# The Exceptionalist's Approach to Private Sector Cybersecurity: A Marque and Reprisal Model

By
Michael Todd Hopkins
B.A., June 2000, University of Nevada, Reno
J.D., May 2003, Southern Methodist University

A Thesis submitted to

The Faculty of
The George Washington University Law School
in partial satisfaction of the requirements
for the degree of Master of Laws
August 15, 2011

Thesis directed by
Gregory E. Maggs
Interim Dean; Professor of Law

Acknowledgement

I wish to thank Interim Dean Gregory E. Maggs for his feedback and comments in this endeavor. Any errors or omissions are solely that of the author.

## Disclaimer

Major Michael T. Hopkins serves in the U.S. Air Force Judge Advocate General's Corps. This paper was submitted in partial satisfaction of the requirements for the degree of Master of Laws in National Security and U.S. Foreign Relations at The George Washington University Law School. The views expressed in this paper are solely those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense or United States Government.

Abstract

The Exceptionalist's Approach to Private Sector Cybersecurity:

A Marque and Reprisal Model

As practitioners and academics debate our nation's cybersecurity policy the focus remains upon our national security interests as the federal government lacks the resources and people to protect all areas of society. However, this approach largely ignores the private sector despite an estimated global loss of one trillion dollars annually to cyberattacks and exploitations. Moreover, current domestic and international law do little to provide self-defense options for the private sector. Private entities cannot utilize Article 51 of the U.N. Charter as they are not a member of the United Nations. The European Convention on Cybercrimes lacks the global acceptance required to provide enforcement of its provisions and deterrence from future attacks. The Computer Crimes and Fraud Act, designed to protect computers from cyberattacks and cyber-exploitations, does not exclude computers engaged in illegal conduct from the definition of a "protected computer." Further, the act does not provide any self-help remedy for those victimized by an attack. These shortcomings leave victims of cyberattacks and exploitations helpless in defending against such attacks.

To respond to this cybersecurity gap, this article uses Professor David Post's Exceptionalist and Unexceptionalist as a framework in the debate over cybersecurity. This article notes that previous cybersecurity policies were based upon an Unexceptionalist approach; that is, applying laws of the physical world to cyberspace. These policies have failed to gain wide acceptance because the laws in the physical world do not scale to cyberspace. I propose an Exceptionalist approach to the private sector

cybersecurity gap. I recommend the government authorize private entities to engage in uses of force, consistent with the Constitution and international law, to provide the private sector adequate means to defend against cyberattacks and exploitations. This model is patterned after letters of marque and reprisal used effectively in the infancy of the United States, but long-since outmoded in the world today. This article argues that modeling a policy after letters of marque and reprisal results in a body of law scalable to the uniqueness of cyberspace. In reaching this opinion, I examine the prior use of letters of marque and reprisal by the United States. In regulating "cyberteers," Congress should limit responses to three levels of force that could be regulated by of an agency under the Department of Homeland Security. The three levels of authorized force would correspond to increasing evidentiary burdens before action could be taken, ranging from probable cause to clear and convincing evidence. This article then examines the legality of the proposal under international and domestic law. Under international law, I examine the applicability under the U.N. Charter and the Hague Convention (V). Under domestic law, I examine concerns regarding individual privacy rights pursuant to the Fourth Amendment and other relevant privacy acts. Finally, this article concludes that while the proposal is constitutional and conforms to international and domestic law, the major hurdle to its implementation is the Unexceptionalist's unwillingness to recognize that cyberspace is unique and requires an Exceptionalist's approach.

Table of Contents

# Introduction

*Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies.*[1]

In September 2010, William Lynn, the Undersecretary of Defense stated that America cannot retreat behind a Maginot Line of firewalls.[2] This referred to the current "accepted" policy of passive defenses such as regularly updating software with the latest patches, using firewalls, and employing antivirus protection. The analogy can be expanded. The French, during World War II, failed to account for the potential of Germany flanking the Maginot Line and invading France from Belgium. Like France entering into World War II, the government has reinforced its "cyber-fortifications" where it sees the greatest concern—attacks on, and infiltration of computer networks used by the government and entities designated as "critical infrastructure." This fails to account for the possibility of attackers "flanking" government or critical infrastructure networks and attacking the computer systems of major corporations creating public concern, or worse, fear that the government cannot protect the country from a cyberattack.[3]

In late 2008 through early 2010, twenty-five hundred companies around the world, including over 30 large energy, technology, defense, and financial companies in

[1] William J. Lynn III, *Defending a New Domain*, 89 FOR. AFF. 100 (Sep./Oct. 2010).
[2] *Id.* at 99. The Maginot Line was a static defense along the board between France and Germany and focused on what France saw as the greatest threat (an invasion from Germany).
[3] *See generally Annual Threat Assessment of US Intelligence Community for the S. Select Comm. on Intelligence*, 111th Cong. 3 (2010) (statement of Dennis Blair, Director of National Intelligence) available at http://www.dni.gov/testimonies/20100202_testimony.pdf) (noting, the information stolen from public and private sector computers undermines confidence in the computer systems and the information stored).

the United States, fell victim to a sophisticated and coordinated cyber-exploitation.[4] The exploitation, called Operation Aurora, sought proprietary corporate data including e-mails, credit card transaction information, and login information.[5] Operation Aurora represented what many believe to be a fundamental shift in cyberattacks and exploitation. It was considered the first major highly orchestrated cyber-exploitation against entities other than the government, military, or defense industry base and was "designed to infect, conceal access, siphon data or, even worse, modify data without detection."[6] Operation Aurora used a social engineering technique called "phishing" to gain access to businesses. Phishing entails the attacker sending out e-mails in an attempt to entice unsuspecting victims to click on a weblink or open an attached file. When a user unwittingly clicks on the link or file from the e-mail, malware is installed and executed on the computer allowing the attacker to gain unauthorized access to that computer system. After taking over one computer, the attacker uses the exploited computer's user profile to send messages to others within the organization giving the appearance that the e-mail came from a trusted source.[7] In Operation Aurora, e-mails sent by the attacker enticed other users to click on links appearing to be a trusted website. After clicking on the link, the user was directed to a website hosted in Taiwan that downloaded malicious

[4] Ellen Nakashima, *Large Worldwide Cyber Attack Is Uncovered*, Wash. Post, Feb. 18, 2010, at A03.
[5] *Id*.; George Kurtz, *Operation "Aurora" Hit Google, Others*, MCAFEE BLOG CENTRAL (JAN 14, 2010 3:34 PM) http://siblog.mcafee.com/cto/operation-"aurora"-hit-google-others/ (According to McAfee, the attack was so named "Operation Aurora" because "'Aurora' was part of the filepath on the attacker's machine that was included in two of the malware binaries that we have confirmed are associated with the attack. That filepath is typically inserted by code compilers to indicate where debug symbols and source code are located on the machine of the developer.").
[6] Kurtz, *supra* note 5.
[7] Michael Arrington, *Google Defends Against Large Scale Chinese Cyber Attack: May Cease Chinese Operations*, TechCrunch (Jan. 12, 2010), http://techcrunch.com/2010/01/12/google-china-attacks/ (last visited on May 11, 2011).

code exploiting a previously unknown vulnerability in Microsoft's Internet Explorer.[8] The attackers encrypted the original malicious code placed on the computers to conceal its detection.[9] The code, once executed, created a hidden backdoor that allowed the hacker to gain unauthorized access to the infected computers' operating systems at their leisure.[10]

Google was one of the U.S. companies victimized by Operation Aurora. Google publicly announced that it was a victim of a cyberattack on January 12, 2010.[11] It announced that the attacks, originating from China, sought and successfully accessed Gmail accounts of Chinese human rights activists.[12] It is unknown whether Google conferred with the U.S. government before making the announcement. In any event, the announcement resulted in a highly politicized exchange between the U.S. and Chinese governments.[13] After Google's announcement, Secretary of State Hillary Clinton declared, "States, terrorists and those who would act as their proxies must know that the United States will protect our networks."[14] She added, "Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government and our civil society."[15]

Google subsequently enlisted the help of the National Security Administration (NSA) to better understand how the cyber-exploitation occurred and identify actions to

---

[8] Kurtz, *supra* note 5.
[9] Kim Ketter, *Google Hack Attack Was Ultra Sophisticated, New Details Show*, WIRED (Jan. 14 2010 8:01 PM), http://www.wired.com/threatlevel/2010/01/operation-aurora/ (last visited May 11, 2011).
[10] *Id*.
[11] David Drummond, *A New Approach to China*, THE OFFICIAL GOOGLE BLOG (JAN. 12, 2010 3:00 PM), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.
[12] *Id*.
[13] John Markoff et al., *In Digital Combat Us Finds No Easy Deterrent*, N.Y. Times, Jan. 26, 2010, at A.
[14] *Id*.
[15] *Id*.

minimize the chances of it recurring.[16] Weeks after Google's initial announcement, the investigation found the attacks allegedly were launched from two Chinese schools touted as premiere computer science schools; one of which is closely associated with the Chinese military in the Shandong Province.[17] While tracing the attack back to the schools was a major breakthrough, it raised more concerns than it answered. Debates ensued within the computer security industry and the U.S. government as to whether the schools were a front for Chinese government activity or merely decoys by the actual attackers.[18] Another source close to the investigation noted that the attack was conducted by a variety of entities including consultants, contractors, and six Chinese hackers.[19] What remains unclear to the public is whether any action has or will be taken by the U.S. government against those individuals and entities. Due to the lack of clear attribution, the U.S. government refrained from further responding to the incident. As for the arrangement between Google and the NSA, the agreement remains confidential.[20] Critics questioned whether a private company like Google should be sharing its data and practices with the government.[21]

What is clear, however, is that Google will unlikely have any legal recourse unless the people or entities involved have sufficient ties to the United States to subject them to the court system. It is also unlikely that the U.S. government will take any further public action beyond the condemnation by Secretary of State Clinton.

---

[16] Ellen Nakashima, *Google to Enlist NSA to Help It Ward Off Cyberattacks*, Wash. Post, Feb. 4 2010, at A01.
[17] John Markoff & David Barboa, *2 China Schools Said to Be Tied to Online Attacks*, N.Y. Times, Feb 18, 2010, http://www.nytimes.com/2010/02/19/technology/19china.html.
[18] *Id*.
[19] *See* Ellen Nakashima, *Security Pros, Consultants Wrote Code to Attack Google; 'Hack for Prestige' Servers at Technical Schools in China Used*, Wash. Post, Feb. 20 2010, at A09.
[20] Ellen Nakashima, *supra* note 16, at A01.
[21] *Id*.

Additionally, any retribution by Google other than vacating the Chinese market likely would require U.S. government approval due to the assistance of the NSA and the sensitivity of relations between the United States and China. The full extent of the long-term consequences may never be realized. The immediate cost to Google, however, was the decision to vacate the Chinese market, a drop in its shares by roughly one percent on the day of the announcement, and a 14 percent increase in the stock price of its Chinese competitor, Baidu.[22]

Microsoft's dominance in the operating system market makes it subject to continual attacks on its software and networks. Until 2010, Microsoft collaborated with major computer security companies and Internet service providers to combat the most serious malware attacks through passive measures.[23] In 2003, for example, Microsoft offered a quarter of a million dollars for information leading to the arrest and conviction of the author of the self-replicating worm Conficker.[24] Microsoft offered similar rewards for other malware attacks such as Blaster, MyDoom, and Sobig.[25] Despite the monetary award offered, the authors of the malicious code never were caught.[26] In September 2010, Microsoft took a different approach to combat the Waledac botnet targeting the Microsoft Windows operating system. Instead of monetary awards or turning to the NSA, it took legal action to shut down the websites acting as command and control for the botnet. Microsoft obtained injunctive relief against 27 unnamed "John Does" in the District Court of Eastern Virginia. The injunction compelled VeriSign, the

---

[22] *See* Jessica Guynn, *Chinese Hacking Risk Seen as Dire; Cyber Attacks on Google, Other Firms Alarm U.S. Officials*, L.A. Times, Jan. 15 2010, at A1.
[23] Maggie Shiels, *Microsoft Bounty for Worm Creator*, BBC NEWS, (Feb. 13, 2009 8:42:34 GMT), http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/7887577.stm.
[24] *Id*.
[25] *Id*.
[26] *Id*.

manager of the ".com" top-level domain, to remove 276 Internet domains used by the Waledac botnet.[27] Like Operation Aurora, Waledac operated by sending spam e-mail to people enticing them to click on a link. That link took the unsuspecting recipient to one of the 276 domain names identified in the Microsoft complaint. Then malicious code was downloaded to the person's computer altering the Microsoft Windows operating system. This allowed the botnet to control computers as zombies and created a virtual army to do the bidding of the botnet operator.[28] This had multiple effects on Microsoft and its users. The infected computers operated slower for the owner because the resources were consumed by the botnet. The computers also may have unwittingly participated in criminal activity. Finally, the botnet lowered consumer confidence in the safety and security of Microsoft products, thereby directly affecting Microsoft.

Microsoft based its pleadings upon a plethora of federal laws, including the Computer Fraud and Abuse Act (CFAA), the CAN-SPAM Act, and the Electronic Communications Privacy Act among others.[29] Microsoft successfully petitioned the court to seal the proceedings until VeriSign could remove the domain names that would sever the communication between the command and control servers and the zombies. This prevented the botnet operators from learning of the legal action and rerouting the

---

[27] Nick Wingfield & Ben Worthen, *Microsoft Battles Cyber Criminals*, Wall St. J., Feb. 26 2010, at A3. *See also*, Declaration of Andre M. Dimino in Support of Application of Microsoft Corporation for an Emergency Temporary Retraining Order and Order to Show Cause re Preliminary Injunction at 4, Microsoft v. John Does 1-27, (E.D. Va., 2010) No 1:10CV156 (Andre Dimino, President of The Shadowserver Foundation, an organization that tracks and reports on malware and electronic fraud, best described the importance of terminating the domain names. The Waledac domain names (all ending in .com) "act as a distribution point for the Waledac malware and other related files that they host. Links to these domains are often sent out in the Spam e-mails in which they utilize social engineering tactics to trick people into visiting their URLs from the e-mails. [] The domains also serve as a fall back mechanism for the Waledac malware should it not be able to contact any of the seeded IP addresses.").

[28] Complaint, at 10-11 Microsoft v. John Does 1-27, (E.D. Va., 2010) No 1:10CV156.

[29] William Jackson, *Can We Fight Cyber Crime Like the Untouchables Fought Capone?*, GOVERNMENT COMPUTER NEWS (Sep. 10, 2010), http://gcn.com/articles/2010/09/13/cybererye-targeting-the-head-of-cybercrime.aspx?sc_lang=en.

communications to other servers before VeriSign could revoke the domain names. This would have thwarted the entire effort by Microsoft making the injunction worthless.[30] Despite the effort expended to shut down 276 domain names, some argued that it only represented a small portion of the top-level domains used by Waledac to control unsuspecting computers and had no lasting effect.[31] From a legal standpoint, some may question whether the effort and expense invested by Microsoft was justified. The entire process took several months only to obtain injunctive relief. Microsoft's burden to obtain the injunctive relief was arguable increased with the hurdles of notice requirements to shadowy defendants eluding the long-arm of the law. Despite the cost and effort, Microsoft found this to be an effective means of combating the botnet and on February 9, 2011, it initiated a second lawsuit against 11 unnamed defendants who allegedly own domain names exercising control over the "Rustock" botnet.[32]

Businesses are not the only entities targeted, however. During the 2008 presidential campaign, both Barrack Obama and John McCain were victims of a cyber-exploitation where the attack stole large amounts of digital files from both candidates.[33] Another example of a highly sophisticated cyber-exploitation targeted the Dalai Lama and the Tibetan Government-in-Exile in 2008 and 2009. Although not an attack on a U.S. entity, the GhostNet cyber-exploitation offers additional insight into cyberattacks and exploitation against private entities. The GhostNet investigation remains unique in several ways. First, the offices of the Dalai Lama provided almost complete access to the

[30] Wingfield & Worthen, *supra* note 27, at A3. *See generally*, Microsoft Corporation's Motion for a Protective Order Sealing Documents, Microsoft v. John Does 1-27, (E.D. Va., 2010) No 1:10CV156.
[31] Wingfield & Worthen, *supra* note 27, at A3.
[32] Complaint, Microsoft v. John Does 1-11, (W.D. Wash., 2011) No C11-0222JLR.
[33] Jaikumar Vijayan, *Report: Obama, McCain Campaign Computers Were Hacked by 'Foreign Entity'*, ComputerWorld, November 5, 2008 12:00 PM ET, http://www.computerworld.com/s/article/9119221/Report_Obama_McCain_campaign_computers_were_hacked_by_foreign_entity_ (last visited May 12, 2011).

computer systems—a luxury not generally given by private businesses protective of tradecraft and intellectual property or by the government when attacks involve classified systems.[34] Second, the investigators were free to interview many of the people within the offices to learn more about their computer security habits.[35] Third, the investigators had a history of documented attacks on the Tibetan computer systems dating back to 2002.[36] This included prior samples of malware used against the Tibetan group as well as the means used to deploy the malware on the networks. With this background, investigators watched as the malware operated in real-time to examine how the malware functioned over a 10-month period in 2008. To gain greater insight into the command and control of GhostNet, investigators established a "honey pot" computer to attract the attackers.[37] This enabled the investigators to trace-back the malware to several servers in the Hainan province in China.[38] After tracing back the attacks, the investigators gained access to the command interface of the attackers' control server and watched as infected computers reported to the control server. This helped the investigators identify other infected computers outside the Tibetan group to understand the magnitude of the GhostNet operation.[39] While this hack-back would be unlawful under current U.S. laws, the investigators were non-U.S. persons operating outside of the United States.

GhostNet infected nearly 1,300 computers in over 100 countries, 30 percent of which were considered high-value targets.[40] Consistent with Operation Aurora and the Waledac botnet, GhostNet relied on social engineering over the Internet to take initial

[34] *Tracking GhostNet: Investigating a Cyber Espionage Network*, THE SECDEV GROUP, 14 (2009) http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.
[35] *Id*. at 14.
[36] *Id*. at 17.
[37] *Id*. at 30.
[38] *Id*. at 5 & 7.
[39] *Id*. at 18.
[40] *Id*. at 5.

control of an unsuspecting computer.[41] Then, similar to Operation Aurora, GhostNet used familiar e-mail addresses to send malware to other computers increasing the probability those users would open the e-mail and execute the malware.[42] GhostNet created a backdoor in which the attackers could come and go as they pleased siphoning information stored on the computer. The program used by the attackers provided the ability to access all the files on the infected computers, make screen captures, capture audio, use the webcam, and force the computer to download and run other malware.[43] The investigators determined that of 34 commercially available anti-virus programs, only 11 would have recognized the malware in the document sent to the Dalai Lama's office.[44]

It appears the GhostNet attackers were after personal contact information of people assisting the Offices of Tibet. In one instance, a member of the Drewla, an online outreach project advocating for the Tibetan situation in mainland China, was held for two months and extensively questioned by the Chinese intelligence agency about her employment in Dharamsala (the location of the Tibetan Government-in-Exile). When she denied involvement with the organization, the interrogators then showed her copies of online chats with the organization.[45] Despite this indication of Chinese involvement, the investigators did not draw a direct link to the Chinese. This was due to the inability of attributing a particular attack to a person, entity, or government and determining the motive of the attackers. The investigators could neither conclude that the attackers had the intent to exploit the accessible information nor determine if the Chinese were at the

[41] *Id*. at 5-6.
[42] *Id*. at 6.
[43] *Id*. at 34.
[44] *Id*. at 18.
[45] *Id*. at 28.

center of the attacks.[46] Although the investigation did not reach a conclusion as to who was behind the exploitation or why the particular computers were targeted, it points to a broader concern regarding cybersecurity. The offices of the Dalai Lama, similar to the other exploitations described above, resulted from social engineering schemes preying on unsuspecting computer users. That, coupled to unsecured computer networks, provided the attackers with unfettered access to sensitive information.[47]

In the physical world, one would expect the government to protect its citizens from such attacks. But in the network of networks known as cyberspace, borders do not exist and the quickest path between A and B may not be a straight line.[48] This borderless medium compounds the problem by blurring the distinction between military and civilian targets.[49] In a world where economic might is arguably as powerful as military might, the need to ensure cybersecurity of the private sector is at a zenith. Crippling an economy by launching cyberattacks on a few select commercial targets is just as powerful as marching an army across one's borders. Unfortunately, current federal laws designed to protect computer systems from unauthorized access, prohibit those attacked from performing a "hack-back." This places private entities at the mercy of the government that has implicitly acknowledged an inability to protect civilian computer networks. Since both the private sector and the government have a vested interest in the security of e-commerce, the questions become who should be responsible to protect

[46] *Id*. at 1.
[47] *Id*. at 5.
[48] For that matter, the same message being sent over the Internet may not even take the same path to reach its destination. David Tubbs et al., *Technology and Law: The Evolution of Digital Warfare*, 76 INT'L L. STUD. 7, 9-10 (2002).
[49] *See* John Markoff et al., *supra* note 13, at A.

private sector networks, who is best suited to do so, and to what extent should the government be involved. Answering these questions requires an Exceptionalist approach.

In Professor David Post's article *Against "Against Cyberanarchy,"* he challenges Professor Jack Goldsmith's proposition that physical-world jurisdictional laws readily translate to the a-geographical world of cyberspace.[50] Professor Post contends that the "Unexceptionalism" advanced by Professor Goldsmith is based upon two beliefs. First in cyberspace activity is "functionally identical to transnational activity mediated by other means."[51] Second, due to the functional equivalency, the "'settled principles' and 'traditional legal tools' of the international lawyer are fully capable of handling [legal issues] in cyberspace."[52] The "Exceptionalist," on the other hand, believes that cyberspace is unique from the physical world in certain ways.[53] While there are fundamental similarities between the physical world and cyberspace, there are also fundamental differences preventing physical world laws from "scaling" to cyberspace.[54] Taking the Exceptionalist view of cyberspace, this paper advocates passage of federal legislation, consistent with the Constitution and international law, authorizing private entities to employ the use of force in cyberspace to defend against private sector cyberattacks modeled after letters of marque and reprisal formerly issued to private vessels to defend against maritime threats. After outlining a proposal for government authorized private sector use of force, and the legality of such a proposal under international and domestic law, I conclude that such a novel proposal would likely fail to

---

[50] David G. Post, *Against "Against Cyberanarchy"*, 17 Berkeley Tech. L.J. 1365, 1369 (2002).
[51] *Id*. at 1365-66 (citing Jack L. Goldsmith, Against Cyberanarchy, 65 U. Chi. L. Rev. 1199, 1240 (1998)).
[52] *Id*. at 1366.
[53] *Id*. at 1368.
[54] *Id*. at 1376-81 (discussing Religious Tech. Ctr. v. Netcom On-line Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995) and how "settled" law of copyright infringement in the physical world did not translate into cyberspace).

gain substantial support. This proposal, jettisoning many of the notions of the laws in the physical world, would fail to gain the support of the Unexceptionalists, despite a lack of existing laws to protect the private sector from cyberattacks and exploitations. For many Unexceptionalists, the step to embracing a marque and reprisal approach remains too great.

Part I develops the various problems currently inhibiting the successful implementation of a cybersecurity policy for the private sector. Among them are a non-cohesive national cybersecurity policy, inadequate resources and means to protect the private sector, and federal laws that prohibit private entities from engaging in actions tantamount to self-defense. This section then provides a brief overview of the structure of the Internet. It then discusses the differences between cyberattacks and cyber-exploitations. Part I concludes with an examination of the "attribution problem" and how it and the Convention on Cybercrimes fail to defend against cyberattacks and exploitations on the private sector.

Part II advocates the need to authorize the use of force for private entities to provide private sector cybersecurity. In advocating for a private sector remedy, this section will first identify the requirements for an effective cybersecurity strategy. Then it examines the use and effectiveness of letters of marque and reprisal during the formation of the United States as a template for a private sector cybersecurity program. After reviewing letters of marque and reprisal, I then advocate for federal legislation, modeled after letters of marque and reprisal, that would allow government authorization for private sector uses of force in limited situations. Finally, Part II examines possible concerns of such a program and the effectiveness of such a program.

Part III looks at the legality of private sector intervention in a cybersecurity program. This section examines the ramifications of the government authorization of a private sector response under international and domestic law. It highlights concerns with such a proposal and responses to alleviate those concerns.

## I. Inadequacy of Cybersecurity for Private Commercial Networks

*This status quo is no longer acceptable—not when there's so much at stake. We can and we must do better.*[55]

### A. The U.S. Lacks a Cohesive Cybersecurity Policy

The examples identified in the Introduction highlight the cybersecurity gap that has developed in America. To demonstrate the gravity of the situation, a 2008 study by McAfee and Purdue University noted that of one thousand companies surveyed the average loss per company of intellectual property was $4.6 million and over $1 trillion is lost globally each year.[56] Despite President Obama's speech on securing the U.S. cyber infrastructure, his administration has taken little action to confront the growing concern over the vulnerabilities of cybersecurity. This inaction is due to a lack of consensus on a solution and a concern that insufficient legal authority exists to justify the defense of

[55] Press Release, White House, Remarks by the President on Securing Our Nation's Cyber Infrastructure, (May 29, 2009), available at http://www.whitehouse.gov/the_press_office/Remark s-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

[56] MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 1 (2008) http://resources.mcafee.com/content/NAUnsecuredEconomiesReport; David DeWalt, *Unsecured Economies – A Trillion Dollar Headwind*, MCAFEE BLOG CENTRAL (JAN. 29, 2009, 5:53 PM), http://blogs.mcafee.com/corporate/ceo-perspectives/unsecured-economies-%E2%80%93-a-trillion-dollar-headwind.

private sector networks.[57] This highlights what Paul Rosenzweig defines as an "organizational deficit" within America's cybersecurity policy.

The organizational deficit as a two-fold problem. First, there is a lack of structure necessary for making a comprehensive cybersecurity policy that encompasses all relevant areas of cybersecurity. Second, the means to implement policy decisions do not exist and there is no effective way of monitoring the programs currently in place.[58] This organizational deficit resulted from patchwork policies developed over the last 20 years by individuals who lack adequate cybersecurity expertise.[59] Furthermore, turf-battles among departments and agencies fighting for a cyber mission add to the patchwork. While agencies battle over who should protect government domains and critical infrastructure, nongovernment domains and computer systems falling outside the category of critical infrastructure remain at risk.[60]

Currently, the military controls all security aspects over the ".mil" domain. Although much of the cyber technology possessed by the Department of Defense (DoD) and the NSA is classified, the information available to the public indicates the United States possesses powerful cyber weapons.[61] Yet, the Posse Comitatus Act prohibits the use of the military to carry out domestic laws.[62] The military may only intervene during instances of emergencies rising to the level of loss of life and wanton destruction of

---

[57] Ellen Nakashima, *US Cyber-Security Strategy Not Yet Solidified*, Wash. Post, Sep. 17, 2010, at A03.
[58] Paul Rosenzweig, *The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence*, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 246 (Nat'l Res. Council, 2010).
[59] William C. Banks & Elizabeth Rindskopf-Parker, *Introduction*, 4 J. Nat'l Security L. & Pol'y 7, 9 (2010).
[60] Michael Chertoff, *Foreword*, 4 J. Nat'l Security L. & Pol'y 1, 3 (2010) (identifying the non-protected addresses to include the ".com," ".edu," ".net," and ".org" extensions); *Critical Infrastructure and Key Resources Sectors*, DHS.GOV, http://training.fema.gov/EMIWeb/IS/ IS860a/CIKR/sectorMenu.htm (last visited Mar. 7, 2011).
[61] *See* Nakashima, *supra* note 57, at A03.
[62] Use of Army and Air Force as Posse Comitatus, 18 U.S.C. § 1385 (1994).

property during civil disturbances, disasters, or calamities or when a state or local government lacks the ability to protect federal property.[63] Yet if the United States was attacked by a cyberwar, the military may not have the resources to protect military, government, and civilian assets if an exception to the Posse Comitatus Act was permitted. Most importantly, outside of a cyberwar, we cannot rely upon the military to provide protection without blurring the lines between traditional military and civilian roles.

The Department of Homeland Security (DHS) protects the ".gov" domain and 18 sectors of "critical infrastructure."[64] Despite owning this role, DHS lacks the funding, resources, and expertise necessary to protect all critical infrastructures, let alone all private sector networks.[65] Consequently, the NSA assumed the role indirectly by launching a program called "Perfect Citizen" designed to protect selected areas of the critical infrastructure.[66] The limited information available to the public regarding Perfect Citizen indicates that it monitors sensors placed into government and private sector critical infrastructure computer networks. These sensors would alert the NSA after detecting abnormal activity.[67] Currently the program lacks the ability to monitor all critical infrastructure networks continuously. Some critics have argued that the NSA is impermissibly encroaching into domestic affairs raising concerns about what data is collected and how it is used. This has ignited a debate over the proper balance between security interests and the individual's privacy interests.[68] Currently, these options do not

[63] 32 C.F.R. § 215.4 (2010).
[64] Chertoff, *supra* note 60, at 3 & 5.
[65] Rosenzweig, *supra* note 58, at 263.
[66] Paul Rosenzweig, *10 Conservative Principles for Cybersecurity Policy*, Heritage Foundation Backgrounder no. 2513, 6 (2011), http://thf_media.s3.amazonaws.com/2011/pdf/bg2513.pdf. *See also* Siobhan Gorman, *U.S. Plans Cyber Shield for Utilities, Companies*, Wall St. J., July 8, 2010, at A03 (noting that currently there is little public knowledge of the program or the extent of its use).
[67] Gorman, *supra* note 66 at A03.
[68] *Id*.

offer a solution to the cybersecurity issues plaguing private sector networks falling outside of critical infrastructure.

B. Current Federal Laws Forbid Private Sector Response

The current federal laws addressing cyberattacks and cyber-exploitation can best be described as a patchwork of laws. Many are antiquated and only have limited applicability to the cyberspace that exists today. While an in-depth analysis of all applicable laws is well beyond the scope of this paper, this section will set forth the major impediments preventing private sector entities from adequately defending themselves. This section focuses on three laws in particular that restrict the actions of private individuals from tracing back cyberattacks and cyber-exploitation. Those are the Neutrality Act, the Logan Act, and the Computer Fraud and Abuse Act. This section will also address the Economic Espionage Act and its limitations in protecting the private sector and conclude by briefly examining problems with the Convention on Cybercrimes, the only international treaty addressing cybercrimes.

The Neutrality Act and Logan Act were enacted to ensure the U.S. responded with "one voice" on U.S. foreign affairs. President Washington issued a Proclamation on April 22, 1793 prohibiting American citizens for aiding or abetting hostilities against any nation currently at peace with the United States.[69] This largely mirrored a similar prohibition under the law of nations. However, it proved difficult to enforce and the following year Congress passed the Neutrality Act of 1794 codifying the principle found

[69] A Proclamation by the President of the United States of America, George Washington (Apr. 22 1793), reprinted in 1 AMERICAN STATE PAPERS, Foreign Relations 140 (W. Lowrie & M. Clarke eds. Washington, D.C. 1832).

under the law of nations.[70] It was initially passed as a temporary measure but was permanently enacted on April 24, 1800 and remains in effect today codified under 18 U.S.C. § 960.[71] The Neutrality Act intended to prevent private citizens from initiating, within the United States, military-like activities with a country currently at peace with the United States.[72] Case law has interpreted "military enterprise" as consisting of three essential elements. First, there must be an organized body acting in concert and unity together. Second, that body must employ "weapons of some kind." Finally, the body must act under command or leadership.[73] The court did not qualify the term "weapons of some kind," leaving open the option that weapons could be non-kinetic in nature. Further, "military enterprise" was defined broadly and not limited to individuals wearing uniforms or insignia.[74]

Under this description of military enterprise, a victim of a cyberattack, located within the United States, engaged in any "active defense" or self-defense measures that amounted to aggression would presumably violate the Neutrality Act. Moreover, the countermeasures used need not be destructive in nature to fall under the Neutrality Act as espionage constitutes a military enterprise.[75] Spies initiating their covert activity within the United States and directing those activities toward a nation at peace with the United States violates the Act as it is a martial undertaking, involving "the idea of a bold,

---

[70] Jules Lobel, *Covert War and Congressional Authority: Hidden War and Forgotten Power*, 134 U. Pa. L. Rev. 1035, 1061 (1986). *See* Neutrality Act, ch. 50, 1 Stat. 381-84 (1794) (codified as amended at 18 U.S.C. §§ 958-960 & 962 (1976)).
[71] Jules Lobel, *The Rise and Decline of the Neutrality Act: Sovereignty and Congressional War Powers in United States Foreign Policy*, 24 Harv. Int'l L.J. 1, 1 n.2 (1983).
[72] *See* Expedition Against Friendly Nation, 18 U.S.C. § 960 (2006).
[73] United States v. Nunez, 82 F. 599, 601 (C.C.S.D. N.Y. 1896).
[74] *Id*.
[75] United States v. Sander, 241 F 417, 420 (S.D.N.Y. 1917).

arduous, and hazardous attempt" against that other nation.[76] Additionally, the statute is not limited strictly to groups of individuals. A single individual engaged in a military enterprise against another nation at peace with the United States violates the act.[77]

The Logan Act addresses private citizens negotiating with another nation without consent of the government.[78] After the French Revolution, President John Adams sent an envoy to France to improve U.S. diplomatic relations.[79] Diplomatic talks failed and Vice President Jefferson secretly sent Dr. George Logan, a private citizen, to France in an attempt to negotiate peace.[80] While he successfully brokered a deal, President Adams was infuriated that a citizen independently spoke on behalf of the United States. President Adams requested Congress to take action against "temerity and impertinence of individuals affecting to interfere in public affairs between France and the United States."[81] Congress subsequently passed a law criminalizing the act of a U.S. citizen negotiating with another nation without the authority of the United States.[82] Although there has yet to be a prosecution under the Logan Act, more than ten cases make reference to the Logan Act—the most recent being in 2001.[83]

Congress enacted the CFAA in 1984 in an attempt to stymie the rising number of computer fraud cases. The act was last revised in 2002 and contains seven categories of

---

[76] *Id.* (citing Wiborg v. United States, 163 U.S. 632, 650 (1896)).
[77] *Id.*
[78] Private Correspondence with Foreign Governments, 18 U.S.C. § 953 (2000).
[79] Michael V. Seitzinger, *Conducting Foreign Relations Without Authority: The Logan Act*, CRS Rep. for Cong. 2 (2006).
[80] *Id.*
[81] 1 MESSAGES AND PAPERS OF THE PRESIDENT 267 (Richardson ed., 1897).
[82] 9 ANNALS OF CONG. 2489 (1798); Seitzinger, *supra* note 79, at 3. The Logan Act is now codified under 18 U.S.C. § 953.
[83] *See* Seitzinger, *supra* note 79, at 3-9; United States v. DeLeon, 270 F.3d 90, 94 (1st Cir. 2001) (the court referenced the Logan Act while discussing 8 U.S.C. § 1326 regarding previously deported aliens illegally attempting to return to the United States).

criminal activity relating to computers.[84] In 1994, Congress amended the CFAA adding the term "protected computer."[85] This extended the protection of the CFAA to certain non-government computers.[86] Congress amended the CFAA two more times, once in 1996 and most recently in 2001 pursuant to the USA PATRIOT Act. The PATRIOT Act expanded the term "protected computer" to include financial institutions, the government, or computers "used in 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."[87] In other words, the definition, as modified, protects computers located within or outside the United States, assuming the computer or network is connected to the Internet.[88]

The legislation also handicapped the victims of cyberattacks and exploitation. Although in certain situations the CFAA permits the victim to file suit in civilian court for damages, it does not permit a victim to trace-back the attack to a perpetrator or to engage in a counter-attack.[89] A civilian suit is meaningless when the attacker is beyond the legal reach of the act. The legislation also protects the cyberattacker from being subject to a trace-back, or hack-back, as the definition of protected computer does not exclude computers being used for unlawful purposes.[90] Simply amending the CFAA to exclude computers used in unlawful purposes would exacerbate the problem unless effective controls were placed on the conditions of a hack-back to prevent vigilantism.

---

[84] OFFICE OF LEGAL EDUC., DOJ, PROSECUTING COMPUTER CRIMES 2 (2006) available at http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf [hereinafter COMPUTER CRIMES MANUAL].
[85] *Id*. at 3.
[86] *Id*.
[87] Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1030(e)(2) (2008).
[88] *See* COMPUTER CRIMES MANUAL, *supra* note 84, at 3-4.
[89] *Id*. at 3.
[90] *See generally* 18 U.S.C. § 1030.

There are at least four provisions under the CFAA that bar trace-back or the use of active defenses. Those provisions include, 1) knowingly and intentionally accessing a protected computer without authorization or exceeding the individual's authorization; 2) knowingly and with the intent to defraud, access a protected computer; 3) knowingly and without authorization, cause the transmission of a program, information, code, and commands thereby causing intentional damage to a protected computer; and 4) intentionally accessing a protected computer without authorization, and thereby causing damage and loss.[91]

"Damage" under the CFAA broadly encompasses "any impairment to the integrity or availability of data, a program, a system, or information."[92] To demonstrate the breadth of the term, below are three instances where damage would be satisfied under CFAA. The first scenario entails a trace-back involving the changing or deleting files or information stored on a protected computer.[93] A second example involves a hacker changing the way the computer would normally operate, such as changing the permissions allowed on a computer to give the perpetrator access to areas otherwise forbidden to the hacker.[94] Finally, any actions that disable access to a computer through means other than altering the computer code, such as a denial of services attack, constitute damage.[95] Because the CFAA did not provide for self-defense carve-out

[91] *See* 18 U.S.C. § 1030(a)(2)(C), (4), (5)(A), (5)(C).
[92] 18 U.S.C. § 1030(e)(8).
[93] COMPUTER CRIMES MANUAL, *supra* note 84, at 34-35.
[94] *Id*. at 35 (citing United States v. Middleton, 231 F.3d 1207, 1213-14 (9th Cir. 2000)).
[95] *Id*. (citing, YourNetDating v. Mitchell, 88 F. Supp. 2d 870, 871 (N.D. Ill. 2000) (court granted temporary restraining order against defendant who installed code on plaintiff's web server diverting users of the website to a pornographic website).

provisions, any person or entity attempting to trace-back an attack to the perpetrator will violate the CFAA.[96]

While the CFAA specifically addresses computer-related crimes, the Economic Espionage Act (EEA) of 1996 more broadly addresses economic exploitation of government and private sector. Specifically, its purpose was to protect against proprietary information and trade secret theft involving clear instances of intent to defraud.[97] The EEA has two sections for prosecuting economic espionage. Section 1831 applies to knowing transfers of proprietary information to a foreign government.[98] Under section 1831, mere negligent or reckless transfer of information is insufficient for successful prosecution.[99] Section 1832, criminalizes the knowing or intentional transfer of trade secrets to a domestic or foreign entity.[100] The act defines trade secret broadly encompassing tangible and intangible items either written or graphical, so long as the owner took measures to keep the information secret and the information has actual or potential economic value.[101] Since the EEA is a criminal statute, each element requires proof beyond a reasonable doubt creating a high evidentiary threshold in order for the government to obtain a conviction. That being said, the government has successfully prosecuted individuals under both sections.

Companies have voiced various concerns with the EEA. The most prominent concern involves further disclosure of sensitive information. While the government may petition for a protective order to prevent further release of sensitive information, that

---

[96] *See* Rosenzweig, *supra* note 58, at 261.
[97] James M. Fischer, *An Analysis of the Economic Espionage Act of 1996*, 25 Seton Hall Legis. J. 239, 240 & 260 (2001).
[98] *See* Economic Espionage Act, 18 U.S.C § 1831(a) (2000).
[99] Fischer, *supra* note 97, at 259.
[100] *See* Economic Espionage Act, 18 U.S.C § 1832 (2000).
[101] *See* Economic Espionage Act, 18 U.S.C § 1839(3) (2000).

same privilege does is not extend to corporate victims.[102] Several entities, including the American Society for Industrial Security (ASIS), claim that the inability for private parties to obtain a protective order to prevent sensitive information from further leaks deters victimized companies from reporting and perusing a claim under the EEA.[103] Another disincentive to reporting involves the proceeds obtained from the stolen trade secrets. Under the EEA, the United States, and not the injured party, receives the profits from any sale of information obtained through the economic espionage if the defendant is convicted.[104] This is in addition to any fine imposed against the entity convicted of proprietary information or trade secret theft.[105] ASIS believes any property forfeited should be given to the injured entity as a means of preventing any additional injury.[106]

C. The Convention on Cybercrime Fails to Provide Adequate Deterrence

International law also fails to adequately advance a cybersecurity policy for the private sector. The European Union Convention on Cybercrime became effective on January 7, 2004. It was hailed as a major step in forming a comprehensive treaty on cyberspace issues and is the only international convention to do so.[107] The Convention only addresses the private actor's criminal conduct, therefore state actor misconduct is not addressed.[108] The three primary goals it sets forth are: 1) harmonizing domestic criminal law statutes regarding cybercrime matters, 2) ensuring domestic criminal

---

[102] Fischer, *supra* note 97, at 265.
[103] *Id*.
[104] Economic Espionage Act, 18 U.S.C § 1834 (2000).
[105] *See* Economic Espionage Act, 18 U.S.C § 1831 & 1832 (2000).
[106] Fischer, *supra* note 97, at 265.
[107] Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 167, available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (ratified by the United States in 2006); COUNCIL OF EUROPE, SUMMARY OF THE CONVENTION ON CYBERCRIME, http://conventions.coe.int/ Treaty/en/ Summaries/Html/185.htm (last visited Jan. 12, 2011). The Convention requires the signatories to implement certain legislation to criminalize the actions describe within the treaty.
[108] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 Lewis & Clark L. Rev. 1023, 1052 (2007).

procedures are in place to investigate and prosecute such crimes, and 3) creating a regime for international cooperation.[109] The Convention applies criminal definitions and evidentiary standards to four different categories of prohibited conduct. They include: 1) offences against the confidentiality, integrity, and availability of computer data and systems; 2) computer-related offences; 3) content-related offences; and 4) offences related to infringements of copyright and related rights.[110] To gain wide acceptance, the Convention elected to define these categories of prohibited acts broadly. This allowed each member to have its domestic law comply with broader goals rather than require members to enact specific domestic legislation.[111] This places the impetus for passing and enforcing the necessary laws upon the individual member states.[112] Consequently, it fails to create a consistent standard of laws across all member states.

As of May 2011, only 30 states are members of the Convention and 17 states have signed but have not ratified the Convention.[113] No members are from Asia, Africa, or South America, making the Convention regional in nature.[114] Notable states that have not ratified the Convention include Japan and China (non-member states of the Council

---

[109] *See* Council of Europe, Convention on Cybercrime, Explanatory Report, C.E.T.S. No. 185, ¶ 38 (Nov. 8, 2001), http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
[110] *See generally* Convention on Cybercrime, *supra* note 107.
[111] Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. Rev. 65, 81 (2009).
[112] *See generally* Convention on Cybercrime, *supra* note 107.
[113] Convention on Cybercrime, CETS No. 185, Status, at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=01/04/2011&CL=ENG (visited on Jan 20, 2011) [hereinafter Cybercrime Status].
[114] Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 220 (Nat'l Res. Council, 2010).

of Europe) and Russia (a member state).[115] Due to the small number of ratifying states, the Convention lacks substantial credibility within the international community.

The Convention does not have any means of enforcement of its provisions *per se*.[116] Consequently, the Convention does little to close the gap on non-state cyberattacks or cyber-exploitation directed towards private sector entities. In fact, countries that are a party to the Convention may refuse to assist if it would prejudice its sovereignty, *ordre public*, or essential interests.[117] Access to data and information relevant to an investigation can also be severely restricted. Although authorization is not required to access any publicly available computer data, any information stored on a private computer system requires the requesting party receive authorization from the owner of that network and data system.[118] This can add considerable delays in identifying the owner of the network and seeking consent to search. While recognizing the right to privacy is paramount in the United States and in other countries, without a reasonable means for member states to compel access to private networks, victim states have little hope in conducting an investigation in a timely manner where a private party refuses to grant access. Extradition imposes an additional impediment. A member state may refuse to extradite a perpetrator. Extradition, even with our close allies, remains less than certain.[119] When that occurs, the victim state must affirmatively request the non-

[115]Cybercrime Status, *supra* note 113 (China is neither a member nor a non-member state of the Council of Europe. Interestingly, Georgia, which was victim to a cyberattack in August 2008 has signed the Convention on January 4, 2008 (before the attack) but has yet to ratify the Convention).
[116] Vatis, *supra* note 114, at 217.
[117] Convention on Cybercrime, *supra* note 107, arts. 27(4), 29(5), & 30(2).
[118] *See* Convention on Cybercrime, *supra* note 107, art. 32.
[119] Planning for the Future of Cyber Attack: Hearing Before the Subcomm. on Technology and Innovation of the H. Comm. on Science, Space, and Technology, 111th Cong. 3 (2010) (noting the cybercrime case of Gary McKinnon, who is still awaiting extradition from England after 8 years) available at http://gop.science.house.gov/Hearings/Detail.aspx?ID=244.

extraditing state to prosecute the offense.[120] This places the victim state at the mercy of the non-extraditing state. Depending on the laws of the non-extraditing state, it may be harder to attain a conviction for the charged offense or if a conviction is obtained the resulting sentence may be lighter.

D. Cyberattacks and Cyber-Exploitations

"Cyberspace" as defined by the DoD is, "[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[121] Stated differently, cyberspace is the inter-connectivity of various networks ranging in type and sizes, independent of physical geography, and includes the mechanisms enabling communication between them. This inter-connectivity, or redundancy, was a core design of the Internet to ensure no single point of failure.[122] Consequently, geographical borders do not easily translate in cyberspace.[123]

The Internet uses packet switching to send information from one point to another.[124] Packet switching breaks the transmission into "chunks" of information with identifying information encoded in the header of the packet at the origination point.[125] Each packet is sent independently of each other "jumping" from node to node getting

---

[120] Convention on Cybercrime, *supra* note 107, art. 24 ¶ 6.
[121] JOINT CHIEFS OF STAFF, JOINT PUBLICATION 1-02, DEP'T OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 92 (as amended through Dec. 31, 2010), http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf [hereinafter DOD DICTIONARY].
[122] Tubbs et al., *supra* note 48, at 9-10.
[123] *See* David R. Johnson & David Post, *Law and Borders -- The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1370 (1996).
[124] *See* PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 19 (4th ed. 2011).
[125] *See Id*. at 18. An example of the header information includes: the sender and recipient information of the message, date and time of the transmission, and the position of the packet in the series of the packets for the message. Tubbs et al., *supra* note 48, at 9-10.

"closer" to its destination.[126] The transmission may be routed through nodes in any city of any country, oblivious to geographical borders.[127] Once the packets reach their destination they are reassembled based upon the header information.[128] Because the information in the packet header will ensure the transmission is reassembled in the proper order, the packets do not need to, and often do not, arrive in the same order as they left or take the same path while in transit.[129] This method of data transport is used in all transmissions over the Internet.

This paper uses cyber-exploitation and cyberattacks as the two general categories of hostile intrusion against computers and networks.[130] Cyber-exploitation, also referred to as cyberespionage, is the exploitation of a vulnerability on another computer system or network by offensive actions usually to conduct and carry out intelligence-obtaining missions by targeting information stored or transiting through that system or network.[131] When carrying out these intelligence-gathering missions they may occur instantaneously or over a span of time.[132] By definition, cyber-exploitation is nondestructive and does not seek to disrupt or disturb the networks or the computers infiltrated.[133] A successful cyber-exploitation remains unnoticed before, during, and after achieving its goal.[134] Herbert Lin identifies three primary objectives of cyber-exploitation: 1) the exploitation

---

[126] Tubbs et al., *supra* note 48, at 9-10 (The transmission of packets is based upon time between the origination and destination as opposed to physical distance. Packet routing takes into account network traffic loads, to determine the quickest route.
[127] *See* BELLIA ET AL., *supra* note 124, at 18. *See also* Johnson & Post, *supra* note 123, at 1372-73.
[128] Tubbs et al., *supra* note 48, at 10.
[129] *Id*. at 7-10.
[130] TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 10 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin, eds., 2009), available at http://www.nap.edu/openbook.php?record_id= 12651&page=1 [hereinafter Cyberattack Capabilities].
[131] *Id*. at ix & 11. *See* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. Nat'l Security L. & Pol'y 63, 64 & 67 (2010).
[132] Cyberattack Capabilities, *supra* note 130, at ix & 11. *See* Lin, *supra* note 131, at 64 & 67.
[133] Lin, *supra* note 131, at 63; Cyberattack Capabilities, *supra* note 130, at 11.
[134] Lin, *supra* note 131, at 63 n.2.

or exfiltration of information existing on a network, 2) the passive monitoring of network activity, and 3) the ability to carry out industrial sabotage.[135] The private sector is more susceptible to cyber-exploitation than cyberattacks, as criminals seek information that they can sell for profit. To compound the problem, barriers to entry for conducting a successful cyber-exploitation is generally lower than what is needed for a successful cyberattack.[136]

Cyberattacks, on the other hand, carry out deliberate actions, either instantaneously or over a period of time, by deploying a destructive payload "to alter, disrupt, deceive, degrade, or destroy" the information, programs, computers, or networks residing in or transiting through the targeted computers or networks.[137] A cyberattack focuses its attack on three general areas of a computer system or network: 1) the integrity or accuracy of the information, 2) the authenticity or reliability of the information, and 3) the consistency in providing results.[138] Viruses and botnets are two categories of examples. Viruses change the way programs work or potentially stop or destroy the system altogether.[139] Botnets are a network of thousands of third party computers (zombies) that act like an army under the control of an attacker

[135] *Id*. at 68-69.
[136] Planning for the Future of Cyber Attack: Hearing Before the Subcomm. on Technology and Innovation of the H. Comm. on Science, Space, and Technology, 111th Cong. 4 (2010) (Statement of Robert Knake, International Affairs Fellow in Residence, The Council on Foreign Relations) available at http://gop.science.house.gov/Hearings/Detail.aspx?ID=244.
[137] Cyberattack Capabilities, *supra* note 130, at 10-11; Lin, *supra* note 131, at 64, 69-70.
[138] Lin, *supra* note 131, at 67.
[139] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l Law 885, 891 (1999).

.[140] Botnets can engage in a plethora of illegal activity such as sending spam, committing online fraud, phishing attacks, and denial of service attacks.[141]

Cyberattacks are divided generally into two categories, cybercrime and cyberwar. Cybercrime is a cyberattack carried out by private or non-state actors.[142] Although cyberwar does not have an accepted definition, most scholars use the DoD definition of "cyber operations." Cyber operations are, "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[143] This definition focuses on the attacks by one state against another enemy state.[144] Therefore, a state-initiated cyberattack with a military objective would constitute a cyberwar. However, the international community has yet to decide if cyberattacks constitute armed conflict.[145] Several scholars advocate an effects-based approach to resolving this debate. Under an effects-based approach, one examines the effects of a computer network attack and applies it to the pre-existing legal model for use of force.[146] As this paper later discusses, this is the Unexceptionalist approach.[147] The effects-based approach can be problematic. It implies a victim state may be unable to respond until the attack concludes and the effects can be determined.

---

[140] Tyler Moore, *Introducing the Economics of Cybersecurity: Principles and Policy Options*, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 6 (Nat'l Res. Council, 2010).
[141] Moore, *supra* note 140, at 6.
[142] *See* Convention on Cybercrime, *supra* note 107.
[143] DOD DICTIONARY, supra note 121, at 141.
[144] AHMAD KAMAL, THE LAW OF CYBER-SPACE: AN INVITATION TO THE TABLE OF NEGOTIATIONS 9 (2005). However, some define the cyberwar as the attacking nation either being a state or non-state actor. *See* MARTIN C. LIBICKI, CYBERDETERENCE AND CYBERWAR 117 (2009), available at http://www.rand.org/ pubs/monographs/ 2009/RAND_MG877.pdf.
[145] Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. Rev. 121 124, (2009).
[146] Lin, *supra* note 131, at 73.
[147] *See generally* Post, *supra* note 50, at 1365.

Due to the commonalities between cyber-exploitations and cyberattacks they can easily be mistaken for each other.[148] The similarities can cause confusion for policy makers and responders attempting to determine whether an act qualifies as a cyberattack or exploitation for each may require a different response.[149] The primary difference between the two is the nature of the payload.[150] Although by the time the payload is deployed it may be too late to thwart an attack. For example, a logic bomb is a type of malware placed on a computer or network where it remains dormant until a predefined condition occurs. At that point, the bomb is triggered and the code is executed.[151] If the logic bomb is detected while lying dormant, one may believe it to be a cyber-exploitation only later to find out it carries a harmful payload when the malicious code is executed.

E. Failure to Impose an Adequate Attribution Model

Attribution is the ability to determine who carried out the attack.[152] It serves multiple functions. Attribution is critical in establishing liability and ensuring an uninvolved government, entity, or person is not targeted in a counterattack.[153] It provides confidence to the aggrieved party that a penalty will be imposed on the proper aggressor.[154] It must also convince third parties that there is credible evidence to warrant

---

[148] Cyberattack Capabilities, *supra* note 130, at 13.
[149] *Id*.
[150] Lin, *supra* note 131, at 64.
[151] Schmitt, *supra* note 139, at 891. An example of a logic bomb is the Stuxnet worm. While referred to as a worm, the most current information about Stuxnet indicates that it was designed only to be triggered under a certain configuration of controllers running a Siemens software that only appeared to match the that found in Iran. *See* William J. Broad et al., *Israel Tests Called Crucial In Iran Nuclear Setback*, N.Y. Times, Jan. 16, 2011, at A0.
[152] Knake, *supra* note 136, at 2; DEP'T OF DEFENSE OFF. OF GEN. COUNS., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 21 (2nd ed, Nov. 1999) (available at www.cs.georgetown.edu/~denning/ infosec/DOD-IO-legal.doc) [hereinafter GC ASSESSMENT]. (The perpetrator could be another state, an agent of that foreign state, an agent or a group not associated with a government, or a private individual acting alone).
[153] Yoram Dinstein, *Computer Network Attacks and Self-Defense*, 76 INT'L L. STUD. 99, 109 (2002).
[154] *See* LIBICKI, *supra* note 144, at 41.

a response against the suspected aggressor.[155] Attribution may also deter an aggressor from launching an attack if he believes the attack will be attributed to him.[156] Attribution seeks to determine whether the perpetrator is a state or non-state actor—a critical element in determining the appropriate response.[157] For non-state actors, domestic criminal law is applied which requires proof beyond a reasonable doubt that the defendant was the individual who actually committed the act. For state actors, attribution must be+ sufficient to justify the necessity of self-defense pursuant to the Law of War and the U.N. Charter.[158]

In cyberspace, attributing the attack to the attacker is generally more difficult and usually more time consuming than in the physical world.[159] There is considerable debate as to the normative level of attribution required in the cyber realm before a victim state may legitimately respond.[160] Cyberattackers do not "fly a flag" of their nationality. Cyberattacks do not require geographic proximity.[161] Attacks can originate from cybercafés, unsecured WiFi locations, or anywhere in the world with Internet access.[162] The design of the Internet promotes anonymity and perpetrators can mask the origin of packets easily.[163] Unlike military radar systems, no technology exist to detect the

---

[155] *Id*. at 67.
[156] *See Id*. at 41.
[157] Eric T. Jensen, *Computer Attacks on Computer National Infrastructure: A Use of Force Invoking the Right of Self Defense*, 38 Stan. J. Int'l L. 207, 232-33 (2002).
[158] Dinstein, *supra* note 153, at 109.
[159] *See* Stephen Dycus, Congress's Role in Cyber Warfare 4 J. Nat'l Sec. L. & Pol'y 155, 163 (2010); David E. Graham, Cyber Threats and the Law of War, 4 J. of Nat'l Sec. L. & Pol'y 87, 92 (2010).
[160] LIBICKI, *supra* note 144, at 67. *See* Knake, *supra* note 136, at 4.
[161] Robert K. Knake, *Internet Governance in an Age of Cyber Insecurity* COUNCIL ON FOREIGN RELATIONS, 13 (Council Special Report No. 56, 2010), http://i.cfr.org/content/publications/attachments/Cybersecurity_CSR56.pdf.
[162] LIBICKI, *supra* note 144, at xvi. It is important to note that computer network attacks are not limited to attacks through the Internet. Many attacks are carried out by networks not connected to the Internet. *See* Knake, *supra* note 136, at 2. Lynn, *supra* note 1, at 97 (noting the attack on the DoD system was by a thumb drive).
[163] Knake, *supra* note 161, at 13.

origination of an attack in real-time or give fair warning of an incoming attack.[164] Even if the origination of an attack is located, it cannot determine who was behind the computer at the time of the attack. Additionally, as the investigators noted in GhostNet, it can be difficult to trace-back to the single event that placed the malicious code on a computer or network.[165] Consequently, it is difficult to determine whether the code was placed on the network hours, days, months, or even years earlier.[166] Cyberattackers have the ability to go relatively undetected. Attacks can easily portray themselves as coming from another location altogether, an act known as spoofing[167] or by hijacking computers in other locations to launch an attack.[168] This is a major concern for the United States as it worries about being tricked into believing an attack originated from a particular state where in fact it originated in another location by another entity.[169] Assuming *arguendo*, that attribution can be traced back to the attacker, that alone does not guarantee deterrence from future attacks if the attacker has little to lose.[170] Due to many of these difficulties, states restrict themselves by requiring conclusive attribution before responding and by limiting any response to passive measures such as firewalls and

[164] *Id.*
[165] THE SECDEV GROUP, *supra* note 34 at 18.
[166] *See* Todd, *supra* note 111, at 93.
[167] David A. Wheeler & Gregory N. Larsen, *Techniques for Cyber Attack Attribution*, INSTITUTE FOR DEFENSE ANALYSES, 18 (Oct. 2003), http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859.
[168] *See* Todd, *supra* note 111, at 99.
[169] Markoff et. al., *supra* note 13, at A.
[170] *See* Knake, *supra* note 136, at 2.

antivirus programs.[171] Some area experts are now looking for alternatives to a conclusive attribution requirement.[172]

## II. A Proposed Model for Private Sector Cybersecurity

*Settled law, and received principles, are worthy of respect; but at times they need to be reconsidered. This is one of those times.*[173]

The difficulty of cyberspace is that the medium does not neatly fit into any existing legal paradigm.[174] Attempts by Unexceptionalists to apply the Economic Espionage Act, the Computer Fraud and Abuse Act, or even the Convention on Cybercrimes fail to provide an effective policy of deterrence and security for the private sector because the physical world principles embodied in these laws simply do not scale to cyberspace. In order to respond to this growing problem, the wheel does not need to be reinvented. All that is needed is a body of laws from the physical world that is scalable to the unique issues of cyberattacks and exploitations on the private sector. Those scalable legal principles are found in letters of marque and reprisal that used private entities regulated by the government to protect against hostile attacks on U.S. merchantmen's goods and vessels. This system provides the flexibility and scalability necessary for an effective private sector cybersecurity program.

---

[171] Graham, *supra* note 159, at 92.
[172] David D. Clark & Susan Landau, *Untangling Attribution*, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 25 (Nat'l Res. Council, 2010) (advocating the inclusion of user identification information in a future version of the Internet); Graham, *supra* note 159, at 93 (advancing the idea of imputed responsibility on the state's own citizens as well as all non-state actors committing cyberattacks); Jensen, *supra* note 157, at 236 (advocating active defenses to protect computer networks).
[173] Post, *supra* note 50, at 1387.
[174] *See generally* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. Chi. Legal F. 207 (1996).

A. Marques and Reprisals as a Template for the Private Sector Cybersecurity

If private entities are to assume the role of defending the private sector, the current laws must be modified to provide the latitude needed to effectively respond to cyberattacks and exploitations. But simply amending the current laws would create greater problems than the private sector is currently facing. That would foster a vigilantism approach to cybersecurity. Those believing they were the victim of a cyberattack or exploitation may feel inclined to attempt hack-backs without having the proper technical and legal background. This could easily result in a less secure Internet. Having private entities provide cybersecurity requires a balance between regulation and flexibility to respond. It also requires legal principles that, when taken from the physical world, are scalable to the uniqueness of the Internet. With those considerations in mind, we examine the use and effectiveness of letters of marque and reprisal as a possible template for a viable private sector cybersecurity policy.

1. History of Marques and Reprisals

Letters of marque and reprisal, as embodied in the United States Constitution, are the merger of two separate, but related, legal concepts: letters of reprisal and letters of marque. A specific letter of reprisal would be issued to an individual for injuries to that person, whereas a general letter was issued to a group of private citizens for injuries to the state by a foreign state or its citizens. In the former case, the letter authorized the holder to confiscate the seized property if the perpetrator did not compensate the victim.[175] In the latter instance, the letter was only a license to take the goods of the

[175] HARRY WHEATON, ELEMENTS OF INTERNATIONAL LAW 310, 311 n.151 (George Grafton Wilson ed., 1936) (1866). *See also* J. Gregory Sidak, *The Quasi War Cases -- And Their Relevance to Whether Letters of Marque and Reprisal Constrain Presidential War Powers*, 28 Harv. J.L. & Pub. Pol'y 465, 472 (2005).

foreign enemy.[176] Congress would then pass corresponding legislation that provided the authority to seize property.[177] This authority to seize property was rooted in the law of nations. Despite this authority, letters of reprisal were lawful only within the sovereign's jurisdiction.[178]

A letter of marque, on the other hand, was a legal authorization for private individuals to cross national borders for redress of damages.[179] However, it functioned similarly to letters of reprisal. Letters of marque were issued generally when diplomatic means failed in order to provide the individual a remedy for the injury while avoiding a formal declaration of war between the two states.[180] Letters gave commercial vessels legal authority to use force to protect against attacks.[181] Nations with weak navies also issued letters of marque to protect national interests on the high seas and along the coast.[182] The letters did not necessarily increase its military might. Rather, the effectiveness of the privateer was in harassing and disturbing the enemy's commercial shipping industry thereby hampering a belligerent's war efforts.

Between the seventeenth and nineteenth centuries, governments began issuing letters of marque and letters of reprisals in tandem.[183] This freed the individual from jurisdictional limits and permitted reprisals wherever he may find the offending foreign

---

[176] Ingrid Wuerth, *The Captures Clause*, 76 U. Chi. L. Rev. 1683, 1738-39 (2009).
[177] *Id*.
[178] Sidak, *supra* note 175, at 473.
[179] Lobel, *supra* note 70, at 1043; Sidak, *supra* note 175, at 473.
[180] Theodore M. Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. Mar. L. & Com. 221, 245 (2009); 2 JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES 94 (Melville M. Bigelow ed., William S. Hein and Co. 1994) (1891).
[181] Theodore T. Richard, *Reconsidering the Letter of Marque: Utilizing Private Security Providers Against Piracy*, 39 Pub. Cont. L.J. 411, 437 (2010).
[182] Robert P. DeWitte, *Let Privateers Marque Terrorism: A Proposal for a Reawakening*, 82 Ind. L.J. 131, 133 & 135 (2007).
[183] Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation*, 45 Harv. Int'l L.J. 183, 211 (2004).

nation or subject.[184] This gave private entities the authority to defend themselves on the high seas while providing the government with monopolistic control over warfare by prohibiting "private wars" unless specifically authorized and regulated by the government. Privateers emerged as the primary entity to use letters of marque and reprisal. A privateer was a vessel owned and armed by private individuals holding a letter to seize enemy cargo and vessels.[185] The letters required the holder to post bond and submit to prize courts in order to transfer title to the privateer.[186] The letters typically included an expiration date and a specific limit on the value of goods to be seized.[187] Captures made by privateers after the letters expired were treated as acts of piracy.[188] Governments frequently imposed restrictions on the amount or type of force permitted, the type of vessel marked for capture or attack, and conditions on treating captives.[189] Privateers acting within the bounds of a valid letter received immunity from criminal prosecution not only from the issuing state, but also by other nations that honored the letters out of reciprocity.[190]

On April 3, 1776, the Continental Congress passed a resolution authorizing the use of letters of marque and reprisal during the Revolutionary War.[191] The newly formed nation lacked a fleet of vessels necessary to combat the British Royal Navy and lacked

---

[184] Lobel, *supra* note 70, at 1042-43. *See also*, William M. Treanor, *Fame, the Founding, and the Power to Declare War*, 82 Cornell L. Rev. 695, 708 (1997); Sidak, *supra* note 175, at 473.
[185] Hooper v. United States, 22 Ct. Cl. 408, 428-429 (1887).
[186] THEODORE DWIGHT WOOLSEY, INTRODUCTION TO THE STUDY OF INTERNATIONAL LAW 208 (Theodore Salisbury Woolsey ed., 6th ed. 1891); Kontorovich, *supra* note 183, at 218.
[187] Sidak, *supra* note 175, at 473.
[188] *Id*.
[189] See Matthew J. Gaul, *Regulating the New Privateers: Private Military Service Contracting and the Modern Marque and Reprisal Clause*, 31 Loy. L.A. L. Rev. 1489, 1501 (1998).
[190] Kontorovich, *supra* note 183, at 213; 216-17.
[191] 4 JOURNALS OF THE CONTINENTAL CONGRESS, 1774-1789, at 252 (Worthington Chauncey Ford ed., G.P.O. 1906) (1776).

sufficient funds to build a navy had it wanted to do so.[192] Privateers added approximately 70,000 men and between 800 to 2,000 armed vessels.[193] This dwarfed the Continental Navy, which possessed between 53 and 64 vessels.[194] While the purpose of the letters was to target the shipment of British war materiel to the colonies, the greatest benefit of privateering proved to be the disruption and harassment the British sea commerce.[195]

The effect of the marques and reprisals on the British economy was astounding. In 1778, it was reported to the House of Lords that over the previous two years 733 vessels were captured by the colonies.[196] That represented a loss of £1,800,633.[197] Moreover, the privateers virtually destroyed the West Indie trade. Britain's estimated loss in trade topped 66 percent largely due to the increase in insurance premiums on vessels, delays in shipping, and falling prices of rum and sugar.[198] While privateering proved devastating to the British economy, it functioned as a boon for local colonial economies.[199] By raiding British merchant vessels, privateers effectively broke the British blockade by supplying port towns with captured goods and opening up a source of goods for the new nation.[200] In turn, privateers would spend their profits in the port towns propping up the local economies.[201]

For all the advantages privateering offered the fledgling nation, issuing letters of marque and reprisals were not without concerns. Several neutral nations complained

---

[192] Sidak, *supra* note 175, at 474; William Young, *A Check on Faint-Hearted Presidents: Letters of Marque and Reprisal*, 66 Wash. & Lee L. Rev. 895, 908 (2009).
[193] C. Kevin Marshall, *Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars*, 64 U. Chi. L. Rev. 953, 964 (1997); Sidak, *supra* note 175, at 474.
[194] *See* JOHN LEHMAN, ON SEAS OF GLORY: HEROIC MEN, GREAT SHIPS, AND EPIC BATTLES OF THE AMERICAN NAVY 39 (2001); Sidak, *supra* note 175, at 474.
[195] Sidak, *supra* note 175, at 474; Marshall, *supra* note 193, at 963.
[196] FRANCIS R. STARK, THE ABOLITION OF PRIVATEERING AND THE DECLARATION OF PARIS, 123 (1897).
[197] *Id*.
[198] *Id*.
[199] Young, *supra* note 192, at 903.
[200] *Id*. *See* Marshall, *supra* note 193, at 964.
[201] Young, *supra* note 192, at 903.

privateers captured vessels not specifically identified in the letters.[202] This led to anti-American sentiment with some European nations.[203] Due to the lure of money, some claimed privateers were siphoning would-be naval recruits and stealing experienced seamen from the navy.[204] This also prompted concern that privateering corrupted the public morals.[205] Many argued that the privateers charged inflated fees for their captured and scarce goods to the people at port.[206] Opponents of privateering saw it as being synonymous to piracy.[207]

To counter some of these concerns, Congress required privateers to post bond and submit to prize court hearings to determine legal title of captured goods. In 1798, the United States based the bond amount upon the size of the crew. A $7,000 bond was required for vessels with 150 men or less and $14,000 for vessels with more than 150 men.[208] That is equivalent to approximately $130,000 for vessels of 150 men or less and $260,000 for vessels in excess of 150 men in 2011 dollars.[209] Another means of enforcing proper conduct were prize courts. Prize courts determined who would receive lawful title to the goods captured. Once the judge entered the decree, all other governments and entities were estopped from making claims against the captor.[210] If, on

[202] STARK, *supra* note 196, at 123-24.
[203] *See Id*. at 125.
[204] Marshall, *supra* note 193, at 966.
[205] *Id*.
[206] *Id*. at 997-98.
[207] Kontorovich, *supra* note 183, at 221.
[208] An Act to Declare the Treaties Heretofore Concluded with France, No Longer Obligatory on the United States, ch. 67, § 4, 1 Stat. 578 (1798).
[209] Values calculated at www.wolframalpha.com using the following input computations "$7000 1798 dollars in 2011" and "$14000 1798 dollars in 2011." The exact values are $129,796.56 and $259,593.12. Values are based on the Consumer Price Index and an average inflation rate of 1.38% a year.
[210] Miller v. Resolution (*Resolution I*), 2 U.S. (2 Dall.) 1, 5 (1781).

the other hand, the court found that the capture was unlawful, the prize courts had the authority to return the captured vessel or goods and impose any damages necessary.[211]

The United States used privateers on two other occasions. The first was during the Quasi-War with France.[212] This led to legal challenges regarding the constitutionality of marques and reprisals during an undeclared war. The Supreme Court held the use of letters of marque and reprisal during an undeclared war was constitutional.[213] It also demonstrated the control Congress exerted over the type and level of permissible force.[214] The last time the United States used letters of marque and reprisals was during the War of 1812. At the outbreak of war, the United States navy consisted of seven frigates and approximately a dozen smaller vessels.[215] The Royal Navy had roughly 1,060 vessels.[216] While the letters contained many of the same provisions used during the Revolutionary War, Congress greatly limited what constituted a lawful target.[217] Additionally, special attention was given to neutral nations to prevent the appearance or

---

[211] Miller v. Resolution (*Resolution II*), 2 U.S. (2 Dall.) 19, 22 (1781).
[212] Young, *supra* note 192, at 906-907.
[213] *Bas*, 4 U.S. at 41 (opinion of Washington, J.) ("[I]t is said, that a war of the imperfect kind, is more properly called acts of hostility, or reprizal, and that congress did not mean to consider the hostility subsisting between France and the United States, as constituting a state of war . . . . [However,] the degree of hostility meant to be carried on, was sufficiently described without declaring war, or declaring that we were at war. Such a declaration by congress, might have constituted a perfect state of war, which was not intended by the government.").
[214] *See* An Act More Effectually to Protect the Commerce and Coasts of the United States, ch. 48, 1 Stat. 561 (1798); An Act to Authorize the Defence of the Merchant Vessels of the United States Against French Depredations, ch. 60, § 1, 1 Stat. 572 (1798); An Act Further to Protect the Commerce of the United States, ch. 68, § 2, 1 Stat. 578 (1798); An Act Further to Suspend the Commercial Intercourse Between the United States and France, and the Dependencies Thereof, ch. 2, 1 Stat. 613 (1799) (The original act was entirely defensive, only permitting U.S. "armed vessels" to respond in kind to attacks initiated by the French on U.S. public and private vessels. The June act authorized the use of force for U.S. private vessels solely to combat any "search, restraint or seizure" attempted by French ships. In July 1798 Congress passed an act authorizing preemptive use of force allowing letter holders to subdue, seize, and capture any armed French vessel or recapture any U.S. vessel, goods, and effects previously belonging to United States citizens found within the jurisdiction of the United States. In February 1799, Congress passed a fourth act permitting the seizure of any American vessel bound for a French port.).
[215] STARK, *supra* note 196, at 127.
[216] *Id*. at 125.
[217] *Id*. *See* Cooperstein, *supra* note 180, at 237.

actual use of force on neutral vessels.[218] By late 1813, the British blockade severely hampered the abilities of the privateers and many gave up the profession finding the risks outweighed the rewards.[219]

2. Efforts to Restrict Letters of Marque and Reprisal

Although the United States resorted to letters of marque and reprisal as a new nation, it always expressed concern over issuing the letters and many advocated abolishing them. During Revolutionary War in the summer of 1782 and again in 1783, Benjamin Franklin proposed to his British counterpart "a proposition for improving the law of nations, by prohibiting the plundering of unarmed and usefully employed people."[220] This proposal would have prohibited privateers from attacking non-military targets. England flatly rejected his proposal.[221] Fifteen years later, Congress voiced concern that letters of marque and reprisal placed the peace of the country at the disposal of privateers who were generally without oversight while out at sea.[222] Many scholars saw reprisals as frequent preludes to war.[223] Ultimately, legislators saw the letters as unavoidable in advancing the naval operations during the Revolutionary War.[224] In 1823, the United States again pushed the international community for a prohibition on

---

[218] *Id*.
[219] Young, *supra* note 192, at 906-907.
[220] Letter from Benjamin Franklin to Richard Oswald (Jan. 14, 1783), in 9 WORKS OF BENJAMIN FRANKLIN, at 466 (Jared Sparks ed. 1839). The language of the proposal read:

> If war should hereafter arise between Great Britain and the United States, which God forbid… And all merchants or traders with their unarmed vessels, employed in commerce, exchanging the products of different places, and thereby rendering the necessaries, conveniences, and comforts of human life more easy to obtain and more general, shall be allowed to pass freely, unmolested. And neither of the powers, parties to this treaty, shall grant or issue any commission to any private armed vessels, empowering them to take or destroy such trading ships, or interrupt such commerce. *Id*. at 469-70.

[221] Kontorovich, *supra* note 183, at 220.
[222] *Id*. at 212; 7 ANNALS OF CONG. 254 & 255 (1797) (remarks of Rep. Livingston and Rep. Swanwick. Rep. Swanwick stating "it would be very difficult to regulate a power of this kind, since private interest were set to work to evade the law").
[223] 2 SAMUEL VON PUFENDORF, DE OFFICIO HOMINIS ET CIVIS JUXTA LEGEM NATURALEM 140 (Frank Gardner Moore trans., Oxford Univ. Press 1927) (1688).
[224] *See* Kontorovich, *supra* note 183, at 221.

privateering.[225] The French and Russian governments agreed, however, the British rejected the idea and the proposal failed.[226]

In 1856, seven nations concluded the Declaration of Paris.[227] It was the first major treaty to implement restrictions on conducting wars at sea.[228] It contained four basic provisions, the first being "Privateering is and remains abolished."[229] In order to ensure enforcement of all provisions, the treaty provisions were non-severable.[230] Professor Stark minimized the importance of the Declaration of Paris saying, "to call it an epoch-making event, or a red-letter day in the calendar of the Law of Nations, would be superfluous," as the treaty failed to abolish the capture of all private property at sea.[231] It is in part due to this reason that the United States never signed the Declaration.

The Declaration, however, failed to prevent private vessels from engaging in war entirely. States began converting private vessels into public vessels and outfitting them for war. As a result, the Hague Convention (VII) of 1907 attempted to clarify and set parameters for the conversion of merchant vessels to ships of war.[232] The Convention outlined six prerequisites before a civilian ship could lawfully be converted into a warship. Article 1 required a merchant ship, once converted to a warship, to be under the

---

[225] Letter from John Q. Adams, Sec. of State, to Richard Rush (Jul. 28, 1823), reprinted in 5 AMERICAN STATE PAPERS, Foreign Relations 229-33 (Gales and Seaton eds., Washington 1858) [hereinafter 5 Papers].
[226] STARK, *supra* note 196, at 41-42.
[227] Declaration of Paris, Apr. 16, 1856, 115 Consol. TS 1, reprinted in 1 Am. J. Int'l L. Supp. 89 (1907); 7 J. B. MOORE, DIGEST OF INTERNATIONAL LAW 563 (1906) (By the end of 1856 forty-three nations had acceded to the Declaration. The United States never acceded to the Declaration).
[228] Cooperstein, *supra* note 180, at 245.
[229] Declaration of Paris, *supra* note 227, art. 1. (The other provisions included the following: "2nd. The neutral flag protects the enemy's goods except contraband of war; 3rd. Neutral goods, except contraband of war, are not subject to seizure under the enemy's flag; 4th. Blockades, to be binding, must be effective; i.e., maintained by a force sufficient to render approach to the enemy's coast really dangerous.").
[230] STARK, *supra* note 196, at 143.
[231] *Id*. at 159.
[232] Gabriella Venturini, *Commentary*, in THE LAW OF NAVAL WARFARE: A COLLECTION OF AGREEMENTS AND DOCUMENTS WITH COMMENTARIES 121 (Natalino Ronzitti ed., 1988).

command of the nation whose flag was flown.[233] The Convention applied the Law of War to converted vessels and the rules of military discipline applied to the crew.[234] But like the Declaration of Paris, the Hague Convention (VII) applied only in wars where all the belligerents were party to the Convention.[235] Thirty-four states acceded to the Convention.[236] The United States, along with China, Dominica, Nicaragua, and Uruguay did not.[237]

3. Laws of Land Warfare Did Not Scale to Sea Warfare

In 1823, then-Secretary of State John Quincy Adams sent a series of dispatches to Britain discussing the possibility of forbidding the capture of private property upon the sea. He sought to bring the law of the sea in line with the laws of land warfare, which did not extend to the law of the sea at that time.[238] He noted, "by the usages of modern war the private property of an enemy is protected from seizure and confiscation as such; and private war itself has been almost universally exploded upon the land."[239] This distinction between land warfare and sea warfare continued during negotiations of the two Hague Peace Conventions in 1899 and 1907. While this distinction was largely the result of diverging opinions among the states, it was also attributed to difference in technological advancements between land and sea. No significant technological change occurred in land warfare over the previous hundred years whereas the uniqueness of the sea fostered a massive advancement in technology. Wooden sailing ships gave way to

---

[233] Hague Convention (VII) Relative to Conversion of Merchant-Ships into War-Ships, Oct. 18, 1907, art. 1, 205 Consol. T.S. 319, 325-26, reprinted in 2 Am. J. Int'l L. Supp. 133 (1908).
[234] *Id*. at arts. 4 & 5.
[235] *Id*. at art. 7.
[236] Venturini, *supra* note 232, at 122.
[237] A. PEARCE HIGGINS, HAGUE PEACE CONFERENCES AND OTHER INTERNATIONAL CONFERENCES CONCERNING THE LAWS AND USAGES OF WAR 320 (1909).
[238] Letter from John Q. Adams, Sec. of State, to Richard Rush (Jul. 28, 1823), reprinted in 5 Papers, *supra* note 225, at 531.
[239] *Id*.

"great floating metal fortresses propelled by steam power."[240] Higgins addressed this technological impact on the law stating, "The rules of maritime warfare, elaborated when wooden walls were the defence of a sea-girt state, are seen to be antiquated, and in some cases useless, when applied to modern conditions."[241] This led many scholars to conclude separate Conventions were necessary to address the unique considerations of sea warfare. A special committee was formed at the Second Hague Conference to specifically examine whether the provisions relating to the Law of War on land could apply to operations of war on the sea.[242] The committee concluded the differences were so great that law of land warfare could not apply to sea warfare without fundamental changes.[243] In other words, laws of land warfare could not scale to naval warfare.

B. Cyberteering Model

Just as merchant vessels represented the heart of the United States economy in late 1700s and early 1800s, online banks and retailers represent a significant part of the U.S. economy today. In 2009, United States online sales reached $134.9 billion.[244] Not surprisingly, cyber fraud continues to grow—from seven percent of total fraud losses in 2007 to 11 percent in 2008.[245] In 2009, the amount of online fraud reported doubled to a staggering $550 million.[246] These numbers, however, cannot reflect the economic loss resulting from consumers' lost confidence in online commerce. By scaling the legal principles used in privateering to cyberspace, the United States can formulate an effective private sector cybersecurity policy that protects our growing e-commerce.

---

[240] HIGGINS, *supra* note 237, at 87.
[241] *Id*.
[242] *Id*. at 88.
[243] *Id*.
[244] Cybersecurity, Innovation and the Internet Economy, 75 Fed. Reg. 144 (Jul. 28, 2010).
[245] *Id*.
[246] *Id*.

As no domestic law currently exists for private entities to engage in self-defense, Congress should authorize limited uses of force to private sector entities so that they may protect private sector networks. In doing so, the legislation must create a limited exception to current domestic laws prohibiting self-defense for cyberattacks. Second, Congress should authorize three distinct degrees of force for self-defense measures. Third, to administer and impose regulations and requirements, Congress should create a public-private agency falling under DHS. Finally, the legislation should establish a "cyber court" to adjudicate claims and issue warrants. This cyberteering program would be based in part upon the legal principles used in issuing letters of marque and reprisal.[247]

This policy differs from other proposed policies in four significant ways. First, as identified above, it would authorize the private sector to carry out specific measures to identify and neutralize cyber-exploitations. Second, it would address the "attribution problem" by coupling the three levels of authorized use of force to increasing degrees of evidentiary thresholds, ranging from probable cause to clear and convincing evidence. Third, modeled from prize courts, the cyber court would be analogous to an administrative hearing as opposed to the criminal court system. Finally, as with prize courts, the burden of proof would fall upon the perpetrator. Congress would be responsible for passing the legislation and authorizing the various forms of responses to cyberattacks and exploitations. The legislation would impose limited government oversight controlling the level of authorized response based upon the circumstances of the attack or exploitation. This oversight would also ensure compliance through

[247] In this paper I will refer to privateering in cyberspace as cyberteering, to mean an entity providing services to combat hostilities in cyberspace. Originally, the suffix "teer" was associated with a person involved with the military. For example, "privateer" originated from a private man-of-war, "musketeer" was a soldier armed with a musket, and a volunteer was originally one who freely offered himself for service in the military.

licensing, bonding, and reporting requirements. Finally, as a check on the actions of the cyberteers, the agency would establish Rules of Engagement (ROEs) when responding to a cyber threat or attack on a private sector entity. Violations of the ROEs by cyberteers would result in disciplinary measures from sanctions to criminal or civil liability.

1. A Different Approach to Attribution

Nothing requires the U.S. cybersecurity policy to apply a criminal law evidentiary standard to cyber attribution. This has, however, become the *de facto* standard due to political concerns. Cyber attribution merely requires effective legal mechanisms for stopping cyberattacks and exploitations as they happen and investigating those that do occur.[248] There are three paramount concerns when formulating an attribution policy for cyberspace. First, what level of certainty is needed to satisfy the attribution requirement before a responding to an attack? Second, how is that level of attribution integrated into the overall cybersecurity policy? Finally, how will the attribution policy be conveyed to potential attackers to deter their behavior?[249]

A criminal approach to cyberattacks and exploitations require the evidentiary threshold of beyond a reasonable doubt. This high standard makes the likelihood of a conviction more difficult. If convicted, however, the punishment stands to be more severe. While this evidentiary standard is readily accepted in the physical world with geographic boundaries, a growing number of experts are questioning the use of criminal standards to cybersecurity. One scholar notes, the criminal approach to a criminal activity that knows no geographic boundary is highly suspect.[250] Proposals applying a

[248] Knake, *supra* note 136, at 6.
[249] *See Id*. at 2.
[250] Banks & Rindskopf-Parker, *supra* note 59 at 9.

beyond a reasonable doubt standard to identify a cyberattacker greatly decreases the possibility that any action will be taken in response to an attack.

To demonstrate, it is worth comparing the criminal evidentiary standard to the civil injunctive relief hearing regarding the Waledac botnet. Microsoft's burden merely was to establish a lack of legal remedy available, that the harm to Microsoft was real, any potential harm to the defendants from the injunctive relief was low, and injunctive relief served a public interest.[251] This standard made it easy for Microsoft to obtain relief; however, the "penalty" to the defendants was simply losing access to the website addresses in question. Yet despite the modest restrictions imposed on the defendants, some argue such an approach is effective not because of a strict punishment, but because the probability that some response will be taken by the victim.[252] This highlights the principle of deterrence. Regardless of the form the deterrence or penalty takes, the punishment imposed must be sufficiently severe in nature to induce behavioral changes by the attacker.[253] Additionally, the penalty should compensate the victim or society for the actual or potential harm resulting from the actions of the attacker.[254] Applying these concepts to privateering shows, privateers did not need to be successful fighting the enemy at sea because they were extremely successful in frustrating the enemy by harassing the enemy's sea commerce.

---

[251] Cooper v. Tazewell Square Apts., Ltd., 577 F.Supp. 1483, 1488 (W.D. Va. 1984); Blackwelder furniture Co. v. Seilig Mfg. Co., 550 F.2d 189, 195-96 (4th Cir. 1977).
[252] Take for example studies demonstrating that when firearms are in the hands of citizens it deters potential assailants. Lawrence Rosenthal & Joyce Lee Malcolm, *McDonald v. Chicago: Which Standard of Scrutiny Should Apply to Gun-Control Laws?*, 105 Nw. U. L. Rev. Colloquy 85, 105 (2010).
[253] Geoff A. Cohen, *Targeting Third-Party Collaboration*, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 319 (Nat'l Res. Council, 2010).
[254] *Id*.

Under the criminal law model, imposing a beyond a reason doubt standard represents the Unexceptionalist's approach to cyber attribution. It is this model that is used in the Convention on Cybercrimes. Regardless of the type of cyberattack or exploitation, whether it is a phishing scam, logic bomb, or exfiltration of data off a company's server, under the criminal law approach, the same high evidentiary standard is be required before *any* response may be taken. While this standard would be acceptable if cyberattacks were initiated in the same physical jurisdiction as the location of the attack, the criminal law approach fails to scale to the ubiquitous medium of the Internet.[255] As noted in Part I.C, above, criminal investigations become infinitely harder to conduct when attempting to gain access to computer systems in other countries. Coupling the added difficulty of conducting an international investigation with the criminal evidentiary standard, decreases the probability of a successful prosecution. Finally, while a successful prosecution under the criminal law model may lead to a substantial punishment, this must be balanced against the likelihood cyberattackers and exploiters will be caught. Given the number of new exploitations announced to the public each month, many cyberattackers will likely find the rewards far outweigh the risks.

The Exceptionalist's approach inverts the first concern to a cybersecurity policy and asks, "What is the desired response to a cyberattack or exploitation?" After identifying the desired response, a burden of proof will be imposed commensurate to that degree of force. The Exceptionalist's approach balances the degree of force sought to be used in responding to the attack against the amount of evidence available at that time

[255] While preparation of a criminal act may occur in another jurisdiction, there are few instances that does not involve telecommunications where a criminal act is initiated in one jurisdiction and the effects in another.

indicating who the perpetrator was. Unlike the criminal law approach, the Exceptionalist's approach requires increasing degrees of certainty regarding the attribution of an attack to escalate the degree of force permitted. This approach, focuses on frustrating the perpetrator's actions and preventing further attacks as opposed to punishing the perpetrator for past acts committed. This is most analogous to Microsoft's injunctive relief. The goal was to prevent further use of the command and control servers for the botnet and less concerned about punishing the perpetrators. Despite the lack of punishment, this model offers a greater deterrent effect by permitting more use of force responses to thwart perpetrators from carrying out their attacks and exploitations. However, unlike the injunctive relief sought by Microsoft, the cyber courts could handle the matters quicker and more efficiently than traditional Article III courts.

This comparison demonstrates that concerns over attribution cannot be eliminated, but are greatly reduced by abandoning the criminal standard of proof and implementing a sliding scale based upon the level of force the cyberteer seeks to use. Reducing the evidentiary requirements and the severity of the punishment yields several positive results. First, it leads to a greater number of successful legal actions against perpetrators. At the same time, the cyber courts would ensure that penalties are imposed only on those individuals that have sufficient evidence demonstrating their culpability. Second, placing the burden upon the alleged cyberattacker does not infringe upon any constitutional rights of the individual nor is it an uncommon phenomenon. Even in criminal trials, the defendant will have the burden if he or she invokes certain defenses. Placing the burden upon the respondent merely forces the person or entity to show that the cyberteer targeted the wrong entity. The cyber court would also permit the

respondent to lodge any violations to seek reparations and ensure action taken by the cyber privateer meets the statutory guidelines. In Microsoft's legal action against the Waledac botnet only one individual came forward claiming that he did not have any involvement with the botnet.[256] That individual stated he was unaware his domain was used as command and control for the Waledac botnet and subsequently sold the domain name to Microsoft.[257]

While some may be concerned of implementing such an evidentiary standard in responding to cyberattacks and exploitations, the standard is not new as it is based upon the evidentiary standards formerly used in the prize courts. As noted above, members of the international community recognized the authority and evidentiary standards of each other's prize courts through reciprocity. Despite such reciprocal agreements, careful consideration must be made of the rights to be afforded and the burden to be placed on alleged perpetrators. Should a similar policy be implemented by other nations, Americans could potentially be subjected to foreign prize courts. While full examination of the potential ramifications are beyond the scope of this paper, suffice it to say that if the policy is adopted by other nations, United States citizens could quickly find themselves being subjected to uses of force for committing such offenses.

2. Legal Considerations for a Cyberteering Model

While the President may engage in military activities falling short of declared war, the impetus for a private sector cybersecurity policy would fall upon Congress. Even during the Quasi-Wars the President relied upon congressional authority to carry out the various privateering acts against the French. Additionally, Congress has the

[256] *See* Declaration of Gabriel M. Ramsey in Support of Microsoft Corporation's Status Report re Preliminary Injunction, Microsoft v. John Does 1-27, (E.D. Va., 2010) No 1:10CV156.
[257] *Id*.

power to declare war and the power of appropriation. Therefore, it must take the initiative and issue a formal resolution declaring authorized hostilities.[258] It must identify what acts the resolution is attempting to rectify as well as the entity or entities that committed the acts. Because this proposal is to provide cybersecurity to the private sector, the acts would likely include attacks or exploitations on non-state, private sector computer systems and networks. Any cyberattack or exploitation on a government or critical infrastructure asset would be beyond the scope of the proposal. Before identifying the entities, it is helpful to divide perpetrators of cyberattacks and exploitations into one of four categories: 1) a hacker or organization that resides in State A but acts independently of State A's government, 2) a terrorist of State A acting independently of State A's government, 3) a terrorist committing an act directly or indirectly sponsored by State A, and 4) an official body or agent of State A committing an act on behalf of State A.[259] The first two categories fall under non-state actors and are the focus of this proposal. The latter two categories fall squarely under state actors and are outside of the proposal's scope. By excluding state actor conduct, it largely mitigates violations of the Logan and Neutrality Acts. In particular, under the Neutrality Act, the prohibited conduct is against states, not non-state actors.[260] Additionally, the United States, has, diplomatic, economic, social, and military means at its disposal when addressing foreign nations.[261] Therefore, the federal government in the best position to address foreign relation matters involving foreign states.

---

[258] *See* Bas v. Tingy, 4 U.S. (4 Dall.) 37 (1800).
[259] Dinstein, *supra* note 153, at 103. Hackers are private entities or citizens launching cyberattacks against an adversarial nation on their own initiative without the direction or control of their nation's government. Cyberattack Capabilities, *supra* note 130, at 276.
[260] *See* Expedition Against Friendly Nation, 18 U.S.C. § 960 (2006).
[261] LIBICKI, *supra* note 144, at xix. *See also* Cyberattack Capabilities, *supra* note 130, at 16.

Admittedly, it may prove difficult for a cyberteer to determine whether a state or non-state actor committed a particular act. If actions are taken against an entity later determined to be a state actor, it could very easily cause tensions between the United States and that state. However, a system of checks should minimize the likelihood a cyberteer would engage a state actor. By placing states on notice of the cyberteering policy, it may deter state actors from conducting attacks and exploitations on private-sector. Moreover, while it is naïve to believe a state actor would never attack or exploit non-critical infrastructures in the private sector, it is unlikely they would invest time on such endeavors, as many are not high value targets to governments. Under Congress' power to declare war, it must also authorize the use and degree of force permitted.[262] Congress should implement a three-tiered use of force response regulated by a public-private agency under the DHS. The three tiers would include, trace-back, blockade or sanction, and finally, active defenses. This three-tiered response system could then be tailored to each situation based upon the nature of the attack or exploitation and the effects of the attack.

The lowest level response is a trace-back. It constitutes following the path of the attack back to the source.[263] This may involve jumping back through several layers of machines in different jurisdictions.[264] The two primary trace-back methods boast accuracies of 75 and 87 percent.[265] When conducting a trace-back, it is more important

[262] Hooper v. United States, 22 Ct. Cl. 408, 439 (1887).
[263] *See generally* Wheeler, *supra* note 167, at 17.
[264] Clark & Landau, *supra* note 172, at 31.
[265] Jay P. Kesan & Carol M. Hayes, Thinking Through Active Defense in Cyberspace, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 331 (Nat'l Res. Council, 2010) (identifying the two types of trace-backs as the direct traceroute (75 percent accuracy) and the reverse traceroute (87 percent accuracy)).

to look at the machines used for the attack rather than those who operate the machines.[266] Typically when an attacker hijacks an intermediary computer and uses it to stage a cyberattack the owner of that computer is unaware his or her computer is assisting in the attack.[267] Cyber courts should authorize trace-backs after the cyberteer presents sufficient evidence to meet a probable cause standard. This lower evidentiary standard for trace-backs parallels the standard needed to obtain a search warrant, an analogous legal tool used in law enforcement investigations. A successful trace-back may offer greater insight into the attack as well as other victimized computers or networks.[268] This information may then justify increased levels of force.

The second level of response would be the imposition of a blockade or sanction. This would require a finding by the preponderance of the evidence that the target initiated or was actively involved in the cyberattack or exploitation. In the physical world, the distinction between a blockade and a sanction is critical. Article 3 of the Definition of Aggression Resolution holds that blockades constitute a use of armed force[269] although a multilateral or unilateral economic sanction does not constitute a use of force.[270] In practice, the impact of a sanction may, however, rival that of a blockade and cause loss of life and destruction.[271] The apparent difference is in the nature of the measures. Economic sanctions are a refusal of one or more states from engaging in trade with a particular state. Sanctions only limit conduct between the sanctioning states and the sanctioned state. Non-participating states are still free to engage in any conduct with the

---

[266] Clark & Landau, *supra* note 172, at 40.
[267] *Id*. at 31.
[268] *See generally* THE SECDEV GROUP, *supra* note 34.
[269] G.A. Res. 3314, art. 3 ¶ c, U.N. GAOR 29th Sess., Definition of Aggression, Annex, Definition of Aggression, U.N. Doc. A/Res./3314 (XXIX) (1974).
[270] Schmitt, *supra* note 139, at 905.
[271] Lin, *supra* note 131, at 80.

targeted state.[272] Therefore, the sanctioned activity generally requires a multilateral effort for a sanction to be effective. This generally makes sanctions less effective than blockades.[273] A blockade, on the other hand, is usually a unilateral use of force to prohibit trade by all parties to the blockaded state regardless of their willingness to engage in trade.[274] Due to the use of force needed to maintain the blockade, they are only lawful during periods of armed conflict.[275] There have been exceptions, however. During the 2006 Israeli push into Lebanon a blockade was enforced against Hezbollah despite no formal war existing between the two.[276]

The distinctions between blockades and sanctions do not scale when applied to cyberspace. In cyberspace, distinguishing blockades from sanctions based upon use of force is problematic as what constitutes a "use of force" in cyberspace is far less settled than in the physical world. For instance, Article 41 of the Charter states any interruption of communications of a belligerent state imposed by the Security Council is not a use of force.[277] However, Michael Schmitt notes that applying Article 41 in cyberspace would be suspect. He reasons drafters did not contemplate the Internet at the time Article 41was written and to hold that blockading communications does not qualify as a use of force would be over-reaching.[278] This is one more example of a legal premise in the physical world that does not scale to cyberspace. One potential solution is to focus initially on the amount of traffic curtailed instead of the type or amount of force used. Under this analysis if the response blocks all electronic traffic, it would constitute a blockade. If on

[272] *Id*.
[273] *See Id*.
[274] Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. Int'l L. & Pol. 57, 91 (2001); Lin, *supra* note 131, at 80.
[275] LESLIE C. GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 205 (3d ed. 2008).
[276] *Id*.
[277] U.N. Charter arts. 41.
[278] Schmitt, *supra* note 139, at 912.

the other hand, it only blocked traffic to and from the perpetrator and victim, it would constitute a sanction.

Microsoft's actions revoking top-level domains would constitute an economic sanction. The injunction focused on the web addresses to disrupt the Waledac botnet. Revoking the top-level domain names would not prohibit the sanctioned party from carrying on its activities with others by establishing a different domain name through another provider. Additionally, terminating top-level domains do not necessarily require any use of force. A blockade would have occurred, however, if Microsoft initiated an action to disable the server used for command and control so that it could no longer communicate with anyone.[279]

Not all situations are as clear. In 2000, the World Trade Organization selected Conxion Inc. to provide server hosting during its annual summit. A hacker organization conducted a denial of service attack against Conxion during the conference. After tracing back the attack, Conxion was able to determine which packets came from the attacker and rerouted them back to the originating server. This disabled the attackers' server for several hours.[280] It remains unclear whether this constitute a blockade by disabling all communications, from whatever source, to the hackers' server or nothing more than returning unwanted packets of information.

[279] GREEN, *supra* note 275, at 204.
[280] Vikas Jayaswal, et al., Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?, in PROCEEDINGS OF THE IEEE INTERNATIONAL SYMPOSIUM ON TECHNOLOGY AND SOCIETY, 380 (IEEE Society, 2002).

The last level of force, and the most aggressive, is active defense measures. Experts have defined active defenses differently.[281] This paper defines active defense measures as the employment of an electronic force as a countermeasure directed at the source of a cyberattack immediately terminating the attack or preventing it from attacking again.[282] Active defenses are reserved for occasions where the use of force is permitted under the Law of War.[283] Therefore, a victim may engage in an active defense measure only if there is an imminent armed attack or if it currently is being attacked.[284] Due to the aggressiveness in this third level of response, the cyberteer would be subject to similar requirements that are imposed for "super-warrants" under the Wiretap Act.[285] Authorization to use active defense measures would require certification from the agency head, a description of what other efforts were made or why such efforts would be futile, and require the cyberteer to show the target was knowingly involved in the cyberattack or exploitation by clear and convincing evidence.[286]

Setting aside for the moment whether the use of force was authorize, the Stuxnet worm used to infect the Iranian nuclear reactor provides a good example of an active defense. Stuxnet was a malicious code that infiltrated the computer systems at Iranian

---

[281] W. Earl Boebert, *A Survey of Challenges in Attribution*, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 49 (Nat'l Res. Council, 2010) (active defenses include preemptive covert operations); Eric T. Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 Tex. L. Rev. 1533, 1566 (2010) (defining trace-backs as an active defense measure); Kesan & Hayes, *supra* note 265, at 328 (qualifying active defenses as a "cyber counterstrike").

[282] Jensen, *supra* note 157, at 230; Graham, *supra* note 159, at 92.

[283] Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 Mil. L. Rev. 1, 21-22 (2009).

[284] *Id*. at 50.

[285] *See generally* Wiretap Act, 18 U.S.C. § 2511 (2000).

[286] Michael Schmitt, *Responding to Transnational Terrorism Under the* Jus Ad Bellum*: A Normative Framework*, 56 Naval L. Rev. 1, 40 (2008) (advocating a clear and convincing standard as a compromise between the criminal standard of beyond a reasonable doubt and the probable cause standard of more likely than not).

nuclear facilities and prevented the reactors from operating properly. By all indications, Stuxnet did not damage the reactor but merely degraded its ability to enrich uranium.[287] The code was written to execute only when a specific configuration of controllers made exclusively by Siemens were linked together. Presumably, this was to ensure that if the worm spread beyond a specific Iranian nuclear reactor, it would not affect other reactors thereby meeting the distinction and proportionality requirements under the Law of War.[288] Similar active defense measures, when authorized, could provide a powerful tool for the private sector to diminish the possibilities of additional attacks by the same perpetrator. Some argue against the use of active defense measures claiming ultimately, active defenses may cause more harm than good. For instance, use of active defenses may cause the perpetrator to retaliate with additional attacks or the attackers may feign an attack to determine what responses or active defense measures an entity may deploy when the attacker initiates the actual attack.[289]

3. Satisfying Societal Standards

Paul Rosenzweig identified three societal standards that any cybersecurity plan should satisfy. They include economic prosperity, protection of privacy and civil liberties, and limited government involvement.[290] Due to the vast amounts of business conducted over the Internet, any proposal must further an economic well-being of those entities.[291] The proposal must create an environment that encourages businesses subjected to cyberattacks or exploitation to report the incident. A 2006 study reported

---

[287] *See* Broad et al., *supra* note 151, at A0.
[288] *Id*.
[289] LIBICKI, *supra* note 144, at 61.
[290] Paul Rosenzweig & Jena Baker McNeill, *CyberSecurity Enhancement Act of 2009 - A Start, But Not Enough*, HERITAGE FOUNDATION (Feb. 23, 2010), http://www.heritage.org/Research/Reports/2010/02/The-Cybersecurity-Enhancement-Act-of-2009-A-Start-But-Not-Nearly-Enough.
[291] *Id*.

that only 25 percent of computer security attacks were reported to law enforcement. That represented an amount statistically lower than other major criminal offenses.[292] Banks generally do not want to reveal the extent of annual fraud losses for fear of scaring customers away from online banking. Businesses generally don't report incidents of cyber-exploitation as they view the benefit of reporting is outweighed by the costs of trade secret exploitation, negative impact on their stock prices, and ability to maintain or attract new business. The notable exception was Google's announcement in January 2010.[293] A confidential reporting system is critical to the success of cyberteering and to the economic well-being of the private sector. This would promote greater reporting among businesses. Some may argue that transparency is necessary in order to protect the shareholders from substandard security measures. But a transparency requirement would only further curtail a willingness to report incidents of cyber-exploitation.

Privacy is of an equal concern to businesses and a paramount concern to citizens. Building confidence and allaying fears with private entities requires adequate regulations to protect the privacy of any information provided to the cyberteer and ensure it will not be used in any manner inconsistent with performing cybersecurity functions. The regulations require sufficient penalties when a cyberteer or its organization wrongly divulges the information.[294] This is particularly critical if a cyberteer conducts investigations for competing businesses. The agency should also impose basic disclosure requirements to ensure the cyberteer informs businesses that are in competition with each

[292] Ruperto P. Majuca & Jay P. Kesan, *Hacking Back: Optimal Use of Self-Defense in Cyberspace*, 2 (Ill. Pub. Law & Legal Theory Papers Series, Research Paper No. 08-20, 2009), available at http://papers.ssrn.com/abstract=1363932 (noting reported crime rates during a similar period of time for robbery was 60.5 percent, burglary was 54.1 percent, simple assault was 42.1 percent, and sexual assault which generally tends to be under-reported was 38.5 percent).
[293] Moore, *supra* note 140, at 8. *See* Guynn, *supra* note 22, at A1.
[294] Rosenzweig, *supra* note 66, at 5.

other of the possible conflict of interest. Cyber courts must also be sensitive to evidence that would discuss proprietary information or trade secrets. In such instances, the cyber courts must take adequate measures to prevent further disclosure. Additionally, any authorized use of force involving access to a computer located in the United States raises Fourth Amendment concerns regarding unreasonable searches.[295]

Finally, the Constitution requires the government to "provide for the common defense."[296] However, as Part I identified, the federal government does not have the funding, resources, or ability to provide adequate protection of the private sector. Moreover, bureaucracies generally lack the ability to respond quickly to incidents. In cyberattacks, response time is critical. While it may be impossible to stop an attack where a system is compromised in mere minutes, 60 percent of all attacks investigated by Verizon in 2009 took days or months from the point of entry until the system was compromised.[297] While this is encouraging, the government generally does not act this quickly. Although the Constitution places the responsibility upon the federal government, it is not the best entity to ensure protection. While that places the focus on the private sector, it does not mean the government may abdicate its role in "providing for the common defense."[298] As Stewart Baker, former Assistant Secretary of DHS noted, the private sector is ill prepared to defend against a cyberattack alone and the government must be actively involved.[299] The government's role should be providing a legal framework for, and oversight of, private security entities.[300] Likewise, private

---

[295] *See infra* Part III.B. for detailed discussion regarding these concerns.
[296] U.S. CONST. PMBL.
[297] Verizon 2010 Study. Pg 46-47
[298] *See* Rosenzweig, *supra* note 66, at 5.
[299] Ellen Nakashima, *War Game Reveals U.S. Lacks Cyber-Crisis Skills; Staged Emergency Displays Need for Strategy, Organizers Say*, Wash. Post, Feb. 17, 2010, at A03.
[300] Rosenzweig & McNeill, *supra* note 290.

security entities must respond to this challenge and protect the private sector from cyberattacks and exploitations.[301]

C. Regulating and the Effects of the Cyberteering Program

The legislation should authorize a joint public-private agency that monitors and regulates the cyberteering program and reports its findings to DHS.[302] The primary purpose of the agency would be to monitor and regulate the cyberteering entities. It would have the responsibility for imposing licensing and bonding requirements, implementing regulations and codes of conduct, investigating any alleged wrongdoing by cyberteers, and maintaining a registry of authorized cyberteers. Finally, it would serve as a central collection point and maintain a database of malicious code for research. For the agency to be effective, however, it must maintain its own autonomy and not become part of the larger DHS bureaucracy. The government response time will be critical to the success of the program. Due to the speed at which cyberattacks occur, the agency will need to be flexible and quickly respond to proposals to avoid destruction of evidence and ensure a timely response to attacks.

Licensing requirements would help legitimize a program that some may view as promoting cyber mercenaries.[303] Among the many licensing requirements, a minimal level of experience and education would be required for anyone conducting computer forensic investigations or performing the various authorized responses. This should help avoid similar situations that have occurred with private contractors serving in military

[301] *Id*. *Cf*. Knake, *supra* note 136, at 2 (It is not, however, a central part of U.S. strategy to prevent terrorist attacks and its importance in preventing conventional military attacks is more limited than in the nuclear case.).
[302] *See* Rosenzweig, *supra* note 58, at 266-67 (Paul Rosenzweig outlines a public-private partnership called the "Cybersecurity Assurance Corporation" designed to foster information sharing between victims of attacks and the government to better protect businesses).
[303] *See* Mark W. Bina, *Private Military Contractor Liability and Accountability After Abu Ghraib*, 38 J. Marshall L. Rev. 1237, 1245 (2005).

operations in Iraq and Afghanistan. In one shocking instance, many translators employed by a private military contractor (PMC) tasked with translating for Operation IRAQI FREEDOM were "artists, grocery baggers, recent college graduates, and others with no background in translating."[304] While education is important in becoming competent in cybersecurity, requiring a minimum amount of experience in computer forensics or other related fields will help ensure cyberteers also have practical experience. Finally, annual certification and continuing education courses should be mandated. This will ensure that those authorized to conduct cyberteering operations remain current with technological trends and advancements.

Imposing a bond requirement will serve several ends as well. It should operate to curb abuses of power by ensuring cyberteers have a vested interest in their actions. Privateers received compensation by acquiring lawful title to a portion of the goods seized from captured vessels.[305] This fostered an abuse of the system. Bond requirements helped curb some of the abuses of privateering and ensured privateers followed the requirements in the letters of marque.[306] Imposing a sufficiently high bonding requirement should price smaller firms and individual hackers out of the market leaving large, well-established organizations to conduct cyberteering operations. Comparing the bond requirements from the Quasi-War to the Waledac litigation shows a disparity between what was requires with privateers and what one court required of Microsoft. During the Quasi-War, the minimum bond amount was equivalent to $130,000 in 2011 dollars. Microsoft, on the other hand, was ordered to maintain a bond of only $54,600 during the period of injunctive relief in the event a defendant would

[304] *Id.*
[305] 2 BOUVIER'S LAW DICTIONARY 2723 (8th ed. 1914).
[306] WOOLSEY, *supra* note 186, at 207-08.

come forward claiming damages.[307] The bonding requirement must strike a balance between imposing too low of a bond thereby attracting non-reputable entities and setting the requirement too high and pricing competent firms out of the market.

Most importantly, this new private sector cybersecurity policy most strike the proper balance between flexibility in responding to incidents and the necessary regulations and oversight to minimize abuses of the system. More specifically, those charged with implementing this cybersecurity policy must contend with the negative stigma PMCs have recently received regarding lack of sufficient oversight and address concerns of handing a perceived "state function" to the private sector.[308] By creating a new agency, it will have the opportunity to draft regulations with these abuses in mind to help ensure they do not scale to cyberspace. In doing so, the regulations must address both private sector companies seeking assistance and the cyberteers. Victimized entities seeking redress would be required to report the incident to the agency and have an assessment of the cyberattack or exploitation conducted before being able to avail itself of the use of force procedures. The regulations would require the assessment to be conducted by independent and properly licensed cyberteering organizations. The private company would be able to select which cyberteering organization it would hire from a registry the agency maintains. Forcing the private companies to use licensed cyberteers would minimize the possibility of corporations falsifying their own assessment or planting malicious code on their own systems then wrongly accusing a competitor or other agency of conducting a cyberattack or exploitation. Regulations directed to the

[307] Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 6, Microsoft v. John Does 1-27, (E.D. Va., 2010) No 1:10CV156.
[308] Oliver Jones, *Implausible Deniability: State Responsibility for the Actions of Private Military Firms*, 24 Conn. J. Int'l L. 239, 249 (2009).

private sector companies would also set rules as to what the privateers may and may not have access to in conducting their investigation.

ROEs will be the central piece to establish a baseline of conduct for cyberteers. The ROEs should outline the evidentiary requirements for the various tasks the cyberteer could perform, establish a clear standard of conduct, and identify penalties for abuse. Once the cyberteer was selected by the entity that was exploited, it would conduct an investigation similar in nature to the GhostNet investigation addressed in the Introduction. Then it would issue a report and proposal outlining a response plan. The agency would have a set time to review and act on the proposal by authorizing, denying, or modifying the proposal. As new evidence is discovered, warranting an increased use of force, the cyberteer would repeat the process. Cyberteers would be required to make regular reports to the agency and be subjected to random audits. This would ensure that cyberteers act not only in their clients' best interest, but also in the best interest of the United States. This allows the government to intervene with diplomatic or other options in situations where the incident may become sensitive to U.S. foreign relations.[309] Violation of the established ROEs could range from reprimands, to sanctions on the individual or organization, to civil or criminal action. It is this form of accountability that was conspicuously lacking with PMCs operating in the middle east.

This public-private partnership offers many synergistic effects. A central feature of the agency would be a malicious code database. To develop the database, the cyberteers would be required to provide any discovered malicious code to the agency.

[309] While this may appear to be unfair to the victim of the cyberattack or cyber-exploitation, a similar process exists with the "restrictive form" of sovereign immunity under the Tate Letter of 1952 where the United States government could grant immunity of an act committed by a foreign sovereign. This policy was later abandoned and replaced with the Foreign Sovereign Immunities Act of 1976, 28 U.S.C. §§ 1330, 1602-11 (2000).

This database would be accessible to other government agencies and departments as well as other registered cyberteers. By sharing the "captured" code, the government and cyberteers could analyze and better respond to attacks exhibiting similar characteristics as many cyberattackers tend to reuse large portions of malicious code for subsequent attacks.[310] This in turn makes the private sector more resilient and the response time diminishes as well. Knowledge of how malicious codes operate could also lead to effective blockade or sanction methods to prevent transmission from the block of IP addresses where the attack originated. Through such a system, a perpetrator may be able to launch one successful attack, but subsequent attacks could be thwarted.

Critics may argue that the program will siphon talent from the government for more lucrative cyberteering positions. This competition between the public and private sector was a concern regarding privateering and has proven to be a major concern for the military today as Special Forces are separating from the service to join more lucrative PMCs.[311] While cybersecurity analysts within government agency may move to the private sector under this policy, the government will nevertheless benefit from the policy and will be minimally impacted. The public-private partnership under this proposal allows the government to leverage the knowledge and skills of the private sector experts investigating and neutralizing cyberattacks without the need to compete against the private sector to lure them into government cybersecurity positions.

At the same time the government leverages private sector talent, the private sector could benefit from the resources and political influence of the government. Microsoft

---

[310] *See* Kelly Jackson Higgins, *Storm Worm Reappears*, DARKREADING (Apr. 28, 2010) http://www.darkreading.com/story/showArticle.jhtml?articleID=224700110.

[311] *See supra* note 204 and accompanying text; Michael N. Schmitt, *War, International Law, and Sovereignty: Reevaluating the Rules of the Game in a New Century: Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 Chi. J. Int'l L. 511, 515 (2005).

was able to terminate the top-level domains used by the Waledac botnet because the courts had jurisdiction over VeriSign as a corporation based in Virginia and the registrar of the .com and .net domains. In situations where the United States court system lacks jurisdiction over an entity, the private sector could turn to the government for assistance. The government could implement an IP address blacklist program requiring ISPs to prevent communication to and from designated IP blocks known for launching attacks.[312] Similarly, the United States could impose economic sanctions upon states permitting attacks without taking measures to prevent the launching of the attacks.[313] There are, however, substantial concerns regarding each of these measures. Any IP blacklist would likely be over-inclusive thereby blocking innocent Internet users.[314] At the same time, such an effort would likely be under-inclusive as well and not adequately block the threat. As noted above, government intervention could come at the expense of the victim of the attack.[315] Should politics or foreign relations trump cybersecurity of the private sector, the proposal may lack the enforcement authority necessary to deter attacks and victimized companies may be without a remedy.

Ultimately, this proposal is a reactionary program designed to deter attacks. If perpetrators believe subsequent attacks will be blocked, degraded, or revoked, thereby making it costlier to launch an attack, some will exit the market. This was a goal of privateering and should be the goal of cyberteering—making it too costly for the perpetrator. Referring to privateers, Thomas Jefferson said, "Let nothing be spared to

---

[312] Knake, *supra* note 161, at 19-20.
[313] *Id*. at 19. *See generally* Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague Convention (V)].
[314] *See generally* Ctr for Democracy & Tech. v. Pappert, 337 F.Supp. 2d 606 (E.D. Pa. 2004).
[315] *See supra* note 309.

encourage them. They are the dagger which strikes at the heart of the enemy, their commerce."[316] Recently, one security researcher noted, "A shutdown hits criminals where it hurts the most – in the wallet."[317] These quotes demonstrate that a deterrence policy based upon disrupting a revenue stream will in fact scale to cyberspace.

## III. Legality of Cyberteering Legislation

The legality of the proposal must be examined on both the international and domestic levels. Although international law generally applies to state actors, actions committed against a state's nationals may trigger self-defense protections under Article 51 of the U.N. Charter in certain instances. In examining the application of international law with respect to cyberteering, this article focuses on state responsibility as identified in the International Law Commission (ILC) Draft Articles on State Attribution (Draft Articles), the Charter, and the Hague Convention (V). After concluding international law generally would not apply, this article addresses the legality of an authorization to use force, due process concerns, and finally a brief examination of the Law of War as guiding principles for conducting cyberteering.

### A. Application of International Law

#### 1. International Law Commission Draft Articles on State Attribution

While the ILC Draft Articles represent a codification of customary international law, they are not binding upon states.[318] However, they do offer persuasive evidence as to the current state of international law on the topic of state responsibility. Therefore, the

---

[316] Letter from Thomas Jefferson to James Monroe (Jan. 1, 1815), in 9 THE WRITINGS OF THOMAS JEFFERSON, at 498 (Paul Leicester Ford ed. 1898).
[317] Tim Wilson, *Malware-Serving ISP Taken Down, Researchers Say*, DARKREADING (Mar. 11, 2010, 4:48 PM) http://www.darkreading.com/taxonomy/index/printarticle/id/223600018 (comment by Mary Landesman of ScanSafe).
[318] Jones, *supra* note 308, at 261.

Articles reflect general principles as opposed to binding rules.[319] Article 4, which addresses organs of a state, is viewed as the "first principle of attribution" for state responsibility.[320] It holds that the conduct of a state organ will be deemed conduct of the state.[321] But actions of organizations that maintain a separate legal personality, even if owned or controlled entirely by the state, will not be deemed an act of the state.[322] Consequently, under Article 4, cyberteers, although carrying out authorized uses of force by the government, would not constitute an organ of the state.

Article 5 addresses instances where a particular entity is not an organ of the state but exercises certain functions of governmental authority. In such instances, the action when conducted by the entity will be deemed an act of the state.[323] The commentaries to Article 5 specifically note that in certain instances private companies exercise state responsibility if the act is something typically carried out by state organs, such as police powers.[324] However, the non-state entity must not only carrying out the governmental function, but "must also be 'empowered by the law' of the state to do so."[325] Cyberteers seeking warrants and subsequently executing the searches clearly qualify as conducting a government function. More importantly, the proposal would empower them by law to do so. This would likely qualify cyberteers as exercising state responsibility as would carrying out any of the three uses of force outlined above. When the analysis is applied to subpoenas, a different outcome is reached. Subpoenas, while a function of the

---

[319] *Id*.
[320] Responsibility of States for Internationally Wrongful Acts (Proposed Draft with Commentaries), [2001] 2 Y.B. Int'l L. Comm'n 40, U.N. Doc. A/56/10 [hereinafter Draft Articles], available at http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
[321] *Id*. at art. 4.
[322] Jones, *supra* note 308, at 263.
[323] Draft Articles, *supra* note 320, at art. 5.
[324] *Id*. at 43
[325] Jones, *supra* note 308, at 268.

government, are carried out by private lawyers representing private litigants, and therefore would not qualify as an act of the state. The primary difference is the inherent law enforcement nature of warrants that is lacking in subpoenas. The recipient of the subpoena may refuse to comply with the subpoena, risking a potential court order to compel. But the individual served with a warrant has no right to decline the search. However, without the power of the warrant or the explicit state authority to use the various levels of use of force, the cyberteering proposal would be futile. This may prove to be the greatest hurdle in implementing a cyberteering program.

2. United Nations Charter

Prior to World War II the decision to declare war against another belligerent rested with the sovereign.[326] Today, the U.N. Charter is the primary source for addressing conflicts of an international nature. Since only states are members of the Charter, only states may invoke the right to self-defense.[327] The Charter, however, does not limit the use of self-defense to instances where government property and agencies were targets.[328] A state may invoke the right to self-defense on behalf of their nationals when the effects on the nationals are substantial.[329] It is under this lens of self-defense that we examine the applicability of the Charter to cyberteering. However, as developed below, given most incidents would involve cyber-exploitation, it is unlikely the Charter's provisions would be triggered.

---

[326] Sklerov, *supra* note 283, at 27.
[327] Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, in PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 163 (Nat'l Res. Council, 2010).
[328] *Id*. *See generally* Sean D. Murphy, *Terrorism and the Concept of "Armed Attack" in Article 51 of the U.N. Charter*, 43 Harv. Int'l L.J. 41 (2002) (describing the September 11, 2001 terrorist attacks as an armed attack and the United States invoking rights under Article 51).
[329] Schmitt, *supra* note 327, at 163.

Responding to hostile acts under the Charter requires a state to examine whether such actions rise to the level of armed conflict. This invokes the *jus ad bellum* paradigm.[330] Article 2(4) of the Charter prohibits member nations from engaging in a "threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[331] When a member state violates Article 2(4), the self-defense provision under Article 51, permits the victim state to respond, but only in instances of an "armed attack." The paradigm is the gap between Article 2(4)'s general prohibition on the use of force and the amount of illegal force required by an aggressor before the victim may engage in self-defense pursuant to Article 51.[332] In other words, under the Charter an aggressor may engage in an illegal use of force short of an armed attack but the victim state may not avail itself of self-defense measures under Article 51. Only when the aggressor crosses the line into an armed attack, the victim may engage in self-defense.[333]

To complicate the analysis, the Charter does not define "armed attack" and "use of force."[334] Michael Schmitt defines an "armed attack" as "an intentional military attack or other intentional act resulting in, or designed to result in, immediate violent consequences."[335] These consequences generally result in physical damage and may

---

[330] The Charter embodies the two major categories of the law of armed conflict, *jus ad bellum* and *jus in bello*. *Jus ad bellum* addresses conflict management—the laws of how states initiate armed conflict and the circumstances when the use of military power legally and morally justified. *Jus in bello* is concerned with the law as it applies once conflict is initiated. THE JUDGE ADVOCATE GENERAL'S SCH, U.S. ARMY, LAW OF WAR HANDBOOK 5 (2005) [hereinafter LAW OF WAR HANDBOOK].
[331] U.N. Charter art. 2, para. 4.
[332] Sean Condron, *Getting It Right: Protecting American Critical Infrastructure in Cyberspace*, 20 Harv. J. Law & Tec 404, 412 (2007).
[333] Dinstein, *supra* note 153, at 100.
[334] *See generally* U.N. Charter. Additionally, "threat" is not defined by the Charter as well, however, currently, cyberattacks and exploitations have not focused on threatening action against private sector entities.
[335] Schmitt, *supra* note 286, 14 n.60.

apply to computer network attacks.[336] In *Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua v. United States*), the ICJ held that not all uses of force constituted an "armed attack."[337] To qualify as an armed attack, the act must have sufficient "scale and effects" that it would otherwise constitute an armed attack if the same act was committed by regular forces.[338] This led many scholars to employ an effects-based model when determining whether a particular use of force constitutes an armed attack.[339] While no consensus exists for what constitutes a "use of force," the ICJ held in *Nicaragua v. United States* that the term use of force is of less severity than an armed attack.[340] Actions not rising to the level of a "threat or use of force," regardless of their effects, include "unfavorable trade decisions, space-based surveillance, boycotts, severance of diplomatic relations, denial of communications, espionage, economic competition or sanctions, and economic and political coercion…"[341]

The Charter provides two exceptions to the prohibition against the use of force. The first exception can be found in Articles 39, 41 and 42. Under Article 39, the Security Council may permit a member state to use force when responding to "any threat to the peace, breach of the peace, or act of aggression" in order "to maintain or restore international peace and security."[342] This is; however, contingent upon Articles 41 and 42. The Security Council must first determine if a response short of the use of armed

---

[336] *Id*.
[337] Michael Schmitt, *Preemptive Strategies in International Law*, 24 Mich. J. Int'l L. 513, 539 (2003). *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 195 (Jun. 27) [hereinafter *Paramilitary Activities*].
[338] *Paramilitary Activities*, *supra* note 337, ¶ 195.
[339] IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362-63 (1963); THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT, NATIONAL SECURITY LAW IN CYBERSPACE 117-130 (2000); Graham, *supra* note 159, at 91.
[340] *Paramilitary Activities*, *supra* note 337, ¶ 247. *See also* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161 ¶ 51 (Nov. 6).
[341] Cyberattack Capabilities, *supra* note 130, at 242. The U.N. Charter and Resolution 3314 do not define "attack."
[342] U.N. Charter art. 39.

force could result in a peaceful resolution of the matter.[343] If a resolution is not reached by peaceful means, the Council may authorize measures amounting to the use of force.[344] The second exception is Article 51, which holds: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense 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."[345] Article 51 codifies the inherent right for a state to defend itself when attacked pursuant to customary international law.[346]

Article 51 is based upon three criteria: necessity, proportionality, and timeliness.[347] Necessity and proportionality were recognized as criteria for Article 51 in *Nicaragua v. United States* and was affirmed in the *Nuclear Weapons Advisory Opinion*.[348] Necessity examines whether a peaceful resolution may be attained without the use of force.[349] If non-forceful responses are either futile to implement or have already been exhausted then the use of force meets the necessity requirement.[350] Proportionality requires the amount of force used to be limited in scope, intensity, and

[343] *Id*. at art.41.
[344] *Id*. at art.42.
[345] *Id*. at art.51.
[346] *See* INTERNATIONAL LAW: CASES AND MATERIALS 59 (Lori F. Damrosch et al. eds., 5th ed. 2009).
[347] LAW OF WAR HANDBOOK, *supra* note 330, at 44; THE JUDGE ADVOCATE GENERAL'S LGL. CTR. & SCH, U.S. ARMY, OPERATIONAL LAW HANDBOOK 4 (2008) [hereinafter OP LAW HANDBOOK].
[348] *Paramilitary Activities*, *supra* note 337, ¶ 194; Legality of the Threat or Use of Nuclear Weapons, 1996 I.C.J. 4, 245, ¶¶ 41 & 42 (Jul. 8).
[349] OP LAW HANDBOOK, *supra* note 347, at 4; Dinstein, *supra* note 153, at 109.
[350] OP LAW HANDBOOK, *supra* note 347, at 4; Dinstein, *supra* note 153, at 109. The definition of necessity under self-defense is slightly different than under the Law of War. Necessity under the Law of War could be thought of as proactive; what is necessary to accomplish the military mission. Whereas necessity under Article 51 could be thought of as reactive; only after peaceful means were already attempted or would otherwise be futile may force be used to obtain a peaceful resolution.

duration for what is necessary to counter the hostile act.[351] This represents symmetry between the use of force and the use of counter-force.[352] Further, proportionality permits a state subjected to a series of smaller attacks to respond with a single larger attack in an attempt to prevent further escalation of hostilities.[353] Finally, timeliness refers to the time between the hostile act and victim state's response.[354] In such situations where attribution is unambiguous, a delayed response will weaken the ability for a state to claim self-defense.[355] In other situations where attribution is harder to establish, timeliness should be viewed broadly.[356] This is a fluid concept based upon the facts, circumstances, and abilities of the victim state at the time. In some cases, a delay of minutes or hours is acceptable. In other situations, a delay of weeks or months may be appropriate to ensure the necessity, proportionality, and attribution are met.[357] Some argue timeliness is less critical than the ability for the victim state to deter the attacker from attempting subsequent attacks.[358]

As noted above, for a state to invoke Article 51 on behalf of its nationals, the acts by the aggressor must constitute an "armed attack" and have substantial effects on its

---

[351] OP LAW HANDBOOK, *supra* note 347, at 4. Although the definitions of proportionality under both Law of War and self-defense are similar in nature, under a Law of War analysis the focus is on whether the act will cause excessive incidental injury or collateral damage. Under self-defense, the focus is directly upon responding to the hostile act.
[352] Dinstein, *supra* note 153, at 109.
[353] 2 Y.B. Int'l L. Comm'n, State Responsibility, pt. 1, at 69-70 (1980), available at http://untreaty.un.org/ilc/publications/yearbooks/Ybkvolumes(e)/ILC_1980_v2_p1_e.pdf. Additionally, "frontier incidents" do not rise to the level of a use of force. Frontier incidents are isolated and limited hostile engagements between forces across a border and generally lack a conscious strategic decision to initiate an international armed conflict. That does not mean a victim is without recourse. A victim possesses the right of self-defense and defense of property under domestic laws and law enforcement may use force in order to combat criminal activity. See *Paramilitary Activities*, *supra* note 337, ¶ 195; Schmitt, *supra* note 286, at 14 n. 60 & 540.
[354] LAW OF WAR HANDBOOK, *supra* note 330, at 44; OP LAW HANDBOOK, *supra* note 347, at 4.
[355] Todd, *supra* note 111, at 98.
[356] Dinstein, *supra* note 153, at 110; Schmitt, *supra* note 286, at 534.
[357] Dinstein, *supra* note 153, at 110.
[358] LIBICKI, *supra* note 144, at 88.

nationals. Michael Schmitt's definition of armed attack, requiring immediate violent consequence, would exclude most cyber-exploitations as they tend to involve the syphoning of data over an extended period of time. This conclusion is consistent with the Law of War, which has permitted the use of espionage since the issuance of the Lieber Code during the Civil War.[359] The Hague Convention (IV) later adopted these principles under Articles 24 and 29.[360] Based upon these principles, the three instances of cyber-exploitation noted in the Introduction do not violate international law and the victim state cannot use Article 51 self-defense remedies on behalf of its nationals.[361] For this reason, states attempt to deter spying by prosecuting such acts through domestic criminal laws.[362]

2. Other International Laws

In addition to the Charter and the Convention on Cybercrimes, many legal experts have turned to the Hague Convention (V) to ensure neutral states prevent cyberattacks from being launched in its territory. The Hague Convention (V) prohibits belligerents from moving "troops or convoys of either munitions of war or supplies across the territory of a neutral Power."[363] This places an affirmative obligation on neutral states to prevent belligerents from engaging in those actions.[364] But a neutral state need not forbid or restrict the transmission of signals over telegraph or telephone lines or over wireless

---

[359] INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD art. 88 (Francis Lieber ed., Washington, Government Printing Office 1898) (1863), available at http://www.loc.gov/rr/frd/Military_Law/ pdf/Instructions-gov-armies.pdf (Article 88 states a spy is "a person who secretly, in disguise or under false pretense, seeks information with the intention of communicating it to the enemy.").

[360] Article 29 states: "A person can only be considered a spy when, acting clandestinely or on false pretences, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party." Hague Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, art. 29, 36 Stat. 2277, 1 Bevans 631.

[361] Todd, *supra* note 111, at 94.

[362] W. Hays Parks, *The International Law of Intelligence Collection*, in NATIONAL SECURITY LAW 433-34 (John Norton Moore, et al. eds., 1990).

[363] Hague Convention (V), *supra* note 313, art. 2.

[364] *Id*. at art. 5.

signals owned by the state or by a private entity provided that such decision applies equally to all belligerents.[365] The logical implication of Articles 5 and 8 would make it a violation of the Hague Convention (V) to permit an attacker to use the electronic communications of a neutral state as a waypoint or to stage a cyberattack on another nation. If such attacks nevertheless occur, the neutral nation must, in order to maintain its neutral status, resist such acts by force if necessary.[366] Therefore, it reasonably implies the state has a duty to prevent private communication providers from permitting attacks to be launched or used as a waypoint from their systems.

B. Application of Domestic Law

While most private sector cyberattacks and exploitations will not rise to the level of an armed attack or substantially affect a state's nationals pursuant to international law, domestic law can provide recourse.[367] The three proposed countermeasures, trace-backs, blockades or sanctions, and "active defenses," will likely intrude to varying degrees upon the territory of another state. Congress, however, by limiting the authorized levels of force permitted could ensure that any measure authorized falls short of an armed attack. While the acts may violate the territorial integrity of another nation, these actions would likely fall short of an armed attack under Article 51. The actions authorized would be similar in nature to the U-2 spy plane flights over the Soviet Union in 1960. The Soviet government claimed the flights constituted an act of aggression.[368] The United Nations

[365] *Id*. at arts. 8 & 9.
[366] *Id*. at art. 10.
[367] Schmitt, *supra* note 327, at 163.
[368] WINGFIELD, *supra* note 339, at352.

Security Council held that while the flight was a violation of Soviet airspace and was an unlawful intrusion, it was not a use of force *per se*.[369]

1. Authorizing the Use of Force

Identifying the perpetrator of a cyber-exploitation is a complicated task. But the inability to formally identify the perpetrators does not prevent Congress from passing a legislation authorizing use of force to combat private sector cyberattacks and exploitations.[370] Congress need not specifically identify a belligerent nation before declaring war as was evident with the 9/11 Authorization for Use of Military Force (AUMF). The 9/11 AUMF authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons" determined by the president to have "planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons."[371] The wording used in the 9/11 AUMF is significant in that its application is not restricted by geographic boundaries. In other words, the battlefield is defined by wherever the perpetrators are found. This becomes particularly useful in cyberspace where traditional notions of boundaries do not apply. This approach is also consistent with letters of marque which were free from jurisdictional restraints.

2. Due Process Rights

Cyber courts raise several due process concerns including, notice requirements and public hearing requirements. Under marques and reprisals providing notice was a simple task. An officer of the captured vessel was given notice of the prize court hearing once the vessels reached port. This concept does not scale to cyberspace. That said, the

[369] *Id.* at 353.
[370] *See* Robert Kagan, Editorial, *We Must Fight This War, Editorial*, Wash. Post, Sep. 12, 2001, at A31.
[371] Sense of Congress Regarding Terrorist Attacks, Pub. L. No. 107-40; 115 Stat. 224 (2001).

Waledac botnet litigation does provide guidance. In granting the injunctive relief sought by Microsoft, the court ordered Microsoft to provide notice through several different mediums. First, for those with contact information within the United States, personal delivery was required. Second, personal delivery for those outside the United States was required to conform to the Hague Convention on Service Abroad. Third, service was required to any e-mail, physical mail, or facsimile information maintained by the top-level domain name registrar. Finally, the court required notice to be published on a publicly available website.[372]

Prize courts were public hearings. However, under a cyber court setting, there may be compelling reasons to close the hearings or to seal any records for a period of time. As noted above in Part I, a major concern of corporations regarding the EEA was that private parties were unable to obtain protective measures to prevent public dissemination of proprietary information disclosed during the court. Microsoft wanted the records sealed temporarily to prevent advance warning to the botnet operators who could then take action to redirect its communication with the zombie computers. While a democratic society depends on an open court system, there are instances where hearings are closed. Two examples include military courts-martial involving classified information and hearings before the United States Foreign Intelligence Surveillance Court.[373] While the cyber court should be an open procedure, the possibility of closing the court or sealing the records should be considered under limited circumstances.

[372] Order Granting Preliminary Injunction, at 6 Microsoft v. John Does 1-27, (E.D. Va., 2010) No. 1:10CV156.
[373] *See* MANUAL FOR COURTS-MARTIAL, UNITED STATES, M.R.E. 505 (2008); Foreign Intelligence Surveillance Act, 50 U.S.C. § 1803 (2000).

Suffice it to say, should a cyberteering policy be adopted, the matter will undoubtedly be highly debated.

It is important to keep in mind the cyber court's purpose is to act as a check on the cyberteers' actions and provide a forum for redress. Cyber courts would operate similar to prize courts. Privateers seeking to obtain lawful title to goods and vessels captured had to show the items fell within the description listed in the letter.[374] During the hearing, a representative for the captor could present evidence. The burden of proof rested upon the claimant, who was the representative for the captured vessel or goods.[375] The hearings generally were not an adversarial process between the parties. Rather they were simply a legal process to determine who would receive legal title to the property at issue.[376]

Generally, these matters were relatively easy to determine based upon the physical documentation found on the captured vessels.[377] The hearing sought to distinguish between "a legal and justifiable seizure and an illegal and unjustifiable condemnation."[378] Likewise, the cyber courts would provide a forum for those targeted by a cyberteer. The respondent could issue claims against the cyberteer, such as the cyberteer acted beyond his legal scope or that the use of force was unjustified. If successful, the respondent could then seek monetary redress. However, to limit potential liability to the cyberteer, monetary redress should be limited to instances of clear abuse of discretion. This was the standard generally applied in prize courts. Claimants commonly sought damages claiming insufficient evidence for condemnation of the vessel or

[374] Miller v. Resolution, 2 U.S. (2 Dall.) 19, 22 (1781).
[375] AMOS S. HERSHEY, THE ESSENTIALS OF INTERNATIONAL PUBLIC LAW AND ORGANIZATION 740 n. 22, (rev. ed. 1935).
[376] *Id.* at 524 n.22.
[377] *Id.*
[378] Hooper v. United States, 22 Ct. Cl. 408, 439 (1887).

goods.[379] But prize courts consistently held the privateer would not be liable for damages even if the evidence does not support condemnation assuming probable cause existed for the vessel's seizure.[380]

Domestic concern over privacy rights will undoubtedly be a paramount concern for individuals, businesses, and for the legality of the proposal. Investigators may successfully trace an attack to a computer, but that does not address who sat behind the computer at the time of the attack. This raises a high potential of civil liberty violations.[381] Searches within the United States trigger the Fourth Amendment and the Electronic Communications Privacy Act, which addresses stored communications and wiretaps.[382] Before seeking a warrant, a cyberteer should first determine if the computer owner would give consent. This is the simplest solution especially if the cyberteer believes the computer in question was used as an intermediary in the attack and the owner would consent to a search. If the owner refuses then the cyberteer could obtain a warrant.

While full analysis is beyond the scope of this article, a brief mention of the Stored Communications Act and the Wiretap Act is necessary. The Wiretap Act protects against the intentional interception of communications by a device over a wire.[383] This provision could be triggered if cyberteers were to clandestinely operate a webcam or microphone on a computer, similar to the attackers in the GhostNet investigation. The Wiretap Act requires a "super-warrant" before permitting the interception of the

[379] Murray v. Schooner Charming Betsy 6 U.S. (2 Cranch) 64, 117-18 (1804); *Hooper*, 22 Ct. Cl. at 439.
[380] *Hooper*, 22 Ct. Cl. at 439; The Thompson, 70 U.S. (3 Wall.) 155, 162 (1865).
[381] Condron, *supra* note 332, at 417.
[382] U.S. CONST. amend. IV; 18 U.S.C. § 2510; Stored Communications Act, 18 U.S.C. §§ 2701-12 (2000); United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990).
[383] 18 U.S.C. § 2511.

communications. The general requirements of super-warrant include: exhaustion of other means of obtaining the desired evidence, articulable facts supporting a belief that a crime has been or will be committed, probable cause that the wiretap will obtain the desired information, duration of time and place to conduct the surveillance, and certification by the Attorney General or prosecutor that all requirements are met.[384] The Stored Communications Act addresses retrieved and unretrieved communications such as e-mail in electronic storage.[385] The Stored Communications Act, depending upon the information sought to be disclosed, requires either a subpoena, court order, or a search warrant.[386] When searching a computer believed to contain contraband, a search warrant based upon probable cause is required.[387] This requires an affidavit establishing "a fair probability that contraband or evidence of a crime will be found in a particular place."[388] Bare suspicion alone is insufficient.[389] To provide cyberteers with the flexibility needed to investigate attacks and exploitations, the legislation must create the ability for cyberteers to present evidence to the cyber courts that could then authorize search warrants based upon probable cause for computers involved in cyberattacks located within the United States. Additionally, given the ease that one can destroy digital

[384] 18 U.S.C. § 2511.
[385] 18 U.S.C. §§ 2701-12.
[386] OFFICE OF LEGAL EDUC., DOJ, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 138 (2009) available at http://www.cybercrime.gov/ ssmanual/ssmanual2009.pdf.
[387] Id., at 63-64.
[388] Illinois v. Gates, 462 U.S. 213, 238 (1983).
[389] *See* Brinegar v. United States, 338 U.S. 160, 175 (1949). Cf. The George, 10 F. Cas. 201, 201 (C.C.D. Ma. 1815) (No. 5,328); The City of Mexico, 24 F. 33, 40 (S.D.N.Y. 1885) (Privateers were permitted to search other vessels based upon suspicion. Under international law belligerents could search any vessel on the high seas in order to determine the actual nature and conduct of the vessel. If the search involved a neutral vessel, the belligerent was required to perform the search in the least infringing manner possible. But if a belligerent found contraband upon a neutral vessel, the belligerent may confiscate the goods. Likewise, if a neutral vessel was under the command of a belligerent it too was liable for condemnation.)

evidence, the court must be capable of issuing "sneak-and-peek" warrants when justified by the situation, excusing the cyberteer from providing notice at the time of the search.[390]

When addressing search and seizures outside the United States, the Supreme Court previously held that the provisions of the Fourth Amendment were not "intended to restrain the actions of the Federal Government against aliens outside of the United States territory."[391] In *Verdugo*, the Court addressed whether the Fourth Amendment applied to the search and seizure of property of a non-resident alien in a foreign country by United States agents.[392] Holding that the Fourth Amendment did not apply, the majority discussed at length the legal significance of the congressional acts authorizing use of force during the Quasi-War.[393] A seizure was unlawful when a captain of a vessel exceeded the authorization under the congressional act.[394] But if a captain acted within the scope of the authorization and upon probable cause, the seizure of a neutral ship was lawful.[395] In both instances, the Fourth Amendment was never a determinative factor. Turning to the case before the Court, the majority held the Fourth Amendment did not restrain Congress' authority or prohibit United States agents to seize evidence from an alien's residence outside the United States without a warrant.[396] The Court concluded that if such restrictions were to be imposed on property of a non-resident alien outside the United States it must be imposed by the political branches of government.[397]

---

[390] United States v. Grubbs, 547 U.S. 90, 98-99 (2006).
[391] *Verdugo-Urquidez*, 494 U.S. at 266.
[392] *Id.* at 261.
[393] *Id.* at 267 (noting that during the Quasi-War 365 private armed vessels were commissioned by the United States government pursuant to Article I, section 8, clause 11 of the Constitution).
[394] *Id.* (citing Little v. Barreme, 6 U.S. (2 Cranch) 170, 177-178 (1804)).
[395] *Id.* (citing Talbot v. Seeman, 5 U.S. (1 Cranch) 1, 31 (1801)).
[396] United States v. Verdugo-Urquidez, 494 U.S. 259, 268 (1990).
[397] *Verdugo-Urquidez*, 494 U.S. at 275.

3. Law of War

While Law of War principles are not generally viewed as domestic law principles, they do offer guidance when evaluating the appropriate response to cyber-exploitations. By employing the principles of Law of War, the authorized uses of force can be tailored to avoid a response rising to the level of an armed attack. There are four main principles of the Law of War: necessity, proportionality, distinction (discrimination), and humanity (unnecessary suffering). Necessity permits the use of any actions, not banned by international law or the Law of War, necessary to bring a belligerent into submission when settlement by peaceful means is unattainable.[398] Proportionality requires belligerents to minimize incidental loss of civilian life, injury to civilians, and damage to civilian objects that "would be excessive in relation to the concrete and direct military advantage anticipated."[399] However, the military advantage sought from an attack is not limited to only tactical gains, but is viewed in context of the full war strategy.[400] Distinction requires attacks to be limited to combatants and those military objectives be distinguished from protected property or places.[401] Distinction generally prohibits the use of weapons that cannot distinguish between civilians and civilian objects on the one hand and military objectives and combatants on the other.[402] Belligerents are required to make a concerted effort to distinguish between the civilian and non-civilian categories when conducting military operations and prohibit indiscriminate acts.[403] Finally, humanity requires a military force to minimize unnecessary suffering by restricting the

[398] OP LAW HANDBOOK, *supra* note 347, at 12; Graham, *supra* note 159, at 89; Dinstein, *supra* note 153, at 109.
[399] OP LAW HANDBOOK, *supra* note 347, at 13.
[400] GC ASSESSMENT, *supra* note 152, at 6.
[401] OP LAW HANDBOOK, *supra* note 347, at 13.
[402] Michael N. Schmitt, *Wired Warfare: Computer Network Attack and the* Jus in Bello, 76 INT'L L. STUD. 187, 201 (2002).
[403] *Id*.

weapons, ammunition, and the methods in which they are used.[404] Humanity is related closely to distinction and prohibits indiscriminate weapons that lack any form of precision.[405]

Setting aside for the moment of who was behind the Stuxnet worm, it provides an excellent example of how Law of War principles can be used in a cyberteering context. Many states and non-state actors in the international community attempted to entice Iran to forego a nuclear program out of concerns that the program was being used to produce weapons-grade uranium. After multiple failed attempts to dissuade Iran, Stuxnet was released and effectively degraded Iran's nuclear program. One could make the argument that the use of the Stuxnet worm satisfies the necessity test as the international community has not banned computer viruses and it effectively brought Iran into submission, at least in the near-term. By programming Stuxnet to infect only a particular configuration of controllers produced by Siemens used at the Natanz facility, it arguably limited its destructive capability only to the nuclear plant believed to be producing weapons-grade uranium meeting the distinction requirement. While the true purpose of the Natanz nuclear facility will remain debated, the purpose of Stuxnet to disable and degrade but not destroy the facility meets the proportionality and humanity principles as well. By requiring the cyberteering agency use Law of War principles as a baseline for all uses of force employed, it will help ensure compliance on an international level.

## Conclusion

The Unexceptionalists have applied, and continue to apply, physical world notions of attribution and self-defense to cyberspace. But these proposals do little to

[404] OP LAW HANDBOOK, *supra* note 347, at 14.
[405] *See* GC ASSESSMENT, *supra* note 152, at 7.

deter cyber criminals and only impose more restrictions and hurdles on the victims and the responders. The Unexceptionalists' cybersecurity proposals are shackled to the principles of the physical world and lack the flexibility to respond to the private sector cyber threats. As this paper noted, it is the Unexceptionalists' approach that has led to an overall fragmented national cybersecurity policy and all but ignored a private sector cybersecurity policy. Moreover, the policies advanced by Unexceptionalists impose a criminal law evidentiary standard greatly defeating a deterrence effect due to the heightened attribution requirements in responding to cyberattacks and exploitations. This calls for a departure from past ways. I have taken an Exceptionalist approach in this paper. By first recognizing that cyberspace is inherently different, cybersecurity policy proposals are then free to discard traditional notions of laws in the physical world and apply laws that scale to the unique medium of cyberspace.

In many ways, the sea of the late 1700s is much like cyberspace today. No state exercised exclusive control over it, it was impossible to monitor and patrol effectively, and it was difficult to provide defense for a state's entire coastline. Likewise, just as land warfare could not be applied to naval warfare, the physical world cannot be applied to cyberspace. The use of letters of marque and reprisal provided a mechanism for fledgling nations with small navies to fill their naval security gap by outsourcing certain aspects of naval protection to the private sector. Privateering, for its many shortcomings, provided effective deterrence by striking the enemy where it hurt most—its economy. This paper demonstrated that the concept of letters of marque and reprisal can scale to cyberspace and provide a legal foundation for nations of all sizes to combat cyberattacks

and exploitation against their private sectors by curtailing the profitability of such attacks and exploitations.

This proposal takes a new approach to cyberdeterrence. It first jettisons the criminal law evidentiary standard. Second, the burden of proof is placed on a sliding scale commensurate with the level of force authorize for responses to attacks. Third, this proposal empowers the private sector private to provide security response for itself. Finally, it establishes a cyber court to issue warrants and adjudicate claims by those targeted by cyberteers. Most importantly, by ensuring that there will be a response to cyberattacks or exploitations on the private sector, it will likely provide a greater level of deterrence than the criminal law standard currently used.

Privateering was the Exceptionalist's answer to the question of how colonial America, in its infancy with no sizable navy to speak of, could possibly challenge the world's largest and best trained navy in the world. As America grew in size and power, letters of marque and reprisal fell into disuse as there was no longer a need to augment the U.S. Navy. With high speed Internet only recently becoming widely available to the public as a whole, the United States is only in the infancy of e-commerce and leveraging the power of the Internet. But just as in colonial America, the United States does not have the funding, resources, or trained personnel to compete against the sea of cyber criminals and hackers. The time has come for the United States to employ the Exceptionalists' approach to U.S. private sector cybersecurity by implementing cyberteering to counter the rising tide of cyberattacks and exploitation on the private sector.