David B. Kopel, Paul Gallant & Joanne D. Eisen, *The Human Right of Self-Defense*, 22 BYU J. PUB. L. 43, 178 (2007) ("[T]he overwhelming consensus among the sources of international law, from ancient times to the present, among diverse legal systems, religions, and nations: self-defense is a fundamental human right.").

196 *Id.*

197 *Compare id.*, *with* John Cerone, *Is There a Human Right of Self-Defense?* 2 J.L. ECON. & POL'Y 319, 319 (2006) ("[T]here is no norm of international law providing a human right to self-defense.").

198 THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS 13–16 (Louis Henkin ed., 1981).

199 *See, e.g.*, Pembina Consol. Silver Mining & Milling Co. v. Pennsylvania, 125 U.S. 181, 189 (1888) ("Under the designation of 'person' there is no doubt that a private corporation is included [in the Fourteenth Amendment]."); Cty. of Santa Clara v. S. Pac. R.R. Co., 118 U.S. 394 (1886) (applying the Fourteenth Amendment to corporations).

make a business a "human" as understood by international law.[200] As such, it is impossible and impractical to bestow a fundamental right of self-defense on an entity that is a legal fiction.

### D. *Summary*

The U.N. Charter purposefully restricts use of force to states. The document, drafted following the unprecedented destruction and devastation of World War II,[201] was a collective attempt by the international community to stymie aggression.[202] For this reason, the U.N. Charter intentionally excludes all nonstate actors, including corporations, from having a right to invoke self-defense against a state actor, regardless of the reason. Further, even for those actions that may fall below the use-of-force threshold, the Articles of State Responsibility make clear that it is a state's obligation to respond to breaches of sovereignty.[203] In their role as nonstate actors, corporations are limited to implementing defensive, protective measures when victimized by state-sponsored cyber hostilities. Finally, it is clear that a human rights argument does not apply to corporations and is irrelevant to determining a legally justified cyber response. Viewed in its entirety, it is apparent that international law does not provide an avenue for a corporation to respond to state-sponsored cyber hostilities.[204] A corporation is left with the singular option of relying upon its host state to intervene on its behalf.

---

200 *See, e.g.*, UDHR, *supra* note 192, art. 16 (referring to "humans" as men and women).

201 *See* DESKBOOK, *supra* note 144, at 15 (discussing how post–World War II the international community recognized the need for a world body with greater power to prevent war); *1943: Moscow and Teheran Conferences*, UNITED NATIONS, http://www.un.org/en/sections/history-united-nations-charter/1943-moscow-and-teheran-conferences/index.html (last visited Jan. 14, 2016) ("By 1943 all the principal Allied nations were committed to outright victory and, thereafter, to an attempt to create a world in which 'men in all lands may live out their lives in freedom from fear and want.'" (quoting FRANKLIN D. ROOSEVELT & WINSTON S. CHURCHILL, THE ATLANTIC CHARTER ¶ 6 (1941))).

202 *See* U.N. Charter pmbl. ("We the peoples of the United Nations determined . . . to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind . . . .").

203 *See* Articles on State Responsibility, *supra* note 132, art. 49 (noting that only an injured state may take countermeasures against another state).

204 *See* Cerone, *supra* note 197, at 319 ("While there is a clearly established right of self-defense in international law, this right applies only to states.").

## IV. RECOMMENDATIONS AND CONCLUSION

It seems unreasonable to expect a corporation to stand by idly while its business interests are attacked. As discussed above, corporations are allowed to take defensive protective measures as long as they do not violate existing international or domestic law. However, it is important to reiterate that a corporation must tread lightly as the law clearly does not allow a company to initiate cyber hostilities. As most corporate lawyers lack the technical aptitude to properly attribute a cyber incident or to understand the appropriate response, their advice in the face of hostilities should err on the side of caution. More specifically, the best course of action for a corporation is to contact the government to respond on the corporation's behalf.

Of course, this requires a strong partnership between the government and the private sector. Unfortunately, in the United States this partnership is in its infancy and is complicated by a host of problems, including distrust between the private and public sector, corporate reputational concerns, potential liability caused by a cyber incident, and sensitivity of operating in a global economy.[205] This complex web of issues incentivizes both public and private actors to hew to their own interests, withhold critical information, and make decisions without consultation. As a result, the response to any cyber hostilities typically leaves the victimized corporation damaged, unsatisfied, and frustrated.[206]

The government is not obtuse to this problem and has taken steps to better coordinate a response to hostile cyber activities while simultaneously promoting information sharing between the public and private sectors. On February 25, 2015, the Director of National Intelligence, as ordered by the President, established the Cyber Threat Intelligence Integration Center.[207] The Center, intended to be "a national intelligence center focused on 'connecting the dots' regarding

---

205 This Article does not delve into the complex and rapidly evolving nature of cybersecurity insurance. However, all too often companies buy cybersecurity insurance thinking that this will be of value dealing with a cyber incident that occurs abroad, only to learn that this is not the case. Please feel free to email Daniel Garrie (daniel@lawandforensics.com or dgarrie@zeklaw.com) if you would like to learn more about these issues.

206 *See, e.g.*, Devlin Barrett & Danny Yadron, *Sony, U.S. Agencies Fumbled After Cyberattack*, WALL ST. J. (Feb. 22, 2015, 4:43 PM), http://www.wsj.com/articles/sony-u-s-agencies-fumbled-after-cyberattack-1424641424 (discussing how there are major shortcomings in how the government and companies work together to respond to cyber hostilities and in particular the hack of Sony Entertainment).

207 *See* Press Release, White House Office of the Press Sec'y, Fact Sheet: Cyber Threat Intelligence Integration Center (Feb. 25, 2015), https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests," has the mission of assisting "relevant departments and agencies in their efforts to identify, investigate, and mitigate those threats."[208] Additionally, on February 13, 2015, the President issued an Executive Order to promote private sector cybersecurity cooperation by authorizing greater intelligence sharing while protecting business confidentiality.[209] While these efforts are a significant step in the right direction, they are insufficient for handling the ever-growing cyber threat to corporations. Instead, a sufficiently robust public-private cyber partnership will require considering more radical ideas.

For example, a corporation that is the victim of a cyber incident must feel comfortable disclosing information to the government. However, a corporation that shares information with the government may face irreparable damage to its reputation and immense present or future customer claims through its disclosure. Only by creating a confidential reporting mechanism, coupled with limiting financial liability, will corporations be willing to openly report a cyber incident. One possibility is to adopt a regulatory regime similar to that imposed on financial institutions following the passage of the Patriot Act.[210] Currently, a financial institution must notify the Financial Crimes Enforcement Network of any transactions suggestive of criminal behavior, money laundering, or terrorist financing by filing a suspicious activity report (SAR).[211] To encourage this reporting, the Bank Secrecy Act was instituted to prohibit "financial institutions from disclosing the contents of a SAR or even its existence."[212] Other banking regulations "expand this confidentiality privilege and shield financial institutions from liability for reporting such activity."[213] By shielding SAR-reporting activity from "discovery in civil litigation" and limiting the financial liability of a corporation that reports suspicious activity, information sharing dramatically increased between financial institutions and regulators.[214] This regulatory model is useful for those interested in increasing public-private information sharing involving cyber incidents as corporations have the same concerns as financial institutions when they file a SAR.

---

208 *Id.*

209 Exec. Order No. 13,691, 80 Fed. Reg. 9,349 (Feb. 13, 2015).

210 USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

211 *See* GARRIE & SILBER, *supra* note 13, at 16; FINCEN, THE SAR ACTIVITY REVIEW—BY THE NUMBERS (2007), http://www.fincen.gov/news_room/rp/files/sar_by_numb_08.pdf.

212 GARRIE & SILBER, *supra* note 13, at 16 (citing 31 U.S.C. § 5318(g)(2)(A)(i) (2012)).

213 *Id.* (footnote omitted) (citing 12 C.F.R. § 21.11(k) and 31 U.S.C. § 5318(g)(3)).

214 *Id.* at 16–17.

Another possibility is to expand the powers of the Federal Intelligence Surveillance Court (FISC) to allow companies to petition for a government response to cyber offenses committed against their interests. Presently in the United States, the FISC is responsible for issuing warrants for domestic surveillance of suspected foreign operatives in the United States.[215] But imagine a scenario whereby an American corporation in the aerospace industry is hacked and all investigations point to the responsible party being an agent of a sovereign nation. While the corporation may be able to recover fiscally through insurance policies, the damage caused by the hack to the company may be of permanent significance. Currently, there are few options for the victimized corporation. But with an expansion of the FISC, the aggrieved corporation would be able to petition a government body for redress. The government body, acting on behalf of the corporation, would make a special appeal for emergency action. If the expanded FISC agreed that action was necessary, the government actor would be permitted to take action against the sovereign nation with impunity. One possible variant of this idea would be to create a stand-alone cyber court to provide judicial oversight of the response rather than adding cyber jurisdiction to the FISC.

These two relatively unexplored recommendations are not intended to be a panacea for the corporate cyber problem but rather illuminate the need for creativity in developing a response strategy. It will take unorthodox solutions to remove the disincentives currently inhibiting the public-private partnership. Yet, the importance of enhancing this public-private partnership cannot be overstated and is of utmost importance for both corporations and the national security of the United States. Neither corporations nor the government can afford to remain static as the speed and ferocity of cyber hostilities, in particular those launched by state actors against private companies, are the new normal. Former U.S. Secretary of Defense Leon Panetta succinctly summarized both the opportunities and threats created by the increased dependence on cyber operations when he stated:

> Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers. The Internet is open. It's highly accessible, as it should be. But that also presents a new terrain for warfare. It is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens. . . .

---

215 *Foreign Intelligence Surveillance Court*, ALLGOV, http://www.allgov.com/departments/department-of-justice/foreign-intelligence-surveillance-court?agencyid=7206 (last visited Jan. 19, 2016).

> But the even greater danger—the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states [or] violent extremist[] groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.[216]

While the importance of cyberspace is obvious, the sobering truth is that cyber hostilities discussed by Secretary Panetta are now a reality. This could not be more clearly demonstrated than by the actions of North Koreans against Sony. It is time to stop reacting to these attacks and instead proactively develop a comprehensive response strategy built upon a corporate-government partnership.

---

216 Leon E. Panetta, U.S. Sec'y of Def., Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.