

Hitting the Cyber Marque: Issuing a Cyber Letter of Marque to Combat Digital Threats

Major Christopher M. Kessinger*

I. Introduction

At any given time, millions upon millions of people connect to each other via cyberspace.¹ While a convenient method for grandparents to view pictures of their grandchildren, the Internet is also an exceedingly effective vehicle by which to attack a state, a company, or an individual. These attacks occur with frightening frequency, over 1,000 per hour in Great Britain alone²; and Britain recognizes the severity of the cyber threat.³ In the first four days of the November 2012 fighting between Israel and Gaza militants, over 44 million attacks on Israeli websites⁴ and an estimated 100 million total attacks occurred.⁵ Cyber-attacks cost Australia “an average of \$2 million per incident” and exceed a billion dollars per year.⁶ Successful attacks also occur against international bodies, such as the International Atomic Energy Agency.⁷ These cyber attacks seek not only military targets, but also industrial espionage.⁸

Despite the frequency and increasing severity of cyber attacks,⁹ many governments and industries around the world, to include the United States, are either seemingly helpless against the cyber onslaught,¹⁰ too dysfunctional¹¹ to create a useful offensive or defensive cyber scheme,¹² or are “highly immature with limited vision and strategic foresight.”¹³ Some foreign jurisdictions, our allies¹⁴ in the fight against cyber-attacks, fail to stem the tide of these attacks and now punish the cyber victims.¹⁵

This article explores the improbable, if not politically impossible, application of the letter of marque concept to the cyber arena. Despite the likely political stigma such a proposition would have in today’s Congress, letters of marque are nevertheless a constitutional and valid tool to execute cyber operations, and thus worthy of discussion.

Proposed defenses to cyber attacks are becoming increasingly complex and bizarre.¹⁶ However, one

* U.S. Army, Judge Advocate. Presently assigned as Administrative Law Attorney, Administrative Law Division, Office of The Judge Advocate General, U.S. Army.

¹ There were 2,405,518,376 Internet users accessing the Internet on 30 June 2012 alone. Enrique de Argaez, *Internet Usage Statistics: The Internet Big Picture*, INTERNET WORLD STATS <http://www.internetworldstats.com/stats.htm> (last visited Aug. 20, 2013).

² Tom Whitehead, *Britain Is Target of Up to 1,000 Cyber Attacks Every Hour*, TELEGRAPH, Oct. 22, 2012, <http://www.telegraph.co.uk/news/uknews/crime/9624655/Britain-is-target-of-up-to-1000-cyber-attacks-every-hour.html>.

³ “Today we are not at war, but I see evidence every day of deliberate, organised attacks against intellectual property and government networks in the United Kingdom from cyber criminals or foreign actors with the potential to undermine our security and economic competitiveness.” William Hague, Foreign Sec’y, U.K., Speech at Bletchley Park (Oct. 18, 2012), available at <http://www.fc.gov.uk/en/news/latest-news/?view=Speech&id=824617382>.

⁴ Shaun Waterman, *Israel Faces Attack On Cyber Front As Artillery, Air Fight With Gaza Continues*, WASH. TIMES, Nov. 19, 2012, <http://www.washingtontimes.com/news/2012/nov/19/israel-faces-attack-on-cyber-front-as-artillery-ai/?page=all>.

⁵ Nati Tucker & Orr Hirschauge, *Cyber Offensive Against Israel: 100 Million Attacks with Little to Show for It*, HAARETZ, Nov. 23, 2012, <http://www.haaretz.com/business/cyber-offensive-against-israel-100-million-attacks-with-little-to-show-for-it.premium-1.479998>.

⁶ Robert McClelland, Att’y Gen., Austl., Ten Years On: The Budapest Convention—A Common Force Against Cybercrime (Nov. 28, 2011), available at <http://www.attorneygeneral.gov.au/Speeches/Pages/2011/Fourth%20Quarter/23--November-2011--Cyberspace%20-%20The%20new%20international%20legal%20frontier.aspx>.

⁷ Adam Kredo, *IAEA Incursion*, WASH. FREE BEACON (Dec. 3, 2012, 5:00 AM), <http://freebeacon.com/iaea-incursion/>. The attack stole the personal information of 200 International Atomic Energy Agency (IAEA) scientists and highly sensitive information including satellite images. This was the

second time in two weeks that hackers compromised the IAEA’s internal computers.

⁸ China has infiltrated 141 companies in twenty industries and stolen “hundreds of terabytes of data.” MANDIANT, APT 1: EXPOSING ONE OF CHINA’S CYBER ESPIONAGE UNITS (Feb. 19, 2013).

⁹ Jana Winter & Jeremy A. Kaplan, *Washington Confirms Chinese Hack Attack on White House Computer*, FOX NEWS.COM (Oct. 1, 2012), <http://www.foxnews.com/tech/2012/10/01/washington-confirms-chinese-hack-attack-on-white-house-computer/>.

¹⁰ Greg MacSweeney, *Can Banks Prevent the Next Cyber Attack?*, WALL ST. & TECH. (Nov. 29, 2012), <http://www.wallstreetandtech.com/data-security/can-banks-prevent-the-next-cyber-attack/240142926>.

¹¹ Josh Rogin, *Who Runs Cyber Policy?*, THE CABLE (Sep. 25, 2012), http://thecable.foreignpolicy.com/posts/2010/02/22who_runs_cyber_policy.

¹² Michael Riley & Eric Engleman, *Why Congress Hacked Up a Bill to Stop Hackers*, BUS. WK. (Nov. 15, 2012), <http://www.businessweek.com/articles/2012-11-15/why-congress-hacked-up-a-bill-to-stop-hackers>.

¹³ Jeff Bardin, *Caution: Not Executing Offensive Actions Against Our Adversaries Is High Risk*, CSO SECURITY & RISK (Nov. 29, 2012), <http://blogs.csoonline.com/security-leadership/2469/caution-not-executing-offensive-actions-against-our-adversaries-high-risk?page=0>.

¹⁴ Fellow signatories to the European Convention on Cyber Crime. See *infra* Part IV.

¹⁵ John Leyden, *Crap Security Lands Sony £250,000 Fine for PlayStation Network Hack*, THE REGISTER, Jan. 24, 2013, http://www.theregister.co.uk/2013/01/24/sony_psn_breach_fine/.

¹⁶ E.g., Charles Q. Choi, *Auto-Immune: “Symbiotes” Could Be Deployed to Thwart Cyber Attacks*, SCI. AM. (Nov. 26, 2012), <http://www.scientific-american.com/article.cfm?id=auto-immune-symbiotes-could-be-deployed-to-thwart-cyber-attacks>.

historically effective and constitutional¹⁷ method of conducting both offensive and defensive operations has yet to be applied in a cyber context: the letter of marque.

This is a method of cyber self-help in which,

[i]n the context of privately conducted cyber attacks, letters or licensing could be used to specify the circumstances under which threat neutralization may be performed for the defense of property, the criteria needed to identify the attacking party with sufficiently high confidence, the evidence needed to make the determination that any given cyber attack posed a threat sufficiently severe as to warrant neutralization, and the nature and extent of cyber attacks conducted to effect threat neutralization.¹⁸

At its core, the letter of marque serves both military and law enforcement functions. Militarily, the government retains control over the letter of marque holder (a “privateer”) and responsibilities as delineated within the express terms of the letter of marque while at the same time broadening the military’s reach.¹⁹ As a law enforcement tool, a letter of marque deputizes an individual or company, thus vesting that entity with police powers. This authority allows the privateer to detain targets, bring them before the sovereign, and receive compensation based on successes, much like a bounty hunter.²⁰ Using civilian forces in a military/national defense context is not a concept limited to antiquity. For example, monitored non-governmental civilian participation in governmental operations exists with private military contractors. The United States spent over \$300 billion on military contractors from 2001–2007.²¹

There is an apparent aversion to the use of letter of marque and privateers.²² Various bills introduced throughout

the years proposing the revival of letter of marque have stalled or failed outright.²³ Despite the hesitation, letters of marque and privateers served a legitimate military purpose,²⁴ both in supplementing regular combat forces and crippling enemy commerce while protecting American commerce.²⁵ A cyber letter of marque would enable a privateer to seize digital assets, disrupt fiscal and communication networks, destroy attacking networks,²⁶ and act as a cyber bounty hunter.

Applying a letter of marque scheme to the cyber world would not only provide authority for American companies to defend themselves from cyber threats, but also allow them to take proactive measures to neutralize a cyber threat before it coalesces into danger. In addition to providing requisite authorization, a letter of marque scheme would regulate the conduct of a prospective cyber privateer and ensure accountability to effect compliance with the letter of marque’s mandate.

Part II of this article examines the historical usage of letters of marque and privateers. A brief historical discussion shows the use of letters of marque in national defense. Such historical perspective provides a useful background when considering their application to cyberspace. Part III applies legal and historical principles to a modern letter of marque regime. In particular, the application of letters of marque within the context of existing technologies and proposed authorization and oversight safeguards are examined. The various laws implicated in a modern cyber letter of marque regime are reviewed in Part IV. Finally, Part V addresses the authorizations and oversight necessary to effectively manage a successful, and lawful, cyber letter of marque regime. While not meant to be an exhaustive analysis of all possible facets related to the implementation of a cyber letter of marque regime, this article shows that despite some initial political and legal issues, using a cyber letter of marque can effectively mitigate the threats posed by cyber attacks.

II. History of Letter of Marque and Privateering

The concept of allowing private individuals to wage war on a foreign sovereign is not new, nor is it unique to United

¹⁷ Congress is authorized to “grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water.” U.S. CONST. art. I, § 8, cl. 11.

¹⁸ COMM. ON OFFENSIVE INFO. WARFARE, NAT’L RES. COUNCIL OF THE NAT’L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 208 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT].

¹⁹ Theodore T. Richard, *Reconsidering The Letter of Marque: Utilizing Private Security Providers Against Piracy*, 39 PUB. CONT. L.J. 452 (2010).

²⁰ *Id.* at 452.

²¹ Alexander Tabarrok, *The Rise, Fall and Rise Again of Privateers*, 11 INDEP. REV.: J. OF POL. ECON., No. 4, at 575 (2007), available at <http://www.independent.org/publications/tir/article.asp?a=631>.

²² *E.g.*, Elaine Supkis, *Ron Paul Wrong on Letter of Marque and Reprisal*, CULTURE OF LIFE NEWS (May 10, 2011, 2:32 PM), <http://e.smews/wordpress.com/2011/05/10/ron-paul-wrong-on-letter-of-marque-and-reprisal/>.

²³ H.R.J. Res. 290, 94th Cong. (1975); H.R.J. Res. 995, 94th Cong. (1976); H.R. 3074, 105th Cong. (2001); H.R. 3076, 107th Cong. (2001); and H.R. 3216, 110th Cong. (2007).

²⁴ They were not a method through which the U.S. Government could instigate “conquest, revolution, or general mayhem.” Kevin C. Marshall, *Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars*, 64 U. CHI. L. REV. 953, 958 (1997).

²⁵ EDGAR STANTON MACLAY, HISTORY OF PRIVATEERS 214–15 (1900); Jules Lobel, *Covert War and Congressional Authority: Hidden War and Forgotten Power*, 134 U. PA. L. REV. 1035, 1044 (1986); Marshall, *supra* note 24, at 958.

²⁶ See Robert P. DeWitte, *Let Privateers Marque Terrorism: A Proposal for a Reawakening*, 82 IND. L.J. 131, 140 (2007).

States history. The letter of marque²⁷ and privateering concepts have been a part of both international law and the accepted norms of warfare for centuries,²⁸ despite the Declaration of Paris—which purportedly banned privateering.²⁹ Hugo Grotius, considered by many to be the father of the modern Law of Armed Conflict, noted that letters of marque and reprisal are endorsed by the entirety of the law of nations.³⁰ Historians credit the expansion and development of the Western world from 1600 to 1815 to privateers.³¹

The letter of marque originally served as a “self-help” authorization, allowing a private individual to seek reprisal against a foreigner who caused him harm.³² Over time, this developed into a government’s authorization to act on its behalf and seize property belonging to an enemy government, usually in the form of ships and cargo.³³ In its most fundamental form, a letter of marque authorized private merchant ships to carry arms in self-defense.³⁴

²⁷ Originally, there was a distinction between a privateer and a letter of marque, however most scholars agree that by the time of the American Revolution there was no substantive difference between a letter of marque and privateer commission. See Richard, *supra* note 19, at 425. Therefore, for purposes of this paper, we will use Sir Thomas Barclay’s definitions of letter of marque and privateer: “a privateer is a private vessel, the captain of which received a commission (letters of marque) to carry on war and effect captures at his own risk and expense.” THOMAS BARCLAY, PROBLEMS OF INTERNATIONAL PRACTICE AND DIPLOMACY, WITH SPECIAL REFERENCE TO THE HAGUE CONFERENCES AND CONVENTIONS AND OTHER GENERAL INTERNATIONAL AGREEMENTS 204 (1907). Considerable research and writing is devoted to defining these terms and to their respective history should the reader wish to pursue this discussion in more depth. See, e.g., Richard, *supra* note 19 at 423–25; Todd Emerson Hutchins, *Structuring a Sustainable Letters of Marque Regime: How Commissioning Privateers Can Defeat the Somali Pirates*, 99 CAL. L. REV. 819, 844 (2011).

²⁸ See generally THOMAS GIBSON BOWLES, THE DECLARATION OF PARIS OF 1856: BEING AN ACCOUNT OF THE MARITIME RIGHTS OF GREAT BRITAIN; A CONSIDERATION OF THEIR IMPORTANCE; A HISTORY OF THEIR SURRENDER BY THE SIGNATURE OF THE DECLARATION OF PARIS; AND AN ARGUMENT FOR THEIR RESUMPTION BY THE DENUNCIATION AND REPUDIATION OF THAT DECLARATION 77 (1900) (referencing the *Consolato del Mare*, in 3 WILLIAM BLACKSTONE COMMENTARIES 250 (1765–1769)), available at <http://www.gutenberg.org/files/30802/30802-h/30802-h.htm> (“These letters are grantable by the law of nations.”).

²⁹ See *infra* Part IV.A (detailing discussion of why The Declaration of Paris is not applicable to the United States and the application of letters of marque to the cyber arena.).

³⁰ HUGO GROTIUS, THE RIGHTS OF WAR AND PEACE 312 (1624).

³¹ Larry J. Sechrest, *Privateering and National Defense: Naval Warfare for Private Profit* (2003), reprinted in *The Myth of National Defense: Essays on the Theory and History of Security Production* 247 (Hans-Hermann Hoppe ed., 2003).

³² See, e.g., Richard, *supra* note 19, at n.75; Hutchins, *supra* note 27, at 845; Marshall, *supra* note 24, at 954.

³³ Marshall, *supra* note 24, at 954.

³⁴ Richard, *supra* note 19, at 416.

Upon its founding, due to its small navy,³⁵ not only did the United States employ letters of marque, but it also was “the world’s biggest proponent of privateering.”³⁶ The Continental Congress issued many letters of marque,³⁷ as did individual states.³⁸ In fact, John Adams reportedly called an early letter of marque scheme, the Massachusetts Armed Vessels Act, “one of the most important documents of the Revolution.”³⁹

Thomas Jefferson was also an ardent proponent of privateering: “every possible encouragement should be given to privateering in time of war. . . . Our national ships are too few . . . to . . . retaliate the [sic] acts of the enemy. But by licensing private armed vessels, the whole naval force of the nation is truly brought to bear on the foe.”⁴⁰ Jefferson also realized that letters of marque served more than an offensive purpose, detailing how they are also a means of self-defense:

The ship Jane is an English merchant vessel . . . employed in the commerce between Jamaica and these States. She brought here a cargo of produce . . . and was to take away . . . flour. Knowing of the war when she left Jamaica, and that our coast was lined with small French privateers, she armed for her defense [sic], and took one of those commissions usually called *letters of marque*. She arrived here safely Can it be necessary to say that a merchant vessel is not a privateer? That though she has arms to defend herself in time of war, in the course of her regular commerce, this no more makes her a privateer, than a husbandman following his plough in time of war, with a knife or pistol in his pocket, is thereby made a soldier. The occupation of a privateer is attack and plunder, that of a merchant

³⁵ DeWitte, *supra* note 26, at 132; Richard, *supra* note 19, at 427. The colonial governments relied on privateering “to augment their weak navies.” *Id.*

³⁶ DeWitte, *supra* note 26, at 134.

³⁷ WORTHINGTON CHAUNCEY FORD, ED, 4 JOURNALS OF THE CONTINENTAL CONGRESS 1774-1789, at 229–33 (Mar. 23, 1776) (GPO 1906) (providing text of the resolution delineating national rules for letter of marque).

³⁸ CHARLES OSCAR PAULLIN, THE NAVY OF THE AMERICAN REVOLUTION: ITS ADMINISTRATION, ITS POLICY, AND ITS ACHIEVEMENTS 148 (1906); Mass Armed Vessels Act, 1775, Mass Acts. ch. 7, reprinted in 5 Mass Acts and Resolves 436–37.

³⁹ Marshall, *supra* note 24, at 960.

⁴⁰ DeWitte, *supra* note 26, at 134; SECHREST, *supra* note 31, at 247.

vessel is commerce and self-preservation.⁴¹

Support for letters of marque by the founding fathers was not merely philosophical consent. Thomas Paine and George Washington both owned stock in privateering ventures.⁴² Additionally, Benjamin Franklin practically ran his own privateering operation while he was assigned to France.⁴³ While most privateering ventures were for money, Franklin used the captured British ships, goods and men to trade for American prisoners of war.⁴⁴

Privateering in general weakened an enemy's economy and its ability to wage war.⁴⁵ The American privateers devastated British commerce, funding the first two years of the war substantially through British captures.⁴⁶ By early 1777, the British had lost 250 ships, resulting in the collapse of several major London-based West India merchant companies.⁴⁷ Within a year, American privateers captured 559 British ships.⁴⁸ Of the approximately 796 British ships captured during the Revolutionary War, American privateers and armed merchant ships accounted for roughly 600.⁴⁹ British merchants, feeling the crippling effect of American privateers,⁵⁰ ensured that "every pressure was brought to bear on Parliament for [the Revolutionary War's] discontinuance."⁵¹ Even ships carrying linen from England to Ireland feared the American privateers, to the point of demanding warship escorts.⁵²

⁴¹ Richard, *supra* note 19, at 437 (citing Letter from Thomas Jefferson, to Gouverneur Morris (Aug. 16, 1793)), in 3 MEMOIR, CORRESPONDENCE AND MISCELLANIES FROM THE PAPERS OF THOMAS JEFFERSON 275 (1829).

⁴² Tabarrok, *supra* note 21, at 567.

⁴³ *Id.*; see generally WILLIAM BELL CLARK, BEN FRANKLIN'S PRIVATEERS (1956).

⁴⁴ Tabarrok, *supra* note 21, at 567.

⁴⁵ CARL E. SWANSON, PREDATORS AND PRIZES: AMERICAN PRIVATEERING AND IMPERIAL WARFARE, 1739-1748, at 1 (Univ. of S.C. Press 1991).

⁴⁶ JAMES A. HUSTO, THE SINEWS OF WAR: ARMY LOGISTICS 1775-1953, at 21 (1966).

⁴⁷ ROGER KNIGHT, THE PURSUIT OF VICTORY: THE LIFE AND ACHIEVEMENT OF HORATIO NELSON 45 (2005).

⁴⁸ SECHREST, *supra* note 31, at 250.

⁴⁹ MACLAY, *supra* note 25, at viii.

⁵⁰ *Id.* ("God knows, if this American war continues much longer we shall all die with hunger.").

⁵¹ *Id.*

⁵² *Id.* at xii ("In no former war,' said a contemporary English newspaper, 'not even in any of the wars with France and Spain, were the linen vessels from Ireland to England escorted by war ships.'").

At the outset of the War of 1812, the British Navy consisted of 1,060 warships. In contrast, the United States Navy had only sixteen, including several that were unfit for sea.⁵³ As a consequence, the United States Navy was not considered to be a serious threat to British naval superiority.⁵⁴ In response, Congress passed a statute authorizing the use of privateers, but tightly controlled them.⁵⁵ The President could revoke, "at pleasure," any letters of marque he issued after June 1812. The applicant had to list specific details about the ship, crew, and owners, and "Ample security" submitted to ensure compliance with both international and United States law. Further, and perhaps most relevant to modern application, the ship commanders were required to keep a detailed log of everything "that occurs, daily, and transmit them to the government," and regular United States Navy commanders had to examine these logbooks when "meeting the privateer at sea."⁵⁶ Failure to abide by these rules would mean forfeiture of the bond and "of all interest in any captures which they may make."⁵⁷

With this new authorization in hand, American privateers wreaked havoc on British shipping and secured victory in America's second war for independence.⁵⁸ In the process, privateers tallied \$39 million in prizes, or roughly \$672.5 million in 2012 dollars.⁵⁹

Following the War of 1812, letters of marque did not disappear from the American landscape. President Andrew Jackson, in 1834, discussed the use of letters of marque against France.⁶⁰ Texas, upon declaring independence from Mexico, realized its coast was vulnerable due to a nascent navy. In response, the fledgling Texas legislature began to issue letters of marque with the intent to "protect the coast, harass Mexican shipping, and bring prizes that could be

⁵³ FRANCIS R. STARK, THE ABOLITION OF PRIVATEERING AND THE DECLARATION OF PARIS 127 (1897).

⁵⁴ MIRIAM GREENBLATT & JOHN STEWART LOWMAN, WAR OF 1812, at 82 (John S. Bowman ed., 1994) (2003) (British naval officers described the U.S. Navy as "bundles of pine boards" with "bits of striped rag floating over them.").

⁵⁵ An Act Concerning Letters of Marque, Prizes, and Prize Goods, ch. 107, § 9, 2 Stat. 759, 761 (1812).

⁵⁶ *Id.*

⁵⁷ FRANCIS H. UPTON, THE LAW OF NATIONS AFFECTING COMMERCE DURING WAR: WITH A REVIEW OF THE JURISDICTION, PRACTICE AND PROCEEDINGS OF PRIZE COURTS 181 (1863).

⁵⁸ See JEROME R. GARITEE, THE REPUBLIC'S PRIVATE NAVY: THE AMERICAN PRIVATEERING BUSINESS AS PRACTICED BY BALTIMORE DURING THE WAR OF 1812, at 244 (Wesleyan Univ. Press 1977).

⁵⁹ MACLAY, *supra* note 25, at ix (dollar equivalency for 2012 (\$39,000,000 to \$672,413,793.10) calculated using <http://www.davemanuel.com/inflation-calculator.php/>).

⁶⁰ UPTON, *supra* note 57, at 175.

auctioned off, with part of the proceeds going to the public treasury. In all, Texas issued six letters of marque.⁶¹ Similarly, President Polk recognized the lawful ability of Mexico to issue letters of marque during the Mexican American War.⁶²

In 1856, Britain, France and other titular world powers met in Paris to discuss concerns arising from wartime maritime law.⁶³ France and Great Britain sought to end privateering as they could not effectively control the use of privateers by their enemies, i.e., the United States and Russia.⁶⁴ Great Britain, in particular, recognized privateering as an effective tool of weaker navies that posed a threat to its naval supremacy and sought to contain it.⁶⁵ The result of this meeting was the Paris Declaration of 1856, a document attempting to ban privateering.⁶⁶

The Paris Declaration contained three major provisions:⁶⁷ the first provided that “[p]rivateering is, and remains, abolished;” the second prevented the seizing of enemy goods on neutral ships; and the third prevented capture of neutral goods on enemy ships.⁶⁸ Most importantly, the Declaration went to great pains to ensure that its provisions did not apply to any nation save signatories.⁶⁹ This provision is important for two reasons.

⁶¹ TEXAS PRIVATEERS, <https://www.tsl.state.tx.us/exhibits/navy/privateers.html> (last modified Aug. 30, 2011).

⁶² Although President Polk did take issue with the blank letters of marque issued by Mexico, arguing those were illegal under international law and those acting in accordance with such letters are considered to be pirates. UPTON, *supra* note 57, at 182.

⁶³ 1856 Paris Declaration Respecting Maritime Law (1856), *reprinted in* THE LAW OF NAVAL WARFARE: A COLLECTION OF AGREEMENTS AND DOCUMENTS WITH COMMENTARIES 64 (Natalino Ronzitti ed., 1987) [hereinafter PARIS DECLARATION].

⁶⁴

What influenced especially the English Government was the fear of America inclining against us, and lending to our enemies the co-operation of her hardy volunteers. The Maritime population of the United States, their enterprising marine, might furnish to Russia the elements of a fleet of privateers, which attached to its service by Letters of Marque and covering the seas with a network would harass and pursue our commerce even in the most remote waters.

TRAVERS TWISS, BELLIGERENT RIGHT ON THE HIGH SEAS, SINCE THE DECLARATION OF PARIS 10 (1856) (1884).

⁶⁵ Richard, *supra* note 19, at 428.

⁶⁶ “Privateering is, and remains, abolished. . . . The present Declaration is not and shall not be binding, except between those Powers who have acceded, or shall accede, to it.” *Id.*

⁶⁷ A fourth provision dealing with naval blockades that is not germane to the instant discussion. *See* PARIS DECLARATION, *supra* note 63, at 65.

⁶⁸ *Id.* at 64–65.

⁶⁹ *Id.* at 65.

First, it made clear that it was not intended to be a universal ban on privateering, as it only applied to signatory nations at war with other signatories.⁷⁰ Second, as stated in the document, it did not have the power to police the actions of non-signatories.⁷¹

The United States recognized that this agreement was merely a means for England to maintain maritime supremacy at the expense of nations with a smaller seafaring force, and accordingly, demanded conditions prior to capitulation.⁷² The United States agreed to acquiesce and sign the document only if protection of all non-contraband private property from capture at sea was included.⁷³ The United States reasoned that since all private property is protected on land, “why should it not be [protected] also on the sea?”⁷⁴

While the United States wanted to ensure it would be allowed to trade with both sides of a conflict, free from privateer entanglements, another more vital concern existed. According to Secretary of State William L. Marcy, “the United States could not forgo the right to send out privateers, which in the past had proved her most effective maritime weapon in time of war, and which, since she had no large navy, were essential to her fighting power.”⁷⁵ The United States realized that if privateering was banned, its nascent navy⁷⁶ would be no match for the greater naval might of countries such as Britain and France.⁷⁷ As the plenipotentiaries who signed the Declaration would not adequately address American concerns regarding private goods, and factoring in Marcy’s concern about the resulting unequal balance of naval power, the United States refused to sign the agreement.⁷⁸

The issue of privateering arose again in April 1861 when Confederate President Jefferson Davis, with Confederate Congressional approval,⁷⁹ issued letters of

⁷⁰ *See* Hutchins, *supra* note 27, at 855.

⁷¹ “The present Declaration is not and shall not be binding, except between those Powers who have acceded, or shall accede, to it.” PARIS DECLARATION, *supra* note 63, at 65; Hutchins, *supra* note 27, at 855.

⁷² EPHRAIM DOUGLASS ADAMS, GREAT BRITAIN AND THE AMERICAN CIVIL WAR 141 (1925).

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ ELBERT JAY BENTON, INTERNATIONAL LAW AND DIPLOMACY OF THE SPANISH AMERICAN WAR 129 (1908).

⁷⁷ ADAMS, *supra* note 72, at 141.

⁷⁸ PARIS DECLARATION, *supra* note 63, at 61–62.

⁷⁹ Confederate Cong., An Act Recognizing the Existence of War Between the United States and Confederate States, and Concerning the Letters of Marque, Prizes, and Prize Goods (1st Sess. Apr. 29, 1861).

marque against Northern shipping.⁸⁰ In accordance with this authorization, the South immediately sought to hire British and French privateers. Perhaps fearing the involvement of the British or French navies in the conflict, the Union declared that it would follow the Declaration and not issue letters of marque and Secretary of State Seward instructed American ambassadors to determine whether the signatories would be amicable to incorporating the proposed changes advocated by Marcy, thus allowing the United States to formally sign the Declaration.⁸¹ As an indication of the Union's fear of privateers, Secretary Seward authorized acquiescence to the Declaration even if the requested exceptions were not approved.⁸² Britain and France declined the advances and the United States remained a non-signatory.⁸³

Consequently, the Union passed a statutory authorization for President Lincoln to issue letters of marque⁸⁴ and declared that all attempts to disrupt, capture or destroy Union shipping would be treated as piracy and dealt with as such.⁸⁵ Regardless, the British entered the Civil War as privateers, sailing under letters of marque issued by the Confederacy. In fact, in a case brought by the United States against Britain for damages caused by a privateer, an international tribunal found no issue with a non-signatory (the Confederacy) issuing letters of marque to a signatory (Britain) "to construct, furnish, and crew ships to be used in commerce raids against a non-signatory, the United States."⁸⁶

When the United States entered into conflict with the Spanish during the Spanish American War, neither the United States nor Spain was a signatory to the Declaration of Paris.⁸⁷ Not only did Spain specifically reserve the right to issue letters of marque,⁸⁸ the Spanish government recognized

America's right and ability to issue the same.⁸⁹ The Spanish never carried out the threat, and President McKinley, for the first time, articulated a U.S. intention to comply with the Paris Declaration, though still not be a signatory.⁹⁰

Despite the reluctance, both Spain and the United States found ways to unofficially authorize privateers without formally issuing letters of marque.⁹¹ Both nations organized "auxiliary cruisers of the Navy."⁹² The United States Navy chartered private merchant ships, heavily armed them, and subsequently entered into naval service.⁹³ The Navy used the ships and manned them with the owner's regular, ostensibly civilian crew, placing the ships "under the entire control of the senior naval officer on board."⁹⁴ One such ship, the *City of Paris*,⁹⁵ actually took prizes, with the United States Prize Court holding that she was not a "vessel of the Navy nor a privateer . . ." ⁹⁶ and finally ruling that she was an "armed vessel in the service of the United States" and the civilian crew was "entitled as of right to share in the prize money."⁹⁷

While the nature of privateering changed with the Spanish-American War, privateering did not disappear. At the 1907 Hague Peace Conference, the United States again voiced its opposition to the privateering prohibition.⁹⁸ Specifically, the United States voiced the same concerns as

⁸⁰ ADAMS, *supra* note 72, at 141; JAMES D. RICHARDSON, A COMPILATION OF THE MESSAGES AND PAPERS OF THE CONFEDERACY INCLUDING DIPLOMATIC CORRESPONDENCE 1861-1865, at 60-62 (1905); MACLAY, *supra* note 25, at 504.

⁸¹ The Union approached Great Britain, France, Russia, Prussia, Austria, Belgium, Italy, Denmark, and the Netherlands. ADAMS, *supra* note 72, at 141.

⁸² ADAMS, *supra* note 72, at 141; STARK, *supra* note 53, at 155.

⁸³ Alexander Porter Morse, *Rights and Duties of Belligerents and Neutrals from the American Point of View*, 46 AM. L. REG. 657, 659-60 (1898).

⁸⁴ An Act Concerning Letters of Marque Prizes, and Prize Goods, ch. 85, 12 Stat. 758 (1863). Lincoln never commissioned any Union privateers. Richard, *supra* note 19, at 428.

⁸⁵ See JAMES RUSSELL SOLEY, THE BLOCKADE AND THE CRUISERS 170 (1883) (noting this meant pirates would be subject to execution).

⁸⁶ Hutchins, *supra* note 27, at 857.

⁸⁷ See PARIS DECLARATION, *supra* note 63, at 61-62 (providing a list of signatories and dates signed).

⁸⁸ BARCLAY, *supra* note 27, at 204.

⁸⁹ On 23 April 1898, Regent Queen Maria Cristina signed a declaration stating, among other things, that "Captains, skippers, officers of ships . . . not being Americans mak[ing] acts of war against Spain, will be considered as pirates . . . although they are protected by American letters of marque for privateers." KENNETH E. HENDRICKSON, JR., THE SPANISH-AMERICAN WAR 128 (Greenwood Publishing Group 2003).

⁹⁰ Morse, *supra* note 83, at 660.

⁹¹ BARCLAY, *supra* note 27, at 205. This scheme seems to have originated with the Prussians, who created a "volunteer navy" in 1870 in an attempt to circumvent the restrictions agreed up in Paris. The Prussians proposed putting civilian merchant seaman in Prussian navy uniforms and leaving them in command of their civilian ships. The French protested, claiming this to be privateering, in violation of the Declaration of Paris, and appealed to the British Secretary of Foreign Affairs, who sided with Prussia. *Id.*

⁹² HENDRICKSON, *supra* note 89, at 127-28; BARCLAY, *supra* note 27, at 204.

⁹³ BARCLAY, *supra* note 27, at 204.

⁹⁴ According to the agreements, the owner was required "to take on board two naval officers, a marine officer, and a guard of thirty marines" and the owner was to pay for all costs, which were reimbursable after certification by the senior U.S. Naval officer on board. *Id.* at 205.

⁹⁵ She was re-flagged as *Yale*. The Rita, 89 F. 763, 764 (1898).

⁹⁶ BARCLAY, *supra* note 27, at 205.

⁹⁷ *The Rita*, 89 F. at 768.

⁹⁸ JOSEPH HODGES CHOATE, THE SECOND INTERNATIONAL PEACE CONFERENCE, HELD AT THE HAGUE FROM JUNE 15 TO OCTOBER 18, 1907: INSTRUCTIONS TO AND REPORT FROM DELEGATES OF THE UNITED STATES, CONVENTIONS AND DECLARATIONS, FINAL ACT, WITH DRAFT OF CONVENTION RELATIVE TO THE CONVENTIONS (1908).

it did during the original 1856 negotiations,⁹⁹ that “the inviolability of unoffending private property belonging to the enemy on the high seas be guaranteed.”¹⁰⁰ Because other delegates gave no such guarantees, the United States, on two separate occasions, refused to acquiesce, proclaiming that “[i]t is well known that the Government of the United States of America has not adhered to that Declaration.”¹⁰¹ The issue of privateering rested with this last American objection¹⁰² until Congress drafted several bills calling for their reemergence.¹⁰³

III. Applying Letters of Marque to Cyber Warfare

Letters of marque were the original “self-help” governmental authorization.¹⁰⁴ While used to great effect in the past, they can now be resurrected and used to achieve similar results, especially in a cyber context. This section addresses the use of a cyber letter of marque in three areas: seizing assets; disrupting, disabling, and dismantling adversarial networks; and conducting cyber bounty hunting and rewards programs.

A. Seizing Assets

In a modern cyber letter of marque scheme, the U.S. government would authorize certain companies or individuals to track, freeze, and seize the illicit funds of designated criminal organizations. The net effect would be cutting off supplies to deliver the United States from its enemies.¹⁰⁵ For example, the United States has recently named several Russians as “transnational criminals” and promulgated an Executive Order that authorizes “seizure of their assets in the United States and prevents them from banking in dollars anywhere in the world.”¹⁰⁶

⁹⁹ See *supra* Part II.

¹⁰⁰ CHOATE, *supra* note 98, at 40.

¹⁰¹ *Id.*

¹⁰² Some have alleged that blimps operated on the west coast of the United States during World War II pursuant to letters of marque. “The Los Angeles based *Resolute* was the only airship . . . operated for the Navy under privateer status. . . .” JAMES SHOCK & DAVID SMITH, *THE GOODYEAR AIRSHIPS* 43 (2002). However, no congressional authorization was ever issued. See Richard, *supra* note 19, n.121; R.G. Van Treuren, *The Goodyear Airships*, NOON BALLOON, No. 83, 2009 at 6–7, available at <http://www.naval-airships.org/resources/Documents/tnb83.pdf> (providing a more detailed discussion).

¹⁰³ See *supra* note 23.

¹⁰⁴ Richard, *supra* note 19, at 416.

¹⁰⁵ Marshall, *supra* note 24, at 969 (quoting a letter from John Adams to the President of Congress).

¹⁰⁶ Kathy Lally, *Russian Crime Boss Gunned Down in Moscow*, WASH. POST, Jan. 16, 2013, <http://www.washingtonpost.com/world/europe/russian-crime-boss-gunned-down/2013/01/16/5b8663ac-600b-11e2-9940->

When rogue states, such as Iran, contravene the will of the international community, the most used method of ensuring compliance is via the United Nations Security Council or unilateral economic sanctions.¹⁰⁷ The United States first instituted sanctions against Iran in 1979, following the seizure of the American Embassy during the Iranian Revolution. These sanctions included freezing roughly \$11 billion in Iranian assets.¹⁰⁸ Iran continues to launder and hide money in contravention of these resolutions, often with the help of international banks.¹⁰⁹ In just one instance, the illicit transactions totaled \$250 billion.¹¹⁰ Iran has also turned to China, specifically its banking system, for help in escaping economic sanctions.¹¹¹ Illicit money laundering in contravention of United Nations resolutions is not limited to Iran, but has also included North Korea, Cuba, Sudan, and Mexican criminal cartels.¹¹²

6fc488f3fecdd_story.html?tid=pm_pop; Press Release, U.S. Dep’t Treas., Treasury Designates Brothers’ Circle Members (June 6, 2012), available at <http://www.treasury.gov/press-center/press-releases/Pages/tg1605.aspx>; Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

¹⁰⁷ Since 2006, at least eight United Nations (UN) Security Council Resolutions (UNSCR) have attempted to secure Iranian compliance with various international mandates. See, e.g., S.C. Res. 1696, U.N. Doc. S/RES/1696 (July 31, 2006), available at <http://www.un.org/News/Press/docs/2006/sc8792.doc.htm>; S.C. Res. 1737, U.N. Doc. S/RES/1737 (Dec. 27, 2006), available at <http://www.un.org/News/Press/docs/2006/sc8928.doc.htm>; S.C. Res. 1747, U.N. Doc. S/RES/1747 (Mar. 24, 2007), available at [http://www.un.org/apps/news/story.asp?NewsID=21997&Cr=Iran&Cr1=](http://www.un.org/apps/news/story.asp?NewsID=21997&Cr=Iran&Cr1=;); S.C. Res. 1803, U.N. Doc. S/RES/1803 (Mar. 3, 2008), available at <http://www.un.org/News/Press/docs/2008/sc9268.doc.htm>; S.C. Res. 1835, U.N. Doc. S/RES/1835 (Sept. 27, 2008), available at <http://www.un.org/News/Press/docs/2008/sc9459.doc.htm>; S.C. Res. 1929, U.N. Doc. S/RES/1929 (June 9, 2010), available at <http://www.unhcr.org/refworld/docid/4c1f2eb32.html>; S.C. Res. 1984, U.N. Doc. S/RES/1984 (June 9, 2011), available at <http://www.un.org/News/Press/docs/2008/sc9459.doc.htm>; S.C. Res. 2049, U.N. Doc. S/RES/2049 (June 7, 2012), available at <http://www.un.org/News/Press/docs/2012/sc10666.doc.htm>; *Factbox: Sanctions Imposed on Iran*, REUTERS, Jan. 20, 2011, available at <http://www.reuters.com/article/2011/11/22/us-iran-sanctions-fb-idUSTRE7AL11K20111122> (an over-view “of major sanctions imposed on Iran by the United States, the United Nations and the European Union over the years”).

¹⁰⁸ Suzanne Maloney, *The Revolutionary Economy*, U.S. INST. OF PEACE, <http://iranprimer.usip.org/resource/revolutionary-economy> (last visited Dec. 18, 2012).

¹⁰⁹ See, e.g., Jessica Silver-Greenberg, *Regulator Says British Bank Helped Iran Hide Funds*, N.Y. TIMES, Aug. 6, 2012, http://www.nytimes.com/2012/08/07/business/standard-chartered-bank-accused-of-hiding-transactions-with-iranians.html?pagewanted=all&_r=0.

¹¹⁰ Agustino Fontevicchia, *Standard Chartered Hid 60,000 Transactions With Iranian Banks Worth \$250B*, FORBES (Aug. 6, 2012 12:38 PM), <http://www.forbes.com/sites/afontevicchia/2012/08/06/standard-chartered-hid-60000-transactions-with-iranian-banks-worth-250b/>.

¹¹¹ Jessica Silver-Greenberg, *Prosecutors Link Money from China to Iran*, N.Y. TIMES, Aug. 29, 2012, <http://www.nytimes.com/2012/08/30/business/inquiry-looks-at-chinese-banks-iran-role.html>.

¹¹² *British Bank Makes \$2 Billion Settlement on Money Laundering Charges*, PBS NEWSHOUR, Dec. 11, 2011 (transcript and video available at http://www.pbs.org/newshour/bb/business/july-dec12/hsbc_12-11.html).

Money laundering is not exclusive to United Nations resolution violators; illegal activity also includes organized crime and tax evasion schemes.¹¹³ According to the United Nations Office on Drugs and Crime (UNODC), they report an estimated \$1.6 trillion dollars in money laundering in 2009 alone.¹¹⁴ While U.S. law enforcement has had some success in prosecuting international banks with substantial United States ties,¹¹⁵ less than one per cent of illegal money is seized globally.¹¹⁶ Seventy per cent of these illicit funds are funneled through the international banking system.¹¹⁷ “[T]racking the flows of illicit funds generated by drug trafficking and organized crime and analyzing how they are laundered through the world’s financial systems remain daunting tasks.”¹¹⁸ When faced with this exorbitant number, the victories scored by the justice system seem hollow. A cyber letter of marque would allow a privateer to seek these illicit funds wherever they may be hidden and either seize them or digitally sequester them for further law enforcement action. Such a cyber letter of marque brings to bear a formidable resource that will increase the likelihood for seizure of illicit funds and the shutdown of avenues for illicit funding.

The idea of using a letter of marque to effect an economic result is not novel. John Adams, in singing the virtues of privateering, said “[I]t is by cutting off supplies, not by attacks, sieges, or assaults, that I expect deliverance from enemies.”¹¹⁹ While letters of marque during the

¹¹³ *Illicit Money: How Much Is Out There?*, U.N. OFF. DRUGS CRIME (Oct. 25, 2011), <http://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money-how-much-is-out-there.html>. Organized crime includes drug trafficking, counterfeiting, human trafficking, and small arms smuggling.

¹¹⁴ This figure does not include funds lost to tax evasion. Most of the roughly \$35 billion income earned from cocaine sales in North America was laundered in North America and Europe. *Id.* The impact of tax evasion on this number is difficult to accurately determine due to the type of tax evaded (personal income tax, corporate tax, property tax, etc.) and the means and methods of actually calculating tax rates differ so much from nation to nation. PETER REUTER & EDWIN M. TRUMAN, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 12 (2004).

¹¹⁵ See, e.g., John Eligon, *Credit Suisse Settles Inquiry Over Iran Sanctions*, N.Y. TIMES, Dec. 16, 2009, http://www.nytimes.com/2009/12/17/business/global/17suisse.html?_r=1 (reporting that Credit Suisse bank agrees to pay \$536 million to settle charges of laundering from \$700 million to \$1.1 billion); Jessica Silver-Greenberg, *British Bank in \$340 Million Settlement for Laundering*, N.Y. TIMES, Aug. 14, 2012, <http://www.nytimes.com/2012/08/15/business/standard-chartered-settles-with-new-york-for-340-million.html> (discussing the agreement that the defendant bank would pay \$340 million in fines for laundering \$250 billion in Iranian funds).

¹¹⁶ U.N. OFF. DRUGS CRIME, ESTIMATING ILLICIT FINANCIAL FLOWS RESULTING FROM DRUG TRAFFICKING AND OTHER TRANSNATIONAL ORGANIZED CRIMES 5 (Oct. 25, 2011) [hereinafter TRANSNATIONAL ORGANIZED CRIME], available at http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

¹¹⁷ *Illicit Money: How Much Is Out There?*, *supra* note 113.

¹¹⁸ TRANSNATIONAL ORGANIZED CRIME, *supra* note 116, at 5.

¹¹⁹ Marshall, *supra* note 24.

Revolutionary War and the War of 1812 had distinct military objectives, they were “also a means of commercial warfare conducted for profit.”¹²⁰ Privateers “were engaged not in patriotic, but business ventures.”¹²¹ Some privateers amassed great fortunes through their letter of marque commissions,¹²² with even the common seaman receiving up to one thousand dollars above his regular wage from just one voyage.¹²³ The proceeds from captured enemy goods, once sold via the United States Prize Courts, were split between the privateer and the sovereign, thus providing a much needed injection of funds to the government and the privateer, while at the same time depriving the enemy of resources.¹²⁴

Motivated by the possibility of retaining a healthy percentage of the roughly \$1.6 trillion presently illicitly laundered worldwide, the number of prospective cyber privateers would be legion. Consequently, the United States government would be in a position to demand an exorbitantly high bond, thus guaranteeing that only the most technically proficient and responsible cyber privateers would seek the commission. As for the cyber profiteer, the prospect of sharing a large percentage of the trillions of dollars, not to mention the potential for criminal or tort liability,¹²⁵ would ensure strict compliance with the terms of the letter of marque. As the privateer in the 1700s and 1800s provided both a much needed governmental funding stream¹²⁶ and served a valid national security function, so too would a modern cyber privateer by removing illicit funds from the hands of organized crime and sanction violators. The end result would be a potential death blow to crime organizations and rogue regimes.

Currently, the law restricts anyone from attempting to seize assets, whether they belong to the most deplorable rogue regime or the most vicious drug cartel. A cyber letter of marque would vest responsible and vetted entities with authority to digitally seize illicit funds while providing legal protections from criminal and/or civil liability. Current laws restricting attempted seizures would remain in place for those acting without a valid letter of marque or those

¹²⁰ *Id.* at 958. Marshall simplistically asserts that privateering was primarily a money seeking venture and did not serve a valid military objective, without recognizing both goals are interchangeable.

¹²¹ PAULLIN, *supra* note 38, at 150–51. While downplaying the role of privateers and alleging they were merely profit seekers and not patriotic, Paullin later admits the “supplies captured from the British were often almost indispensable to the colonists.” *Id.* at 152.

¹²² DONALD A. PETRIE, THE PRIZE GAME 3–4 (1999) (comparing privateering to gambling, which could result in “fortunes [brought] home from the sea”).

¹²³ MACLAY, *supra* note 25, at 7.

¹²⁴ Richard, *supra* note 19, at 426.

¹²⁵ See *infra* Part V.

¹²⁶ See *supra* Part II.

operating outside the scope of their letter of marque commissions.

B. Disrupting, Disabling, and Dismantling Adversarial Networks

In December 2012, a cybercriminal known as “vorVzakone”¹²⁷ announced Project Blitzkrieg, wherein he¹²⁸ planned to attack 30 United States banks in an attempt to steal money from accounts belonging to the “rich.”¹²⁹ McAfee Labs, a leading computer security company,¹³⁰ determined that this “is a credible threat to the financial industry and appears to be moving forward as planned.”¹³¹ The projected losses from the announced attack could reach “hundreds of millions of dollars.”¹³² The targets of the planned attack included Bank of America, Capitol One, Suntrust, Ameritrade, eTrade, and Fidelity and Schwab.¹³³ From April to December 2012, vorVzakone claimed at least 500 cyber victims.¹³⁴

At roughly the same time that the U.S. banking industry began to deal with vorVzakone, bank officials were contending with cyber attacks emanating from Iran.¹³⁵ The attack’s complexities are comparable to that of “a pack of fire-breathing Godzillas.”¹³⁶ In fact, the internet traffic used in the attacks has been “multiple times” the number that Russia allegedly directed or encouraged at Estonia in a month-long online assault in 2007 that nearly crippled the

¹²⁷ Literally translated means “thief in law.” See KREBS ON SECURITY, *New Findings Lend Credence to Project Blitzkrieg*, <http://krebsonsecurity.com/tag/vorvzakone-gozi-prinimalka/> (last visited Dec. 12, 2012).

¹²⁸ While the exact identity of vorVzakone is unknown, he is believed to be a male, as shown by alleged photographs of vorVzakone online. KREBS ON SECURITY, *COM*, <http://krebsonsecurity.com/wp-content/uploads/2012/10/vorvnsdyt.png> (last visited Feb. 21, 2013).

¹²⁹ Bloomberg News, *vorVzakone’s Blitzkrieg Cyber Threat ‘Credible,’ McAfee Says*, *NEWSDAY* (Dec. 19, 2012, 9:05 AM), <http://newyork.newsday.com/business/technology/vorvzakone-s-blitzkrieg-cyber-threat-credible-mcafee-says-1.4352294>.

¹³⁰ See MCAFEE, <http://home.mcafee.com/Root/AboutUs.aspx> (last visited Feb. 21, 2013) (describing services offered and establishing credibility to make these determinations).

¹³¹ *Blitzkrieg Cyber Threat*, *supra* note 129.

¹³² David McMillin, *Banks vs. Cybercriminals*, *BANKRATE.COM*, <http://www.bankrate.com/financing/banking/banks-vs-cybercriminals/> (Dec. 15, 2012, 6:00 AM).

¹³³ KREBS ON SECURITY, *supra* note 127.

¹³⁴ *Id.*

¹³⁵ Nicole Perloth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, *N.Y. TIMES*, Jan. 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?hp&_r=1&.

¹³⁶ *Id.*

Baltic nation.¹³⁷ The attackers warned that they will not cease their attacks: “From now on, none of the United States banks will be safe.”¹³⁸ Iran denied all responsibility.¹³⁹

To add to the growing threat from Russian criminals and rogue nations like Iran, North Korea is greatly expanding its cyber capabilities, enabling it to “disrupt and immobilize [i]nternet traffic and key computer systems.”¹⁴⁰ In fact, Lee Dong Hoon, with the Center for Information Security Technologies at the Korean University in Seoul, surmises that the North Koreans have been preparing their cyber forces since the 1980s and “may rank third worldwide in this field after Russia and the United States.”¹⁴¹

Naturally, victimized United States banks are crying out for help from the federal government, while at the same time spending millions of dollars in an attempt to cease the attacks.¹⁴² Despite the aggressiveness, danger posed, and monetary cost, U.S. companies have received no more assistance than advice not to take any more aggressive defense measures than “contact[ing] the system administrator from the attacking computer to request assistance in stopping the attack or in determining its true point of origin.”¹⁴³ This purely defensive approach, obviously, has not worked, as “[t]he really good cyber hackers . . . are seldom stumped when trying to penetrate a network.”¹⁴⁴

While the U.S. government claims that “[a]ll options are on the table” with regard to responses to these attacks,¹⁴⁵ the one option that has not been discussed is a cyber letter of marque. The current law, and seemingly political position, is basically forcing U.S. companies to “just stand and take a

¹³⁷ *Id.*

¹³⁸ *Id.*

¹³⁹ Lee Ferran, *Iran Denies Cyber Attacks on U.S. Banks*, *ABC NEWS*, Jan. 11, 2013, <http://abcnews.go.com/Blotter/iran-denies-cyber-attacks-us-banks/story?id=18191088>. The entity taking credit for the attacks, the al-Qassam Cyber Fighters, also denies any State involvement. *Id.*

¹⁴⁰ *N. Korea Possesses Considerable Cyber Hacking Capability: Experts*, *YONHAP NEWS AGENCY*, Jan. 17, 2013, available at <http://english.yonhapnews.co.kr/northkorea/2013/01/17/18/0401000000AEN20130117008600315F.HTML>.

¹⁴¹ *Id.*

¹⁴² Siobhan Gorman & Danny Yadron, *Banks Seek U.S. Help on Iran Cyberattacks*, *WALL ST. J.*, Jan. 15, 2013, <http://online.wsj.com/article/SB10001424127887324734904578244302923178548.html>.

¹⁴³ *COMPUTER CRIME AND INTELL. PROP. SEC., U.S. DEP’T OF JUST., PROSECUTING COMPUTER CRIMES 180 (2007)*, available at <http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf>.

¹⁴⁴ RICHARD A. CLARKE & ROBERT K. KNAKE, *CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 127 (2010)*.

¹⁴⁵ Gorman & Yadron, *supra* note 142.

beating.”¹⁴⁶ Even if the U.S. government takes on a more proactive role in the cyber arena, it is widely accepted that U.S. law enforcement lacks the sufficient number of trained cyber police necessary to effectively engage the current and emerging cyber threats.¹⁴⁷

While a lot of “private companies only have simple fire walls that can be overcome [if] the hacker is an expert,”¹⁴⁸ some in the private sector claim to have the skill set required to confront this threat.¹⁴⁹ These attacks continue because, in part, there is no disincentive for the bad actors, as they know nothing will happen to them.¹⁵⁰ However, if the United States authorized tightly controlled offensive cyber capabilities via a congressionally authorized cyber letter of marque, the nation could allow a U.S. cyber entity to neutralize the attacker and their capabilities.¹⁵¹ As a direct consequence, the attacks will most likely cease and the attackers will move to easier targets.¹⁵² In essence, a cyber letter of marque would “arm” U.S. entities, thus allowing them to protect themselves in much the same way the historical letters of marque allowed merchant ships to arm themselves for self-defense purposes.¹⁵³

As with seizure of assets, ample historical support exists for the use of privateering in the disruption of enemy activity. As discussed previously,¹⁵⁴ American privateers disrupted English commerce to such an extent that several London-based firms went bankrupt.¹⁵⁵ British merchants,

¹⁴⁶ Bardin, *supra* note 13.

¹⁴⁷ *Id.*; Jody Westby, *Caution: Active Response to Cyber Attacks Has High Risk*, FORBES.COM, Nov. 29, 2012, <http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/>.

¹⁴⁸ *N. Korea Possesses Considerable Cyber Hacking Capability: Experts*, *supra* note 140.

¹⁴⁹ *See, e.g.*, TREADSTONE 71, <https://www.treadstone71.com/andCROWD-STRIKE>, <http://www.crowdstrike.com/services.html>.

¹⁵⁰ As Jeff Bardin says, “[a]s my information is being stolen, leveraged against me and used to impersonate me (like scores of thousands of other citizens), we continue to sit in rooms and discuss what to do.” Bardin, *supra* note 13.

¹⁵¹ This is as opposed to merely defending against it using tactics such as firewalls, which can be breached. *See generally* JOEL SCAMBRAY, GEORGE KURTZ & STUART MCCLURE, *HACKING EXPOSED* 464–65 (5th ed. 2005). Even the supposedly secure Johns Hopkins University Advanced Physics Laboratory (APL), which has contracts with the National Security Agency, was successfully hacked in 2009, which led to the loss of sensitive data in massive amounts. CLARKE & KNAKE, *supra* note 144, at 127.

¹⁵² “Most cyber criminals have absolutely no defensive posture whatsoever. When hit with an offensive attack, they quickly shift their targets since it is not cost effective and their whole intent is economic in nature.” Bardin, *supra* note 13.

¹⁵³ *See supra* Part II.

¹⁵⁴ *Id.*

¹⁵⁵ KNIGHT, *supra* note 47, at 45.

their livelihoods so disrupted and, in fact, disabled, put pressure on their own government to end the war and allow the Americans to have their independence.¹⁵⁶ The financial toll on the enemy during the War of 1812 by American privateers was staggering, which in turn had the operative effect of weakening both British naval superiority and morale in England. If privateering proved to be such an effective defensive weapon in a naval context, it can certainly be used in a cyber context where disrupting an enemy’s attack can be done through a keyboard by a handful of individuals instead of through fourteen-gun warships manned by over a hundred crewmen.¹⁵⁷

C. Cyber Bounty Hunting

The realm of cyber letters of marque is not limited to offensive or defensive actions in the classic sense. A cyber letter of marque could also be utilized as a method of bounty hunting, providing information to law enforcement agencies necessary to apprehend a cyber attacker.

Bounty hunting, like a letter of marque, is an activity intertwined with the history of the United States. The United States Supreme Court endorsed bounty hunting as a legal activity in the 1872 case *Taylor v. Taintor*.¹⁵⁸ The federal government endorsed, and continues to endorse, bounty hunting for capture (as opposed to kill) as exemplified in the most wanted lists.¹⁵⁹ Perhaps most famously, the United

¹⁵⁶ MACLAY, *supra* note 25, at xiii.

¹⁵⁷ GEORGE COGGESHALL, *HISTORY OF THE AMERICAN PRIVATEERS AND LETTERS-OF-MARQUE, DURING OUR WAR WITH ENGLAND IN THE YEARS 1812, '13, AND '14*, at 5 (1856) (describing the *Privateer America*, which captured twenty-seven British ships during five sorties during the War of 1812).

¹⁵⁸ 83 U.S. 366 (1872). The language usually cited as Supreme Court authorization for bounty hunting states:

When bail is given, the principal is regarded as delivered to the custody of his sureties. Their dominion is a continuance of the original imprisonment. Whenever they choose to do so, they may seize him and deliver him up in their discharge; and if that cannot be done at once, they may imprison him until it can be done. *They may exercise their rights in person or by agent. They may pursue him into another State; may arrest him on the Sabbath; and, if necessary, may break and enter his house for that purpose.* The seizure is not made by virtue of new process. None is needed. It is likened to the rearrest [sic] by the sheriff of an escaping prisoner.

Id. at 371 (emphasis added).

¹⁵⁹ The U.S. Marshal Service offers monetary bounties of up to \$25,000 for the capture of their “most wanted,” as depicted on their web page. *Fugitive Investigations—15 Most Wanted*, U.S. MARSHALS SERV., http://www.usmarshals.gov/investigations/most_wanted/index.html (last visited Feb. 21, 2013). Likewise, the FBI has its own list of wanted fugitives, offering \$100,000 to \$1 million for their capture. *Wanted by the FBI—Ten Most*

States issued a \$25 million bounty for information leading to the arrest or capture of Osama Bin Laden.¹⁶⁰ Even the U.S. Department of State endorses bounty hunting, offering rewards of up to \$5 million for the capture of purported terrorists through their Rewards for Justice Program.¹⁶¹ The United States is not alone in harboring a vibrant bounty hunting industry. Iceland recently hired a financial bounty hunter to track down fugitive bankers.¹⁶²

Individual American states adopted some form of the Uniform Criminal Extradition Act and passed laws¹⁶³ governing the conduct of bounty hunters, bail recovery agents, or similarly named entities. Most states have statutes that detail their licensing requirements, the bounty hunter's arrest authority, and insurance requirements. For example, Virginia sets minimum requirements spanning age, education, citizenship and requisite hours of Bail Enforcement Agent training.¹⁶⁴ Virginia also establishes criminal liability for operating as a bounty hunter without a valid license.¹⁶⁵ Some states restrict "freelance" bounty hunting, allowing only those who actually hold a bond to affect captures,¹⁶⁶ whereas some completely prohibit operation within their boundaries by bounty hunters from another state.¹⁶⁷ Conversely, some states have no training or licensing requirements.¹⁶⁸ Bounty hunting has become

Wanted, available at FED. BUREAU OF INVESTIGATION, <http://www.fbi.gov/wanted/topten> (last visited Feb. 21, 2013).

¹⁶⁰ The \$25 million reward was still active on the FBI's page days after he was killed in 2011. See Andrew Malcolm, *\$25-Million Bounty on Bin Laden Is Still Being Advertised by the FBI*, L.A. TIMES, May 4, 2011, <http://latimesblogs.latimes.com/washington/2011/05/25-million-bounty-on-bin-laden-was-it-withdrawn.html>.

¹⁶¹ REWARDS FOR JUSTICE, <http://www.rewardsforjustice.net/> (last visited Feb. 21, 2013).

¹⁶² Rob Wile, *Iceland Has Hired an Ex-Cop to Hunt Down the Bankers That Wrecked Its Economy*, BUS. INSIDER (Jul. 12, 2012), <http://www.business-insider.com/iceland-has-hired-an-ex-cop-bounty-hunter-to-go-after-the-bankers-that-wrecked-its-economy-2012-7>.

¹⁶³ See BAIL BOND LAWS, <http://fugitiverecovery.com/bail-bond-laws/overview/> for a fairly thorough summary of each state's laws as of 2001 (summarizing fifty state laws) (last visited Feb. 15, 2013).

¹⁶⁴ See VA. CODE ANN. §§ 9.1-186 to 186.13 (2008); 6 VAC 20-260 (Regulations Relating to Bail Enforcement Agents); *Bail Enforcement Agent*, VA. DEP'T CRIM. JUSTICE SERVS. <http://www.dcjs.virginia.gov/pss/special/bailenforcementagent.cfm> (last visited Feb. 10, 2013).

¹⁶⁵ See VA. CODE ANN. § 9.1 to 186.13.

¹⁶⁶ See, e.g., FLA. STAT. ANN. § 648.30 (2011).

¹⁶⁷ See, e.g., 725 ILL. COMP. STAT. 5/103-9 (2009).

¹⁶⁸ The Michigan Department of Licensing and Regulatory Affairs specifically states that no licensing is required to be a bounty hunter in the State of Michigan: "Q: How do I become a bounty hunter (skip tracer)? A: A license is not required in Michigan to become a bounty hunter or skip tracer." MICH. DEP'T OF LICENSING AND REG. AFF., http://www.michigan.gov/lara/0,4601,7-154-35299_10555_13648-141139--,00.html (last visited Jan. 22, 2013).

sufficiently "mainstream" in the United States that industry trade associations¹⁶⁹ have been established, with ethical codes, bylaws, and boards of directors.

The situation changes if a U.S. company uses a computer to track down a hacker, acquire evidence of illegality sufficient to support an arrest, obtain information from his/her computer sufficient to accurately pin point the hackers' location and then provide that information to law enforcement. This, arguably, would be illegal under current United States law.¹⁷⁰

The Computer Fraud and Abuse Act (CFAA) serves as a barrier to a corporation or individual¹⁷¹ from coming to the aid of a cyber-attack victim. Congress could carefully draft cyber letter of marquee legislation authorizing such entities to track and digitally "capture" a cyber criminal or terrorist. The only difference between the reward/bounty programs currently operated by the United States Government and a cyber letter of marquee is the antiquated CFAA prohibition.

Indeed, other scholars have posited the use of bounty hunting letters of marquee.¹⁷² For example, Robert P. DeWitte, writing in the *Indiana Law Journal*, discussed one of the potential downfalls between physical, as opposed to virtual, bounty hunting through the use of a letter of marquee. In particular, he illuminated the legitimate concern that "state authorities could conceivably attempt to capture and/or kill privateers" in their territory while operating under a valid U.S. letter of marquee.¹⁷³ However, this concern in a cyber letter of marquee context is not applicable since the cyber privateer/bounty hunter would be safely ensconced in the territorial United States, outside the physical reach of an unfriendly foreign armed force.

Just as letters of marquee are constitutional,¹⁷⁴ so too are bounties, as over a hundred years of U.S. jurisprudence demonstrates.¹⁷⁵ The issuance of a cyber letter of marquee

¹⁶⁹ See, e.g., NAT'L ASS'N FUGITIVE RECOVERY AGENTS (N.A.F.R.A.), <http://fugitive-recovery.org/> (last visited Dec. 24, 2012); NAT'L ASS'N BAIL BOND INVESTIGATORS, <http://nabbi.org/> (last visited Dec. 24, 2012).

¹⁷⁰ The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006), would most likely prevent a company or individual from taking these steps. See *infra* Part IV.

¹⁷¹ Corporations such as CrowdStrike or Treadstone 71 purportedly offer services that can be used to gather information from an adversary's computers to support an arrest by federal, state, or local law enforcement entities. See *supra* note 149.

¹⁷² DeWitte, *supra* note 26, at 146-47.

¹⁷³ *Id.* at 147.

¹⁷⁴ U.S. CONST. art. I, § 8, cl. 11.

¹⁷⁵ Hutchins, *supra* note 27, at 879-81. Hutchins details the history of the Bounty Act and associated jurisprudence. While Congress repealed the Bounty Act in 1899, "[a]ll the courts' jurisprudence on the law of capture

does not have to have the “bounty hunter” moniker, as it is analogous to a whistleblower or *qui tam*¹⁷⁶ suit whereby the privateer, minus the constraints of current domestic laws such as the CFAA, may gather information about an attacker or enemy and provide it to the proper authorities in return for monetary compensation. A cyber letter of marque would allow a cyber privateer access to those established and protected legal mechanisms.

IV. Legal Barriers

Despite the many potential applications of a cyber letter of marque, some arguments raise concerns about the legality of its application. When discussing letters of marque, most commentators cite to the same alleged legal barriers to implementation: domestic law, usually the CFAA; the Law of Armed Conflict, specifically attribution and self-defense concerns; the Paris Declaration of 1856; and the Council of Europe Convention on Cyber-crime. This section examines each of these areas and analyzes why they are not legal barriers to the implementation of a cyber letter of marque regime.

A. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act,¹⁷⁷ initially a criminal statute protecting government computers and those computers belonging to entities with compelling government interests,¹⁷⁸ forces companies under attack to “just stand and take a beating.”¹⁷⁹ Since its passage in 1984, it has expanded¹⁸⁰ to include civil liability by prohibiting anyone from “intentionally access[ing] a protected computer without authorization or exceed[ing] authorized access . . . [and recklessly causing damage¹⁸¹ involving a loss¹⁸² of] at least

remains unchanged and continues to hold that bounty and prize are constitutional.” *Id.*

¹⁷⁶ 31 U.S.C. §§ 3729–3733 (2006).

¹⁷⁷ 18 U.S.C. § 1030 (2006).

¹⁷⁸ This included not only government computers and networks, but also those of large banks, the New York Stock Exchange, etc. Robert B. Fitzpatrick, *Computer Fraud and Abuse Act: Current Developments*, SS006 A.L.I.-A.B.A. 1035, 1037 (2010).

¹⁷⁹ Bardin, *supra* note 13.

¹⁸⁰ The expanding scope of the Computer Fraud and Abuse Act (CFAA) has been described by Eric Goldman, professor at Santa Clara University School of Law, as “Frankenstein-ing,” resulting in a “horrible, hideous monster.” See Aaron Pressman, *Anti-hacking Law Questioned After Death of Internet Activist*, REUTERS, Jan. 15, 2013, available at <http://www.reuters.com/article/2013/01/15/us-swartz-idUSBRE90E17U20130115>.

¹⁸¹ “Damage” is “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8).

¹⁸² “Loss” includes “any reasonable cost to the victim.” See *id.* § 1030(e)(11).

\$5,000 in value.”¹⁸³ The definition of a “protected computer” has expanded to cover not only U.S. government computers, but also any computer “used in a manner that affects interstate or foreign commerce.”¹⁸⁴ Even those computers located outside the United States are protected.¹⁸⁵ Potentially, every single computer connected to the internet anywhere in the world would be a “protected computer” pursuant to the CFAA,¹⁸⁶ including, potentially, a blue-tooth-enabled garage door opener or coffeemaker in suburbia.¹⁸⁷

While the CFAA prohibits the mere access to a protected computer, causing damage seems to be the lynchpin to triggering civil and criminal penalties under the CFAA. Some courts have homed in on the damage requirement, refusing to find civil or criminal liability. For example, in *Moulton v. VC3*,¹⁸⁸ the court held that an unauthorized port scan and throughput test of a defendant’s servers is not a violation of the CFAA¹⁸⁹ since no “damage” was caused. Likewise, in *United States v. Czubinski*,¹⁹⁰ the court reversed the criminal conviction of an IRS agent who accessed a “protected computer” to satisfy his curiosity.¹⁹¹

While some of the judicial decisions seem to allow some degree of cyber intelligence collection under the current regulatory scheme,¹⁹² the courts clearly would not allow an entity to seize assets, whether they are being laundered at a major international bank or if information leading to their location is on a drug kingpin’s desktop

¹⁸³ See *id.* § 1030(g).

¹⁸⁴ See *id.* § 1030(e)(2).

¹⁸⁵ See *id.* § 1030(e)(2)(B).

¹⁸⁶ Jay P. Kesan & Carol M. Hayes, *Thinking Through Active Defense in Cyberspace*, NAT’L ACAD. PRESS (Oct. 12, 2010), available at <http://papers.ssrn.com/abstract=1691207>.

¹⁸⁷ See, e.g., Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 415, 494 (2012).

¹⁸⁸ *Moulton v. VC3*, 2000 WL 33310901 (N.D. Ga., 2000).

¹⁸⁹ Nor were these acts in violation of the Georgia Computer Systems Protection Act (1991). GA. CODE ANN. § 16-9-91 (1991).

¹⁹⁰ *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997).

¹⁹¹ “[M]erely viewing information cannot be deemed the same as obtaining something of value for purposes of this statute . . . [t]he Government failed . . . to prove . . . [Defendant] . . . intended anything more than to satisfy idle curiosity.” *Id.* at 1078.

¹⁹² Conducting throughput tests and scanning ports can detect system weaknesses, better positioning an attacker for follow-on action at a later date, if need be. While seemingly innocent, this could be an effective Operation Preparation of the Environment (OPE) for full scale cyber conflict. Due to sensitivity of the information discussed (cyber self-help), the expert agreed to be interviewed on the condition of anonymity. Interview with Cyber Security Expert (Nov. 2012) (notes on file with author).

computer. Consequently, government authorization would first be a necessity.¹⁹³

Despite allowing for criminal and civil penalties, the CFAA is not an effective means of preventing cyber attacks.¹⁹⁴ Some have argued that active-defense authorizations, such as a letter of marque, are not necessary as the cyber victim can turn over evidence of a cyber attack to the FBI for prosecution.¹⁹⁵ While this might work in theory, in actual practice it leaves the cyber victim virtually remediless for a host of reasons. For one, law enforcement personnel are questionably competent when it comes to cyber attacks and cyber crime.¹⁹⁶ Further, due to the global nature of cyber attacks, an American court might have a difficult time bringing a cyber attacker within its jurisdiction.¹⁹⁷ Even if a cyber attack victim captures all the information necessary to conduct a thorough law enforcement investigation, the FBI has bungled such gift-wrapped cyber cases in the past.¹⁹⁸

Just as cyber criminals are capable of seizing money from an individual's bank accounts,¹⁹⁹ cyber companies with the technical expertise can track down and seize illicit funds, given the proper governmental authorization. A cyber letter of marque would provide such authorization.

¹⁹³ See, e.g., NRC REPORT, *supra* note 18 (discussing the exemption for lawfully authorized law enforcement and intelligence agencies activities to the CFAA and how government agencies may commandeer private computes or pay for their usage).

¹⁹⁴ See *supra* Part I (discussing of the frequency of cyber attacks). The CFAA, in one form or another, has been in effect since 1984. It has had little to no affect on cyber attacks.

¹⁹⁵ See, e.g., Westby, *supra* note 147.

¹⁹⁶ Ms. Westby, while arguing a cyber victim should turn over information to law enforcement instead of proactively defending themselves, admits that "there are too few of them with skills adequate to match the sophisticated nature of today's cyber criminals." *Id.* Others have agreed with her assessment that there are too few cyber-competent law enforcement officers. Bardin, *supra* note 13.

¹⁹⁷ "[S]treet criminals were not stealing my Xbox and then fleeing to a foreign jurisdiction where the local authorities had no control." Zach, *Active Defense Has High Risk, But So Does Inaction: Forbes/CSO*, CYBER SECURITY LAW & POL'Y (Dec. 1, 2012), <http://blog.cybersecuritylaw.us/2012/12/01/active-defense-has-high-risk-but-so-does-inaction-forbesco/> (providing counter arguments to Westby's simplistic arguments against self help).

¹⁹⁸ An individual basically set up a honey pot webpage attracting Al-Qaeda militants. He turned over the information the FBI, who failed to act in a timely manner and the militants identified the site as a phony and warned their cohorts away. Associated Press, *Man Hijacks Al-Qaeda Site for FBI Use*, USA TODAY, http://usatoday30.usatoday.com/tech/news/2002-07-30-al-qaeda-online_x.htm (last visited Dec. 21, 2012).

¹⁹⁹ Heidi Blake, *Eastern European Cyber Criminal's Draining British Bank Accounts*, TELEGRAPH, Aug. 11, 2010, <http://www.telegraph.co.uk/finance/personalfinance/consumertips/banking/7938184/Eastern-European-cyber-criminals-draining-British-bank-accounts.html>.

B. Attribution and Self-Defense

Attribution is the legal requirement to positively identify the attacker prior to responding with force in self-defense.²⁰⁰ How does a prospective cyber privateer ensure it is striking the proper target²⁰¹ and how does a cyber-privateer cover their tracks so as to not entice further attacks? Admittedly, discovering the source of a cyber attack is "the most important aspect of active defense."²⁰² It necessarily must be a requirement when issuing a cyber letter of marque to ensure that the privateer is targeting the proper bad actor. Critics have complained that it is too difficult to identify the attacker with sufficient accuracy to ensure a counter-attack is accurately aimed.²⁰³ While tracing an attack may not provide actionable results, and some technologies "limit the ability to make perfect surgical strikes with active defense,"²⁰⁴ the problem may not be as big as it appears. Some speculate that it is more difficult for the bad actor to identify the cyber privateer than it is for the cyber privateer to identify the bad actor.²⁰⁵

The attribution concerns may, however, be a bit overblown.²⁰⁶ Even the Russian cyber attacks launched or encouraged against Estonia could be traced back to the "Russian intelligence apparatus."²⁰⁷ In fact, "attribution to at least some level will almost always be possible."²⁰⁸ While the exact technologies available to ensure accurate attribution, which can be done in seconds, are not the focus of this paper, such technology is not new and "is currently the subject of a significant amount of research aimed at improving accuracy and efficiency."²⁰⁹ While it may not be feasible, or even possible, to accurately attribute 100 million cyber attacks,²¹⁰ "it is clear that the current state of the

²⁰⁰ Alexander Melnitzky, *Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses*, 20 CORDOZO J. INT'L & COMP. L. 537, 540 (2012).

²⁰¹ That is, the cyber bad actor who is committing the misconduct leading to the letter of marque commission.

²⁰² Kesan & Hayes, *supra* note 187, at 481.

²⁰³ *Id.* at 451.

²⁰⁴ *Id.* at 481-82.

²⁰⁵ Bardin, *supra* note 13.

²⁰⁶ Lieutenant Commander 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, 77 (2009).

²⁰⁷ CLARKE & KNAKE, *supra* note 144 at 20.

²⁰⁸ Melnitzky, *supra* note 200, at 555 (quoting Robert K. Knake's testimony before the House Sub-committee on Technology and Innovation for the House Committee on Science and Technology).

²⁰⁹ Kesan & Hayes, *supra* note 187, at 330 (providing a basic discussion of the technologies available to ensure accurate attribution).

²¹⁰ See *supra* note 5.

technology is adequately advanced to permit the discussion of active defense to move forward into an evaluation of how an active defense scheme should be implemented.”²¹¹

C. Paris Declaration of 1856

Most critics of the letter of marque, regardless of its application, usually point to the Paris Declaration of 1856, noting that the United States is prohibited from employing privateers due to the agreement.²¹² This argument, however, is without merit.

First, the Declaration does not apply to the United States per the plain language of the treaty. “The present Declaration is not and shall not be binding, except between those Powers who have acceded, or shall accede, to it.”²¹³ The United States did not accede to it in 1856 and has not, in the ensuing 157 years, acceded to it. Under the rules of treaty interpretation,²¹⁴ a treaty is binding only upon parties to it,²¹⁵ and it “does not create either obligations or rights for a third State without its consent.”²¹⁶ Further, in order to impose an obligation on a third State, it must “expressly accept that obligation in writing.”²¹⁷ To date, the United States has not consented to the obligations of the Declaration in writing, as required by the Vienna Convention on the Law of Treaties.

Additionally, the Declaration clearly pertains, and limits itself, to maritime law.²¹⁸ Since a cyber letter of marque regime is not grounded in maritime law and letters of marque are specifically authorized in the United States Constitution, it is permissible under international law, Paris Declaration notwithstanding, to issue cyber letters of marque.

Others argue²¹⁹ that the Declaration has become customary international law.²²⁰ While this might be true at first blush, it ignores the legal and historical fact. A nation, not otherwise bound by a treaty, does not become bound by operation of the rule of customary international law if it has been a persistent objector. In order to be considered a persistent objector, and therefore not bound by a treaty, the State “must have objected to the emergence of a new norm during its formation and continue to object afterwards.”²²¹ Even if it has been state practice to follow the precepts in a treaty, non-signatory states can alter their actions in order to confront new threats.²²²

Regarding the Declaration of Paris, the United States objected during the formation of the proposed privateering ban²²³ and objected to the Declaration by passing legislation authorizing privateers during the Civil War;²²⁴ the Spanish government recognized America’s right to issue letters of marque during the Spanish-American War,²²⁵ and voiced opposition at the 1907 Hague Peace Conference.²²⁶ Clearly, the United States has been a persistent objector to the Declaration and thus not bound by it. Simply stated, American privateering declined not because of acquiescence to international treaties which it did not, and had no intent to, sign. Rather, privateering declined because America, after 1898, no longer had a nascent navy, had become a major

²¹¹ Kesan & Hayes, *supra* note 187.

²¹² See, e.g., Westby, *supra* note 147; Susan Brenner, *Marque and Reprisal*, CYB3RCRIM3 BLOG (May 18, 2009, 7:39 AM), <http://cyb3rcrim3.blogspot.com/search?q=marque>.

²¹³ PARIS DECLARATION, *supra* note 63.

²¹⁴ Vienna Convention on the Law of Treaties, art. 26, 23 May 1969, 1155 U.N.T.S. 331 [hereinafter Law of Treaties]. The United States has signed, though not ratified, this treaty. Nevertheless, the United States follows these rules in large part.

²¹⁵ *Id.* art. 34

²¹⁶ *Id.*

²¹⁷ *Id.* art. 35.

²¹⁸ “That maritime law, in time of war, has long been the subject of deplorable disputes.” Paris Declaration, *supra* note 63, at 64.

²¹⁹ Richard, *supra* note 19, at 429. *But see* DeWitte, *supra* note 26, at 132 (“The United States, however, is not a signatory to this treaty, and Congress could revive letters of marque and reprisal at any time.”).

²²⁰ “Nothing in articles 34 to 37 precludes a rule set forth in a treaty from becoming binding upon a third State as a customary rule of international law, recognized as such.” Law of Treaties, *supra* note 215, art. 38.

²²¹ *Customary Int’l Humanitarian Law*, INT’L COMM. RED CROSS, http://www.icrc.org/customary-ihl/eng/docs/v1_rul_in_asofcuin (last visited Dec. 21, 2012). See Joel P. Trachtman, *Persistent Objectors, Cooperation, and the Utility of Customary International Law*, 21 DUKE J. COMP. & INT’L L. 221 (2010) (providing a more detailed discussion of the persistent objector concept).

²²² This is the crux of the arguments advanced by many writers advocating a return of letters of marque in order to combat new threats such as terrorism and piracy. See, e.g., DeWitte, *supra* note 26; Richard, *supra* note 19.

²²³ ADAMS, *supra* note 72, at 141.

²²⁴ See *supra* note 85.

²²⁵ Morse, *supra* note 83, at 659–60.

²²⁶ CHOATE, *supra* note 98.

naval power,²²⁷ and the “cost-saving advantages of privateering [had] declined.”²²⁸

Assuming, *arguendo*, that the Paris Declaration is customary international law that the United States must follow, the issuance of cyber letters of marque is still not banned. The Declaration never defines privateers.²²⁹ As history demonstrates, a contracted civilian ship can be armed, staffed with civilians, fight, and take prizes—all without violating the Declaration.²³⁰

D. The Council of Europe Convention on Cyber-Crime²³¹

On 23 November 2001, the United States signed on to the Council of Europe Convention on Cybercrime.²³² The Cybercrime Convention came into effect in the United States on 1 January 2007.²³³ The Cybercrime Convention’s main objective “is to pursue a common criminal policy aimed at the protection of society against cyber-crime, especially by adopting appropriate legislation and fostering international co-operation.”²³⁴ It purports to allow countries to work together through substantive, procedural, and jurisdictional laws against a cyber criminal committing crimes in one country while physically located in another.²³⁵ Prior to the Cybercrime Convention (and some would argue even today),²³⁶ the cyber police forces in the United States or internationally did not have the tools or authority necessary to combat cyber-attacks. Additionally, it did not address the

cultural issues that may arise from crimes committed in cyberspace.²³⁷ To make matters worse, some countries did not have adequate laws against cyber-crime.²³⁸

An attempt to correct these law enforcement deficiencies was the impetus for the creation of the Cybercrime Convention. It remains the only international treaty attempting to deal with the issue of transcontinental cyber attacks.²³⁹ It fails, however, to effectively protect anyone from cyber attacks. It is largely a symbolic document, serving mainly to reassure the public that governments are doing *something* to address the threat.²⁴⁰ Those reassurances are hollow, as only roughly half of the ratifying states have passed domestic legislation required to enforce the document.²⁴¹

Remarkably, the exceptions contained in the Cybercrime Convention negate its impact. First, no requirement exists that any cyber attacker actually be prosecuted; instead, the State must merely “report the final outcome to the requesting Party [i.e., the cyber victim’s nation] in due course.”²⁴² In addition, nearly every enforcement provision of the Cybercrime Convention contains a legislative flaw, allowing a nation state to refuse to cooperate.²⁴³ A nation may refuse a request for assistance during or after a cyber attack emanating from its country for a host of reasons. These reasons include, but are not limited to²⁴⁴: if a request for assistance would violate domestic laws,²⁴⁵ if a request for assistance and information gained

²²⁷ The U.S. Navy, under Commodore George Dewey, destroyed the Spanish fleet at the Battle of Manila Bay on May 1, 1898. *Spanish-American War*, U.S. DEP’T OF NAVY—1898 NAVAL HISTORICAL CTR. (July. 15, 1996) <http://www.history.navy.mil/faqs/stream/faq45-11.htm>. *Id.* In July, 1898, Admiral William Sampson decimated the Spanish fleet off of Cuba. *Id.* “America emerged from the Spanish-American War as a major naval power.” *Id.*

²²⁸ Tabarrok, *supra* note 21, at 575.

²²⁹ PARIS DECLARATION, *supra* note 63, at 64.

²³⁰ See *Rita*, 89 F. 763, 768 (1898); BARCLAY, *supra* note 27, at 205; Richard, *supra* note 19, at 429–30.

²³¹ Council of Europe, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, S. Treaty Doc. No. 108-11, 2001 WL 34368783, 41 I.L.M. 282 [hereinafter Cybercrime Convention].

²³² COUNCIL OF EUROPE CONVENTION ON CYBERCRIME, <http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=23/01/2013&CL=ENG>. (last visited Feb. 21, 2013) (providing chart displaying signatures and ratifications by specific countries).

²³³ *Id.*

²³⁴ Cybercrime Convention, *supra* note 231, at pmbl.

²³⁵ Sara L. Marler, *The Convention on Cyber-Crime: Should the United States Ratify?*, 37 NEW ENG. L. REV. 183, 196 (2002).

²³⁶ Bardin, *supra* note 13.

²³⁷ What may be legal in one country, may not be in another, thus creating law enforcement problems when trying to enforce any laws in cyberspace. Nancy E. Marion, *The Council of Europe’s Cyber Crime Treaty: An Exercise in Symbolic Legislation*, 4 INT’L J. CYBER CRIMINOLOGY 699, 700 (2010).

²³⁸ For example, the two creators of the infamous ILOVEYOU virus in the Philippines were never charged as that country had enacted no laws prohibiting their acts. Wayne Arnold, *Philippines to Drop Charges on E-Mail Virus*, N.Y. TIMES, Aug. 22, 2000, <http://www.nytimes.com/2000/08/22/business/technology-philippines-to-drop-charges-on-e-mail-virus.html>. This one virus caused an estimated \$10 billion in damage. Paul Festa & Joe Wilcox, *Experts Estimate Damages in the Billions for Bug*, CNET NEWS (May 5, 2000, 1:55 PM), http://news.cnet.com/Experts-estimate-damages-in-the-billions-for-bug/2100-1001_3-240112.html.

²³⁹ Marion, *supra* note 237, at 701.

²⁴⁰ *Id.*

²⁴¹ *Id.* at 701–02.

²⁴² MICHAEL A. VATIS, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 207, 214 (2010); Cybercrime Convention, *supra* note 232, art. 24.

²⁴³ See, e.g., *id.* arts. 24–29.

²⁴⁴ See VATIS, *supra* note 242, at 214–18 (discussing the numerous loopholes contained in the Cybercrime Convention); Cybercrime Convention, *supra* note 231, art. 24.

²⁴⁵ Cybercrime Convention, *supra* note 231, art. 25.

therefrom could be used in any investigation or court proceedings other than those listed in the request,²⁴⁶ or if an attacked nation believes there are political issues at play.²⁴⁷

Perhaps as a sign of the naïve belief that the feckless Cybercrime Convention will actually curb cyber attacks, the Council of Europe's Committee of Experts on Terrorism opined in February 2010 that no further conventions are needed to address cyber terrorism because "large scale attacks on computer systems appeared to be already covered by the Cybercrime Convention."²⁴⁸ Yet two days later, on 18 February 2010, The Washington Post broke the story that more than 75,000 computers and roughly 2,500 companies in the United States, Saudi Arabia, Egypt, Turkey, and Mexico were victims of "one of the largest and most sophisticated attacks by cyber criminals discovered to date."²⁴⁹ The attack began in 2008 and was not discovered until January 2010.²⁵⁰

In the United States, an unnamed Department of Justice official purportedly alleged that the "impact of the convention [is] 'very positive,'" which, again, seems to ignore the reality of cyber attack's scope.²⁵¹ To the contrary, the Cybercrime Convention seems to merely limit the ability of a law-abiding entity to take proactive steps necessary to cease a cyber threat.²⁵²

²⁴⁶ This provision, in effect, means that if the information leads to more criminals, and a nation wants to prosecute them, it may not use this information in that investigation/prosecution. The nation must start over in the investigative process as it relates to the newly discovered bad actors. *Id.* art. 28.

²⁴⁷ *Id.* art. 27.

²⁴⁸ VATIS, *supra* note 242, at 219 (quoting Council of Europe Committee of Experts on Terrorism (CODEXTER), Opinion of the Committee of Experts on Terrorism (CODEXTER) for the Attention of the Committee of Ministers on Cyber terrorism and Use of Internet for Terrorist Purposes).

²⁴⁹ Ellen Nakashima, *More Than 75,000 Computer Systems Hacked in One of Largest Cyber Attacks, Security Firm Says*, WASH POST, Feb. 18, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021705816.html>.

²⁵⁰ *Id.*

²⁵¹ VATIS, *supra* note 242, at 209 (quoting an unnamed U.S. Dep't of Justice official).

²⁵² As Bardin states:

Do we really think that establishing a convention on cyber crime is going to stop our adversaries? They do not recognize our virtual boards or virtual sovereignty as it is. Why would they recognize a convention on cyber crime? All this does is force offensive cyber forces to establish an unwieldy 'rules of engagement' that ties the hands of those who can execute offensive cyber actions.

Bardin, *supra* note 13.

Because the Cybercrime Convention does not diminish cyber attacks, lacks any enforcement or prosecution mechanism and expressly states that signatory states pass domestic criminal laws covering "illegal access,"²⁵³ "illegal interception,"²⁵⁴ "criminal misuse of devices,"²⁵⁵ [*emphasis added*], the United States is not prevented from issuing letters of marque. If Congress exercised its constitutionally authorized power to issue letters of marque, limited to cyber operations, no violation of any provision of the Convention would occur because no domestic criminal acts occur.

Even the U.S. Attorney General stated, in 2006, that the Cybercrime Convention "is in full accord with *all U.S. Constitutional protections*."²⁵⁶ The activity undertaken pursuant to a constitutionally authorized and congressionally endorsed cyber letter of marque would not, under United States law, be illegal and thus not a violation of any provision contained in the Cybercrime Convention. In short, a cyber letter of marque issued by Congress would not violate the Council of Europe Convention on Cybercrime.

V. Authorizations and Oversight

While a cyber letter of marque is legal, both under domestic and international law, any cyber letter of marque regime must provide for a method of authorizing and subsequently supervising a cyber privateer. This section discusses some potential methods of authorization and oversight necessary for an effective cyber letter of marque regime.

A. Issuance of Bonds and Authorizations

Prior to the issuance of a letter of marque, all prospective cyber privateers should be required to register with a central governmental database. This database would provide the supervising agency²⁵⁷ with a means of not only policing cyber privateers and holding them accountable, but also a means for parties allegedly aggrieved by United States authorized cyber privateers to seek redress. Such a database and registration would also allow the supervisory agency an opportunity to vet the putative cyber privateer. "If a company does not have the skills to defend its systems, it likely does not have the skills to attack back—or make

²⁵³ *Id.* ch. II, art. 2.

²⁵⁴ *Id.* art. 3.

²⁵⁵ *Id.* ch. II, art. 6.

²⁵⁶ Statement of Alberto Gonzales, Attorney General for the U.S., on the Passage of the Cybercrime Convention (Aug. 4, 2006), *available at* http://www.justice.gov/opa/pr/2006/August/06_ag_499.html (*emphasis added*).

²⁵⁷ Whether it is a congressional sub-committee, the NSA, DHS, etc.

decisions about whether to engage in such actions.”²⁵⁸ If the applicant does not possess the requisite skills, then its request for a cyber letter of marque is denied.²⁵⁹

Further, all applicants must be able to post a bond commensurate with potential liability exposure. “Letters of marque should only be issued to security firms able to post a significant bond and meet specific qualification and training requirements.”²⁶⁰ The bond requirement is the most effective method for screening out “start-ups” and “fly-by-night” security companies from seeking a letter of marque.²⁶¹ The Act Concerning Letters-of-Marque, Prizes & Prize Goods specifically states that before the issuance of any commission of letters of marque, a bond in the amount of five thousand dollars, or ten thousand dollars if the ship had more than one hundred and fifty men, would have to be paid by two “responsible sureties, not interested in such vessel.”²⁶² The payment of such a steep bond ensures that privateers strictly adhere to congressional rules.²⁶³

In a cyber context, since the stakes are so high, a prospective cyber privateer should be required to supply a large monetary bond.²⁶⁴ A large monetary bond would not only ensure that responsible entities apply for and receive cyber letters of marque, but also that those with the requisite discretion and technical expertise are the only ones acting with congressional authority as a cyber privateer. The prime importance of competent exercise of the powers enumerated in the letter of marque is underscored when the vast amount of money and intellectual property lost on a frequent and recurring basis, coupled with the exacting nature of establishing positive identification, especially attribution, is contemplated. A large monetary bond would, in effect, keep the cyber cutthroats out of this business.

Singapore established CaseTrust, a similar system, in order to protect consumers engaged in e-commerce. CaseTrust receives complaints against e-vendors and legitimizes member companies. Prior to joining, a

²⁵⁸ Westby, *supra* note 147 (quoting Dave Dittrich, one of the first cybersecurity experts to explore the concept of active defense).

²⁵⁹ *Id.*

²⁶⁰ Richard, *supra* note 19, at 455.

²⁶¹ *Id.* at 456.

²⁶² An Act Concerning Letters of Marque, Prizes, and Prize Goods, Ch. 107, § 9, 2 Stat. 759, 761 (1812).

²⁶³ Tabarrok, *supra* note 21, at 575, 570.

²⁶⁴ See, e.g., *America's Top Cyberwarrior Says Cyberattacks Cost \$250 Billion a Year*, INT'L BUS. TIMES, July 13, 2012, <http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year-722559>; BRIAN CASHELL, WILLIAM D. JACKSON, MARK JICKLING & BAIRD WEBEL, THE ECONOMIC IMPACT OF CYBER-ATTACKS (2004), available at http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

prospective e-vendor must give a banker's guarantee, or a bond, to establish that it is indeed a legitimate and reputable company. The CaseTrust system provides for compulsory adjudication including the power to not only fine a vendor, but also to revoke its certification. As a result, the consumer is protected by providing a source of bonded companies and a policing mechanism. Additionally, the commercial entities are shrouded with governmental legitimacy. To date, enforcement has been effective and participation is growing.²⁶⁵

In a historical context, the putative privateer kept detailed daily logs, which were available for inspection by any U.S. naval commander he might encounter.²⁶⁶ Similar requirements would be made of cyber privateers. As all internet activity can be, or actually is, easily monitored,²⁶⁷ this requirement does not place too onerous a burden on the purported cyber privateer. While most private companies are loathe to share details of their cyber activity for fear of losing intellectual property, a competitive edge, or disclose their cyber defenses or weaknesses,²⁶⁸ a company serious about executing a defensive or even offensive cyber letter of marque should be willing to accept the more stringent scrutiny, such as reviewing cyber logbooks.

A cyber letter of marque would designate the bearers to be licensed combatants for the sovereign, authorizing them to “bear arms” in the cyber sense of the word, and either defend against specific attacks and launch counter attacks (hack-backs) or engage in offensive cyber operations directed at sovereign selected targets or networks.²⁶⁹ A private company could be granted authorization to conduct a hack-back, temporarily incapacitating a cyber bad actor, and then notify the appropriate law enforcement or national security entity for final apprehension or network termination.²⁷⁰

²⁶⁵ COMMONWEALTH SECRETARIAT, LAW IN CYBERSPACE 23 (2001); *Consumers Association of Singapore*, CASETRUST.ORG, <http://www.case-trust.org.sg/> (last visited Feb. 1, 2013).

²⁶⁶ Ch. 107, § 9, 2 Stat., at 761.

²⁶⁷ See, e.g., Andy Greenberg, *Stealthy Government Contractor Monitors U.S. Internet Providers, Worked with Wikileaks Informant*, FORBES, Aug. 1, 2010, <http://www.forbes.com/sites/firewall/2010/08/01/stealthy-government-contractor-monitors-u-s-internet-providers-says-it-employed-wiki-leaks-informant/>.

²⁶⁸ See, e.g., Robert McFarvey, *Threat of the Week: Corporate Credit Unions Should Bolster Defenses Against DDoS*, CREDIT UNION TIMES, Jan. 22, 2013, <http://www.cutimes.com/2013/01/22/threat-of-the-week-corporate-credit-unions-should?ref=hp>.

²⁶⁹ See D. Joshua Staub, *Letters of Marque: A Short-Term Solution to an Age Old Problem*, 40 J. MAR. L. & COM. 261, 265 (2009); Richard, *supra* note 19, at 464 (proposing that letters of marque be used to deal with Somali piracy in both defensive and offensive roles).

²⁷⁰ See Zach, *Steven Chabinsky (Crowdstrike, Ex-FBI Cyber Division) Talks Private Sector Cyberdeterrence at ABA's Natsec Law Conference*, CYBER SECURITY L. & POL'Y (Nov. 30, 2012), <http://blog.cyber->

In recognition that cyber privateers would, to a certain extent, be bearing arms, a workable set of rules of engagement would necessarily be a major part of the actual commission. Professor Susan Brenner has expressed concerns that cyber privateers could be motivated to vigilantism and exceed the bounds of their charter, exhibiting an inability to determine who is a just target.²⁷¹ These concerns can be easily alleviated by carefully drafted rules of engagement and scope of authorization in the letter of marque commission itself. If cyber privateers exceed the scope of the commission, they lose their substantial bond, face debarment from future government contracts, and open themselves up to potential criminal prosecutions since their actions were outside the scope of the immunity granted by the letter of marque. These adverse ramifications should keep a vetted and approved cyber privateer in line.

B. Legal and Judicial Oversight

The legal framework for a workable letter of marque regime already exists under current federal law.²⁷² “Privateering worked only because it was backed by a substantial system of law, not only the common law of property, but also the statutory creations such as admiralty courts and bond requirements.”²⁷³ The federal judiciary is vested with original jurisdiction to determine prizes,²⁷⁴ burdens of proof established,²⁷⁵ the due process rights of both the captor and the captive duly considered,²⁷⁶ and the

securitylaw.us/2012/11/30/steven-chabinsky-crowdstrike-ex-fbi-cyber-division-talks-private-sector-cyberdeterrence-at-abas-natsec-law-conference/.

²⁷¹ Brenner, *supra* note 212.

²⁷² *See, e.g.,* Commissioning Private Vessels for Seizure of Piratical Vessels, 33 U.S.C. § 386 (2006).

The President is authorized to instruct the commanders of the public armed vessels of the United States, and to authorized the commanders of any other armed vessels sailing under the authority of any letters of marquee and reprisal granted by Congress, or the commanders of any other suitable vessels, to subdue, seize, take, and, if on the high seas, to send into any port of the United States, any vessel or boat built, purchased, fitted out, or held as mentions in 33 U.S.C. § 385.

Id.

²⁷³ Tabarrok, *supra* note 21, at 572.

²⁷⁴ Jurisdiction, 10 U.S.C. § 7652 (2006).

²⁷⁵ *See* The Resolution, 2 U.S. 19 (U.S. 1781) (holding that the burden of proving a prize was captured lawfully lies with the captors).

²⁷⁶ The legality of a capture is not determined until a court of competent jurisdiction has issued an order making such a determination. *Id.* Whether property seized may be confiscated as a prize is a judicial question and each case is to be decided on its own facts. Property Captured by the Potomac Flotilla, 10 Op. Att’y Gen. 467 (1863).

interests of the United States represented by a duly appointed authority in the “United States attorney for the district in which the prize cause is adjudicated.”²⁷⁷ In fact, Chapter 655 of 10 U.S.C. contains the entire statutory framework to judicially administer a letter of marque regime.

Historical precedence demonstrates that judicial oversight is an effective means to monitor and police privateers. For example, the court invalidated the first two prizes claimed during the War of 1812 because of improperly issued letters of marque.²⁷⁸ Even the venerable USS *Constitution* was also involved in an illegitimate capture, a situation embarrassingly rectified by the courts.²⁷⁹ Indeed, a rich legal history of privateering cases exists before the United States Supreme Court.²⁸⁰

Some are concerned that the government would not be able to control the behavior of modern privateers, especially in a cyber context.²⁸¹ In reality, these concerns are easily addressed with stiff consequences.²⁸² Penalties can include forfeiture of the bond and any pay due as a result of a successful capture or mission, seizure of assets,²⁸³ debarment from all future government contracts,²⁸⁴ exclusion from future letter of marque commissions, criminal prosecution, and potential tort liability.²⁸⁵

At least two presidents proposed criminal prosecution for misuse of a letter of marque. President Jefferson, a major proponent of privateering during the Revolutionary War,²⁸⁶ declared that individuals operating off the coast without valid commissions be captured and tried as pirates.²⁸⁷

²⁷⁷ Duties of United States Attorney, 10 U.S.C.A. § 7656 (2012).

²⁷⁸ Tabarrok, *supra* note 21, at 568.

²⁷⁹ The United States paid the owners of the captured ship \$11,000 in damages. PETRIE, *supra* note 122, at 160.

²⁸⁰ *See, e.g., In re* The Amiable Isabella, Munos, 19 U.S. 1 (1821); The Adeline, 9 Cranch 244 (1815); The Amy Warwick, 67 U.S. 635 (1862).

²⁸¹ Brenner, *supra* note 212.

²⁸² Richard, *supra* note 19, at 455.

²⁸³ In a cyber context, this could include all computers and network capabilities.

²⁸⁴ 48 C.F.R. §§ 9.406–406-05, (2012).

²⁸⁵ *See* The Santissima Trinidad, 20 U.S. 283 (1822) (holding that illegal privateers, whether public or private, “are tortuous—and the original owner is entitled to restitution when brought within our jurisdiction”). Tort liability has real teeth, as government is generally immune from civil suit, whereas a letter of marque holder would not be. *See* David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1186 (1999); Richard, *supra* note 19, at 455.

²⁸⁶ *See supra* Part II.

²⁸⁷ UPTON, *supra* note 57, at 180.

President Lincoln made a similar proclamation regarding privateers hired by the Confederate States, as he did not believe the “rebellious” states had legal authority to issue letters of marque.²⁸⁸

According to some scholars, one of the major drawbacks of the traditional letter of marque system was the lack of organization or unified command, control and communication.²⁸⁹ To address this concern, all cyber letter of marque holders would report their activities and progress to a central authority on a regular and recurring basis.²⁹⁰ This central authority would have the ability to terminate the cyber privateer’s commission and/or refer the matter to the Department of Justice for criminal prosecution, should the commissionee act outside the bounds of authority. As this central authority would have an over-arching view of which cyber privateers were acting in which arenas, they could de-conflict any possible issues of interrupting law enforcement, intelligence, or national security operations in cyber space. Additionally, purely governmental agencies, such as the National Security Agency, would then be in a better position to work in concert with the cyber privateers to execute specific targeted operations.²⁹¹

VI. Conclusion

“More destructive cyber weapons are being created every day . . . [eventually] . . . those who mean to harm the United States will gain the ability to launch a damaging attack. The United States must develop stronger defenses before this occurs.”²⁹² Despite this threat, the U.S. government seems to be content with merely allowing network owners to “[sit] there . . . trying to swat away these intrusions.”²⁹³ Industry

experts have specifically asked that Congress “provide opportunities and responsibilities to the private sector to hack back.”²⁹⁴

Perhaps in tacit acknowledgement that the private sector is better prepared to handle cyber issues, the United States Air Force solicits private industry for capabilities designed to “destroy, deny, degrade, disrupt, deceive, corrupt, or usurp the adversaries [sic] ability to use the cyberspace domain for his advantage.”²⁹⁵

Additionally, the Defense Advanced Research Projects Agency (DAPRA), through its “Plan X,” sought “innovative research proposals” in an effort to “dominate the cyber battle space.”²⁹⁶ Congress has not only denied these requests, while at the same time ignoring the Air Force and DARPA’s proposed use of private industry, but at the same time tied their hands with respect to possible civil and criminal liability.²⁹⁷ Members of Congress have instead suggested legislative mandates requiring “owners and operators of vital infrastructure [to] better protect networks,” or even tax credits as a means of encouraging corporations to establish stricter cyber security safeguards.²⁹⁸ Congress has failed to provide industry with the tools they are desperately asking for: a means in which to protect themselves in a meaningful way.

Political policy makers must understand that “[i]n cyberspace, the offense has the upper hand” and the nation cannot remain secure while hiding behind a mythical all protective firewall.²⁹⁹ Accordingly, Congress should exercise its constitutional authority and authorize the

²⁸⁸ *Id.* at 487.

²⁸⁹ MACLAY, *supra* note 25, at xxiv (discussing privateers running from or surrendering to friendly ships because they believed them to be enemy warships or even firing on friendly ships due to lack of positive identification and communication).

²⁹⁰ Similar cyber threat and intelligence information-gathering authority is vested in the Secretary of Homeland Security. *See* Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

²⁹¹ This cooperation is not without historical precedence. Between 1739 and 1763, privateers worked with the British Navy in capacities ranging from troop transportation to blockading enemy ports. *See* JAMES G. LYDON, PIRATES, PRIVATEERS, AND PROFITS 25, 136, 132 (1970); *but see* Marshall, *supra* note 24 (arguing that privateers were incompetent and responsible for several failures during the Revolutionary War). Marshall dismisses, almost out of hand, the evidence to the contrary discussed by MACLAY, *supra* note 25, at 214–15, and Lobel, *supra* note 25, at 1044.

²⁹² William J. Lynn, III, *The Pentagon’s Cyberstrategy, One Year Later*, FOREIGN AFF. (Sept. 28, 2011), <http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later>.

²⁹³ Matt Egan, *Hack the Hackers? Companies Itching to Go on Cyber Offense*, FOX BUS. (Dec. 7, 2012), <http://www.foxbusiness.com/technology>

2012/12/07/hack-hackers-companies-itching-to-go-on-cyber-offense/#ixzz2EWE5mlfa.

²⁹⁴ *Id.* (quoting testimony of former Homeland Security adviser and Director of George Washington University’s Homeland Security Policy Institute, Frank Cilluffo).

²⁹⁵ U.S. AIR FORCE LIFE CYCLE MGMT. CTR., BAA ESC 12-0011, BROAD AGENCY ANNOUNCEMENT: CYBERSPACE WARFARE OPERATIONS CAPABILITIES (2012), *available at* <http://fbp.gov/utills/view?id=48a4eeb344432c3c87df0594068dc0ce>.

²⁹⁶ DEF. ADVANCED RES. PROJECTS AGENCY, DARPA-BAA-13-02, BROAD AGENCY ANNOUNCEMENT: FOUNDATIONAL CYBERWARFARE (PLAN X) (2012), *available at* https://www.fbo.gov/index?s=opportunity&mode=form&id=1bc45a18e1ba0763640824679d331e46&tab=core&_cview=0.

²⁹⁷ *See supra* Part IV (discussing Computer Fraud and Abuse Act, 18 U.S.C. § 1030(c) (2006), which allows for up to twenty years imprisonment for violations of the law).

²⁹⁸ Chris Strohm, *Tax Breaks Considered to Improve Cybersecurity on Vital Networks*, BUS. WEEK, (Feb. 12, 2012), <http://www.businessweek.com/news/2012-02-14/tax-breaks-considered-to-improve-cybersecurity-on-vital-networks.html>.

²⁹⁹ William J. Lynn III, *Defending a New Domain: The Pentagon’s Cyberstrategy*, FOREIGN AFF., Sept.-Oct. 2010, <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.

issuance of cyber letters of marque and allow American entities to actively defend themselves in cyber space.

As delineated above, the letter of marque has a rich tradition, not only in international and maritime law, but also in American history. Were it not for this power, the United States might not ever have gained her freedom, much less secured it in the War of 1812.³⁰⁰ The United States justly refused to acquiesce to a ban on privateering and that ban is not binding to this day.³⁰¹ As advanced in this article, a cyber letter of marque can, with adequate safeguards in place,³⁰² protect our current infrastructure, obtain information on emerging threats, and then eliminate such threats. Taking into account the current state of the law and

the restrictions that prevent an adequate method of cyber self-defense, it becomes clear that a well thought out cyber letter of marque scheme would be able to address the fears that led to the enactment of the CFAA.

The current legal framework allows hackers to do what they please,³⁰³ while network owners must follow onerous statutory rules.³⁰⁴ The issuance of cyber letters of marque is a constitutionally authorized method of self-defense Congress should authorize to level the cyber playing field.

³⁰⁰ “Historian Faye M. Kert offers the judgment that ‘without the presence of the American privateers in the Revolutionary War and the War of 1812, the United States would never have been able to hold off the British Navy.’” SECHREST, *supra* note 31, at 7.

³⁰¹ See *infra* Part III.

³⁰² This addresses the emotional and intellectually dishonest reactions of “vigilante justice in cyberspace . . . notions of pirates on the high seas and wild west posses” as voiced by people such as Jim Richards of Tangent Capital. Egan, *supra* note 293.

³⁰³ Some complain that to allow active-defense, cyberspace would devolve into a “wild west.” (“Allowing companies an exception to the CFAA really would turn the Internet into the Wild West.”). Westby, *supra* note 147.

It is in many ways the Wild West. Cyberspace has many similarities to a Wild West world . . . The message of this metaphor for cyberspace security is clear: If there is no way to enforce law and order throughout all of cyberspace, which appears to be the case, one must rely on local enclaves of law and order, and trusted friends.

RICHARD O. HUNDLEY & ROBERT H. ANDERSON, EMERGING CHALLENGE SECURITY AND SAFETY IN CYBERSPACE 12, *reprinted from* IEEE TECHNOLOGY AND SOCIETY MAGAZINE (1995/1996). International scholars have also recognized the Wild West nature of the internet. See Richard de Silva, *Cyber Law: Navigating the Legalities of Digital Weapons*, CYBER DEF. & NETWORK SECURITY, Oct. 2012.

³⁰⁴ “‘It’s unfair that hackers can do whatever they want and companies have to follow rules’ said Ronen Kenig, director of security product marketing at Radware.” Egan, *supra* note 293.