University of Cincinnati Law Review

Volume 81 | Issue 2 Article 9

5-30-2013

Taming the Wild Wild Web: Twenty-First Century Prize Law and Privateers as a Solution to Combating Cyber-Attacks

B. Nathaniel Garrett
University of Cincinnati College of Law, garretbr@mail.uc.edu

TAMING THE WILD WILD WEB: TWENTY-FIRST CENTURY PRIZE LAW AND PRIVATEERS AS A SOLUTION TO COMBATING CYBER-ATTACKS

*B. Nathaniel Garrett**

"If you shut down our power grid, maybe we will put a missile down one of your smokestacks."

– Anonymous military official[1]

* Associate Member, 2011–12 *University of Cincinnati Law Review*. Second Lieutenant, United States Air Force Reserve. The views expressed in this Comment are solely those of the author and do not reflect policy or opinions of the United States Air Force, Department of Defense, or any other Department of the U.S. Government.

1. Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War: Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force*, WALL ST. J. (May 30, 2011), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

I. INTRODUCTION

Cyber-warfare just became warfare, so forget the semantics. On May 30, 2011 the United States Department of Defense (DOD) announced that it had adopted a policy in which cyber-attacks could be deemed an act of war meriting a physical military force response.[2] As one military official is reported to have said, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."[3] This policy lays the foundation for modern warfare and provides recognition of the serious destruction that can be caused through the internet. Several high profile incidents of cyber-attacks have brought to the world's attention just how destructive cyber-attacks can be.[4] Recognizing that cyber-attacks can produce serious damage and that its perpetrators continue to become more sophisticated, it is perhaps unsurprising that the United States has adopted this new cyber-warfare policy.

The problem with the United States' new policy is not with its proclamation, but with the implications of the policy. If cyber-attacks constitute warfare, then the United States is currently at war. Worse yet, the United States is losing that war. The United States is attacked daily by cyber-attacks and the military is ill-equipped, in its current form, to protect the nation from cyber-attacks.[5]

As the United States moves into an era where cyber-attacks are no longer strictly "cyber" due to the real life implications of such attacks, novel questions will arise regarding the use of force in response to cyber-attacks. This Comment addresses one specific question that has

2. *Id.*

3. *Id.*

4. *See, e.g.*, Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INTL. L. 192, 193–94 (2009) (discussing the distributed denial of service (DDOS) attack on Estonia in 2007 which crippled banks, media sources and other communications, and led to rioting).

5. *See* Gerald O'Hara, *Cyber-Espionage: A Growing Threat to the American Economy*, 19 COMMLAW CONSPECTUS 241, 243 (2010) ("In the United States, reports of cyber attacks aimed at industrial information surface almost daily, sparing no company, regardless of its size or technological experience."); William Jackson, *U.S. Not Prepared for 'Potentially Devastating' Cyberattacks, House Panel Told*, GOV'T COMPUTER NEWS (Mar. 17, 2011), http://gcn.com/articles/2011/03/17/critical-infrastructure-vulnerable-to-attack.aspx (quoting several government officials who indicate that US is not prepared for potentially devastating cyberattacks); Lisa Daniel, *DOD Needs Industry's Help to Catch Cyber Attacks, Commander Says*, AM. FORCES PRESS SERVICES (Mar. 27, 2012), http://www.defense.gov/news/newsarticle.aspx?id=67713 (US Cyber Commander says military needs private sector cooperation to help catch cyber-attackers).

arisen from the advent of cyber-warfare: how can the United States, through its constitutionally granted authority, prevent and protect against cyber-attacks given the recognized and increasingly dangerous problems that such attacks pose?

The solution examined by this Comment is novel only as applied to the problem of cyber-attacks, because the solution is based on one of the original powers granted to Congress by the Constitution. The solution to the problems posed by cyber-attacks can be found in Article I, Section VIII of the Constitution. It states in relevant part, "The Congress shall have Power To . . . grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water."[6] Letters of marque and reprisal are the legal mechanisms which authorize the use of privateers, whose actions were regulated by a body of law known as prize. The idea of using letters of marque and reprisal to combat cyber-attacks has been suggested and has gained traction among a number of individuals recently.[7]

This Comment will evaluate the idea of using letters of marque and reprisal to allow hackers to serve as modern day privateers assisting the United States in preventing and protecting against cyber-attacks until a point when the U.S. military can successfully protect the country from cyber-attacks. Part II of this Comment provides an overview of privateering and prize law. Part III discusses the problem of cyber-attacks against the United States. Part IV examines the history of U.S. prize law and addresses why recent attempts to revive prize law have failed. Part V argues that prize law could be revived through letters of marque and reprisal to provide a solution to the current problem of cyber-attacks. Part VI addresses the challenges that would need to be solved if a modern day prize law system were implemented. Part VII concludes the Comment.

II. UNDERSTANDING PRIVATEERING AND PRIZE LAW

In order to understand how privateering and prize law could be applied to cyber-attacks, the historical significance of prize law must first be understood. This requires recognition of the environment in which prize law originated. Subpart A examines the ocean as a strategic military environment and how the distinctiveness of the ocean led to its

6. U.S. CONST. art. I, § 8.

7. *See, e.g.*, Steven M. Bellovin, *The Government and Cybersecurity*, 7 IEEE SECURITY & PRIVACY 96 (questioning whether official sponsored cyberattacks were "the latter-day equivalent to letters of marque and reprisal"?); THE MORGAN DOCTRINE, http://www.themorgandoctrine.com/ (last visited Apr. 26, 2013) (a blog supporting the idea of letters of marque and reprisal for internet privateers).

own independent area of law—maritime law. Subpart B then provides an overview of privateering and prize law, which is one specific aspect of maritime law.

A. The Ocean as a Strategic Environment

Our planet's oceans occupy a very unique and often overlooked position in our world.[8] Nearly seventy-one percent of the planet's surface is submerged underneath seawater.[9] The ocean is home to more than a million different species of plants and animals,[10] and is the largest ecosystem on our planet.[11] It is an inherently mysterious environment that has engendered a range of emotions for as long as humans have encountered its vastness.[12]

Aside from its ecological beauty and perplexities, the ocean is also a strategic military environment.[13] Coastal waters are often the main or only route of access to many countries, and the vast majority of world trade is transported by sea.[14] Oceans are an undeniably critical aspect of our global economy. For thousands of years, oceans have been an environment open to exploitation of resources, communication, trade and military power.[15] Oceans provide "unrivaled capacity for delivering a flexible military force to distant locations en masse."[16]

While nearly every piece of land on our planet has been claimed by government control and some rule of law, the ocean has remained a largely lawless frontier.[17] Describing the ocean as a lawless region is not to say that the law has not tried, and succeeded in some cases, to manifest itself there. But the laws that have succeeded in the ocean take into account the unique characteristics of the ocean. The result is

8. *See* WILLIAM LANGEWIESCHE, THE OUTLAW SEA: A WORLD OF FREEDOM, CHAOS, AND CRIME 3 (2004) ("[I]t is easy to forget that our world is an ocean world . . . . Geographically, it is not the exception to our planet, but by far its greatest defining feature.").

9. TREVOR DAY, OCEANS, REVISED EDITION 2 (2008) [hereinafter OCEANS].

10. Alok Jha, *Study Identifies More than 1 Million Ocean Species*, GUARDIAN (Oct. 4, 2012), http://www.guardian.co.uk/environment/2010/oct/04/census-marine-life.

11. OCEANS *supra* note 9, at 117–45 (describing the biology of the oceans and various organisms within its ecosystem).

12. *Id.* at 197.

13. *Id.* at 194.

14. *Id.*; *accord* James G. Stavridis & Richard E. LeBron, *Taming the Outlaw Sea*, 63 Naval War C. Rev. 4, 72–83 (2010). ("The goods of the world move predominantly by sea. Across that broad global commons, trade generally flows freely and well.").

15. OCEANS *supra* note 9, at 272.

16. *Id.* at 194.

17. *See* LANGEWEISCHE, *supra* note 8, at 3 ("[T]he ocean is a realm that remains radically free. Expressing that freedom are more than forty thousand large merchant ships that wonder the world with little or no regulation . . . .").

maritime law.

Maritime law stands apart from the common law of a state, as it applies somewhat different principles and procedures than what is ordinarily applied in both civil and criminal cases.[18] The creation and interpretation of maritime law is complicated by the myriad of operational, administrative, and maintenance issues that the sea poses.[19] Ships on the ocean can be miles away from nearby witnesses, police, or courts.[20] Further, those on the seas themselves are likely from different jurisdictions, and are at a port only for a brief period of time.[21] Historically, when ships were in port, magistrates with special experience in maritime incidents and the common practices of the seas were the proper parties to adjudicate all disputes that arose on the sea.[22]

Even though the rule of law has manifested itself on the oceans, there are still opportunists who seek to capitalize on the strategic nature of the oceans in contravention of the established laws. Notwithstanding maritime law, individuals committing acts of piracy have been able to capitalize on the complexities posed by the oceans.[23] Pirates, such as those that have made news terrorizing ships around the Horn of Africa,[24] are hardly novel problems.[25] They have been around as long as water travel itself. Pirates take advantage of the strategic nature of the ocean and target the vast amounts of resources that are transported through the waterways. In response to piracy and other opportunists on the oceans, prize law—a part of maritime law—grew and flourished.

B. The Basics of Privateering and Prize Law

Subpart A recognizes that the ocean is a distinct environment that resulted in a unique response from the rule of law known as maritime law. This next Subpart will examine one specific area of maritime law.

Included within maritime law is a subset of rules more commonly known as prize law. Prize law governs the capture of property on the

18. *See* GERARD J. MANGONE, UNITED STATES ADMIRALTY LAW 1 (1997).

19. *Id.*

20. *Id.*

21. *See id.* at 1–2.

22. *See id.* at 2.

23. *See* Stavridis & LeBron, *supra* note 14, at 73–74. ("[P]irates are armed opportunists who stem from a permissive and enabling environment formed by a weak state and who engage in a business enterprise subject to risk-and-reward calculations that can be influenced by the international community.").

24. *See* Paulo Prada & Alex Roth, *On the Lawless Seas, It's Not Easy Putting Somali Pirates in the Dock*, WALL ST. J. (Dec. 12, 2008), http://online.wsj.com/article/SB122903542171799663.html.

25. Stavridis & LeBron, *supra* note 14, at 74 ("Piracy is an ancient profession . . . Nautical bandits have plied the waves for nearly as long as people have used the seas for trade.").

seas during times of war.[26] Prize law has largely been relegated to a mere historical aspect of our jurisprudence. At one time, however, as one author writes, prize law was "as familiar to the American populace as the rules of baseball are today."[27] The essence of prize law was that it allowed privateers, or private individuals acting pursuant to governmental commissions, to seize the assets of enemy ships and retain the assets as their legitimate capture.[28]

Privateering first came into practice at the end of the Roman Empire, and was frequently supported by kings in fourteenth century Europe.[29] Privateering is separate and distinct from acts of piracy. While the latter was viewed as illegal and punishable, acts of privateering were explicitly authorized and governed by the rule of law.[30]

Letters of marque and reprisal were the legal authorization that privateers used to carry out what would otherwise be deemed acts of piracy.[31] The letters granted by the government were generally specific in the amount that could be captured and contained an expiration date, after which any capture would be deemed piracy.[32] Once a capture had been committed on the oceans, the privateer was required to bring the captured vessel or cargo into prize courts to be condemned.[33] The privateer would be authorized to retain the amount specified in the letter of marque and reprisal, and the remainder would go to cover other costs.[34]

The first recorded use of letters of marque and reprisal has been traced to an English statute circa 1354.[35] They were used extensively throughout the fifteenth and sixteenth centuries.[36] While letters of

26. *See generally* Joseph Modeste Sweeney, *A Tort Only in Violation of the Law of Nations*, 18 HASTINGS INT'L & COMP. L. REV. 445, 452–62 (1995) (providing an overview of prize law).

27. DONALD A. PETRIE, THE PRIZE GAME: LAWFUL LOOTING ON THE HIGH SEAS IN THE DAYS OF FIGHTING SAIL 2 (1999) [hereinafter PRIZE GAME].

28. *Id.* at 147–63 (summarizing the basic principles of prize law).

29. *See* William Young, *A Check on Faint-Hearted Presidents: Letters of Marque and Reprisal*, 66 WASH. & LEE L. REV. 895, 900 (2009).

30. *See* PRIZE GAME, *supra* note 27, at 69 ("[A] pirate was clearly defined as a person at war with all the world and engaged in criminal depredations at sea against any vessel which could be victimized. Commissioned privateers followed a far different course of action. Their hostilities were directed solely against the declared enemies of the sovereign whose commission they held or, subject to the control of a prize court, neutral vessels carrying troops or cargo in aid of such enemies.").

31. *See* Theodore M. Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 224 (2009).

32. J. Gregory Sidak, *The Quasi War Cases—and their Relevance to Whether "Letters of Marque and Reprisal" Constrain Presidential War Powers*, 28 HARV. J.L. & PUB. POL'Y 465, 473 (2005).

33. *Id.*

34. *Id.*

35. *Id.* at 468.

36. *Id.*

marque and reprisal are often conjoined, originally they were not synonymous.[37] A government issuing a letter of marque authorized seizures outside of the sovereign's local jurisdiction.[38] A letter of reprisal allowed privateers to capture property within the immediate jurisdiction of the sovereign.[39] As both letters were typically sought after by privateers at the same time, the two forms were nearly always referred to together.[40]

In 1856, at the Congress of Paris ending the Crimean War, the seven participating nations signed the Paris Convention of 1856, effectively ending the use of privateers by abolishing the abilities of nations to issue letters of marque and reprisal.[41] While forty-five other nations ultimately joined in the signing of the treaty, the United States was not a signatory.[42] The United States preserved its ability to use letters of marque and reprisal in the future.

Given that the power to issue letters of marque and reprisal was preserved, the question is whether there are any modern day uses for these historic devices. The next Part discusses the problematic rise of cyber-attacks in the United States and subtly argues that the internet is an environment that is ripe for present day prize law.

III. THE PROBLEMATIC RISE OF CYBER-ATTACKS AGAINST THE UNITED STATES

Subpart A begins with an examination of the internet as a strategic military environment, making relevant analogies to the ocean in an effort to draw out the similarities that support the applicability of prize law to the internet. Subpart B then frames the issue of cyber-attacks and piracy on the internet, pointing out the inadequacy of current defense mechanisms.

A. The Internet as a Strategic Environment

The internet was originally developed out of a Department of Defense program.[43] The internet is not located in one physical location; rather, it is the result of "an international network of interconnected computers that allows millions of people to communicate and exchange

37. *See* Young, *supra* note 29, at 900.
38. *Id.*
39. *Id.*
40. *Id.*
41. *See* PRIZE GAME, *supra* note 27, at 141.
42. *Id.*
43. *See* Reno v. ACLU, 521 U.S. 844, 849–53 (1997).

information."[44] The internet has revolutionized the way businesses conduct themselves, the way that humans interact, and the way governments defend themselves.[45] Most of us are sufficiently familiar with the internet that a long background is unnecessary. As one court recognized, "The ubiquitous presence of the Internet and the all-encompassing nature of the information it contains are too obvious to require extensive citation or discussion."[46]

In more than one way, the internet can be analogized to the ocean. Discovery of the ocean completely revolutionized human interaction, commerce, and political interaction just as the internet has again revolutionized these areas today.[47] The internet, just like the ocean, is an undeniably critical aspect of our global economy.[48]

The internet, much like the oceans of the world, is also an arguably lawless environment.[49] Evidence of daily hacker attacks, business data theft, and foreign government intrusions seem to indicate that the internet is nothing but a wild web of loose information interactions where collective disorder rules the day.[50] Governments have tried to impose constraints on internet activity, but it is difficult for any government to impose technological limitations on internet users.[51] Technological constraints, the geographical dispersion of internet users, and the nature of the content on the internet have forestalled the ability of governments to effectively regulate it.[52]

To say that the internet is lawless, similar to the argument that the ocean is lawless,[53] is not to say that the law does not reach the internet.[54]

---

44. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

45. *See* United States v. Peterson, 248 F.3d 79, 83 (2d Cir. 2001) ("Computers and Internet access have become virtually indispensable in the modern world of communications and information gathering.").

46. United States v. Voelker, 489 F.3d 139, 145 (3d Cir. 2007).

47. *Compare infra* Part II(A), *with infra* Part III(A).

48. .S. 1047, 111th Cong. § 2(a) (1st Sess. 2009) ("The Internet is an invaluable tool that is critical to the ability of the Nation to compete in a global economy.").

49. *See* Bruce Braun et al., *Www.commercial_Terrorism.com: A Proposed Federal Criminal Statute Addressing the Solicitation of Commercial Terrorism Through the Internet*, 37 HARV. J. ON LEGIS. 159, 159–60 (2000) ("[A]long with the benefits of increased access to information, ease of communication, and new avenues for commerce have come the problems associated with a largely unregulated environment. In its present infant stage, the Internet resembles the lawless 'Wild West.'").

50. *See* Kevin Coleman, *Cyber Threats Worsen Every Second*, DEFENSE SYSTEMS (Apr. 22, 2010), http://defensesystems.com/articles/2010/04/26/digital-conflict-cyber-defense.aspx ("Cyberattacks have risen to unprecedented levels of sophistication and frequency. The significant number of viruses, worms and other forms of malware, coupled with the dramatic growth of botnets and the continuous rise in the number of cyberattacks, combine to confirm the significance and severity of the problem.").

51. A. Michael Froomkin, *Habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 HARV. L. REV. 749, 779 (2003).

52. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 178–84 (1997).

53. *See* LANGEWEISCHE, *supra* note 8, at 3 ("[T]he ocean is a realm that remains radically free.

On the contrary, the United States has been quick to pass laws regulating interaction and norms on the internet.[55] However, as previously stated, the ocean poses significant problems to regulation.

From a military perspective, the twenty-first century internet suffers from the identical problems as the eighteenth century oceans.[56] The internet is a novel environment, and the U.S. military has not established the dominance in this environment that it enjoys in nearly every other strategic environment (i.e. land, sea, air, space).

Some scholars have cautioned against using metaphors within the law.[57] Justice Benjamin Cardozo once stated, "Metaphors in law are to be narrowly watched, for starting as devices to liberate thought, they end often by enslaving it."[58] The internet–ocean metaphor used in this Comment, however, is narrow, and has been recognized by other scholars, including Professor Tom W. Bell. Professor Bell states:

> [T]he Internet more closely resembles an ocean—an ocean of information. Maritime lawyers in particular should appreciate this metaphor. Like the ocean, the Internet conceals both great beauty and terrible danger. We usually sail (or, appropriately enough, surf) along its surface intent on our particular destinations, unaware of the mysteries that lurk in its depths. While portions of this information ocean fall within the jurisdiction and control of particular States, much of its broad expanse remains wild and free.[59]

For purposes of this Comment, it is sufficient that both the internet and the ocean are strategic military environments to permit an analogy between the two. The DOD has formally recognized the internet as a new domain in warfare that is as critical to military operations as operations on land, or in sea, air, or space.[60] Prior, to the U.S. military

---

Expressing that freedom are more than forty thousand large merchant ships that wonder the world with little or no regulation . . . .").

54. *See* 18 U.S.C. § 1030 (2008). *But see* David R. Johnson & David Post, *Law and Borders-the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (arguing that cyberspace "requires a system of rules quite distinct from the laws that regulate physical, geographically-defined territories").

55. *See, e.g.*, 18 U.S.C. § 1343 (2008); 18 U.S.C. § 1030 (2008) (fraud and related activity in connection with computers).

56. *See infra* Part IV(A) (discussing the lack of military supremacy in the oceans which necessitated prize law, until a point when the US Navy could stand on its own).

57. *See* Jonathan H. Blavin & I. Glenn Cohen, *Gore, Gibson, and Goldsmith: The Evolution of Internet Metaphors in Law and Commentary*, 16 HARV. J.L. & TECH. 265, 267–68 (2002) (discussing the potentially negative consequences such as limiting human understanding reliance on metaphors within the law).

58. Berkey v. Third Ave. Ry. Co., 155 N.E. 58, 61 (N.Y. 1926).

59. Tom W. Bell, *Law and the Information Superhighway*, 28 J. MAR. L. & COM. 185, 186 (1997) (book review).

60. *See* 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.

gaining superiority of the ocean environment through its Navy, it heavily relied on privateers. As the United States currently lacks superiority in the internet environment, perhaps privateers could help once more.

B. Cyber-Attacks on the Internet

While the internet has advanced society in a number of ways, it also has produced an environment ripe for opportunists, more colloquially known as hackers. Hackers are computer users who gain unauthorized access to the computer systems of others.[61] Hackers are essentially modern day pirates; Team Evil,[62] Cold Zero,[63] and other hacker organizations are the modern day Blackbeard and Captain Kidd of our time. These hackers take advantage of the cloak of invisibility that the internet provides for personal or political gain.[64]

The rise of hackers has resulted in countless amounts of stolen credit card information and millions of dollars in losses suffered by banks and fortune 500 companies.[65] Aside from attacks on electronic commerce, hackers have increasingly begun to target the military and other governmental departments.[66]

The United States is being attacked by cyber-attacks on a daily basis.[67] The Department of Justice, the White House, and nearly every other governmental agency or major American company have all felt the effects.[68] As former Director of National Intelligence Michael McConnell has said, "The United States is fighting a cyber-war today,

61. Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 181 (2000).

62. Team Evil is a hacking group that has defaced more than 8,000 websites between June and Nov. 2006, including hacking into sites belonging to banks, hospitals, major companies, non-governmental organizations, and political parties. *See* JEFFREY CARR, INSIDE CYBER WARFARE 22 (2012).

63. Cold Zero, also known as Cold Z3ro or Roma Burner, has claimed responsibility for 5,000 website defacements. *See id.* at 23.

64. *See* Sinrod & Reilly, *supra* note 61, at 182–83. Hackers with a criminal intent are deemed "Crackers." *See id.*

65. *See* Michael Lee et al., *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 844 (1999).

66. *See, e.g.*, Jason Koebler, *U.S. Nukes Face Up to 10 Million Cyber Attacks Daily*, U.S. NEWS & WORLD REP. (Mar. 20, 2012), http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily (US Nuclear Security Enterprise experiences up to 10,000,000 cyber-attacks daily.

67. *See supra* note 5.

68. *See* Pierre Thomas, *Chinese Hack Into U.S. Chamber of Commerce, Authorities Say*, ABC NEWS (Dec. 21, 2011), http://abcnews.go.com/International/chinese-hack-us-chamber-commerce-authorities/story?id=15207642#.T5mZ2lLU7ak (stating that "Chinese [hackers] have attacked every major U.S. company, every government agency, and NGO's.").

and we are losing . . . . [W]e offer the most targets of significance, yet our cyber-defenses are woefully lacking."[69]

As the sophistication of cyber-attacks has grown, the ability of the U.S. government to effectively protect itself is clearly at issue. Even the head of the U.S. Cyber Command and Director of National Security Agency, General Keith B. Alexander has stressed that the United States' current defensive strategy is inadequate.[70]

Undoubtedly, the United States would not tolerate traditional military attacks on U.S. interests or citizens at home or abroad. However, it has become so common on the internet for U.S. interests to be attacked that it has become an accepted norm. What is paradoxical about the cyber domain is that the United States now recognizes cyber-attacks as acts of war, yet continues to tolerate attacks. In no other context would daily attacks on the United States be met with such acceptance or complacency.

The United States is not prepared for cyber-attacks today. According to General Keith, the current defense against cyber-attacks is analogous to a missile being fired into U.S. airspace with no radars to see it.[71] The United States is in a reactionary position with regards to the internet domain. In nearly every other operational domain the United States enjoys a proactive position.[72]

IV. THE U.S. EXPERIENCE WITH PRIVATEERING AND PRIZE LAW

Subpart A examines the constitutional foundation of letters of marque and reprisal and the history of U.S. prize law. Subpart B then theorizes why prior attempts to revive prize law within the United States have failed.

A. Prize Law Within the United States

While today the U.S. Navy has aircraft carriers stationed around the world and nuclear submarines in undisclosed locations capable of launching a nuclear strike in a moment's notice, the journey towards becoming the world's strongest navy has been a long time in the

69. Mike McConnell, *To Win the Cyber-War, Look to the Cold War*, WASH. POST (Feb. 28, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

70. Donna Miles, *Alexander Cites Need for Greater Cyber Defenses*, AM. FORCES PRESS SERVICES (Sept. 13, 2011), http://www.defense.gov/news/newsarticle.aspx?id=65321 (stating that United States had "not yet solved the defensive portion" of cyber-space policy).

71. Lisa Daniel, *DOD Needs Industry's Help to Catch Cyber Attacks, Commander Says*, AM. FORCES PRESS SERVICES (Mar. 27, 2012), http://www.defense.gov/news/newsarticle.aspx?id=67713.

72. *See* MAX BOOT, WAR MADE NEW: WEAPONS, WARRIORS, AND THE MAKING OF THE MODERN WORLD 429 ("Today America is rivaled in land, sea, and air power by . . . no one.").

making.[73] When the American colonies were founded, there was a navy, but it was a far cry from the naval force that the United States currently operates.[74] In response to its lack of naval power, the Continental Congress directed and authorized privateers to fill the void through letters of marque and reprisal.[75]

The framers of the Constitution understood the importance of letters of marque and reprisal, as they had firsthand experience with the necessity of a naval supplement. Arguably, the United States may never have won the American Revolution without the assistance of foreign naval assistance. Recognizing their importance, the framers granted the powers to grant letters of marque and reprisal to Congress in Article I, Section VIII.

Despite having the authority, the United States has not issued a letter of marque and reprisal since the War of 1812.[76] Why has the United States not issued a letter of marque and reprisal since this time? One explanation is that 1812 is around the time that the U.S. Navy burgeoned into a stronger power that was capable of protecting the country and engaging in attacks abroad.[77] So, U.S. privateers essentially filled the void of naval power that the United States lacked, but once the United States was able to strengthen itself to a point of self-sufficiency, privateers were no longer necessary.[78]

With a strong military, the idea of privateers and prize law fell into a relic of the past. Letters of marque and reprisal, the constitutional mechanism that underpinned prize law, were largely unaddressed within American jurisprudence during this time. It was not until around the Vietnam War that interest in the letters of marque and reprisal arose again briefly as scholars examined presidential authority in conducting war.[79]

Letters of marque and reprisal gained the most attention in recent

73. *See generally* CHESTER G. HEARN, NAVY: AN ILLUSTRATED HISTORY: THE U.S. NAVY FROM 1775 TO THE 21ST CENTURY (2007).

74. *See id.* at 10 (stating that long before the established Navy were lightly armed fisher schooners and sloops sailing by commission for US).

75. *See* Cooperstein, *supra* note 31, at 226.

76. C. Kevin Marshall, *Putting Privateers in their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars*, 64 U. CHI. L. REV. 953, 954 (1997).

77. *See* JEROME R. GARITEE, THE REPUBLIC'S PRIVATE NAVY xvii (1977) ("[T]he year 1862 virtually marked the disappearance everywhere of the privately owned and armed warship operating under a government license.").

78. *Id.* at 249 ("Between the Civil War and the Spanish–American War the United States became a major naval power and was no longer dependent on private enterprise for its maritime power.").

79. Young, *supra* note 29, at 897 ("After lying dormant for nearly two centuries, Vietnam War-era scholars, seeking to clarify the constitutional distribution of war powers between Congress and the President, resurrected the Marque and Reprisal Clause of the Constitution."). *See also* Sidak, *supra* note 32, at 465–66.

years when Congressman Ron Paul proposed legislation in early 2000.[80] While the legislation was ultimately rejected in Congress, it did spawn a renewed discussion among some academics and on the internet regarding the idea of Congress issuing letters of marque and reprisal to bring back a form of prize law. As one scholar has written, "As a means to commission private actors to augment national forces in international crises, the Letter of Marque and Reprisal could yet have modern applications. It remains for innovative executive and legislative experiments to revive the ancient practice in a form befitting modern international problems."[81]

B. Why Prior Attempts to Revive Prize Law Have Failed

Following the September 11, 2001 attack on the United States in which al-Qaeda terrorists hijacked four airliners and crashed the planes into both towers of the World Trade Center and the Pentagon, Congressman Ron Paul introduced H.R. 3074, The Air Piracy Reprisal and Capture Act of 2001, and H.R. 3076, The September 11 Marque and Reprisal Act of 2001.[82] Both bills would have authorized letters of marque and reprisal to combat terrorists.[83] Specifically, H.R. 3076 would have given the president the authority to commission "privately armed and equipped persons and entities" to seize the "person and property of Osama bin Laden, of any al Qaeda co-conspirator, and of any conspirator with Osama bin Laden and al Qaeda" who was responsible for the September 11th attack.[84] While Congress ultimately was not persuaded into passing the bill into law, Congressman Paul was successful in reinvigorating the discussion of the contemporary utility of letters of marque and reprisal.

Following Congressman Paul's proposed legislation, several articles were written supporting or examining the expanded use of letters of marque and reprisal. One article argued that letters of marque and reprisal could provide a Congressional tool to accomplish military objectives that the President was unwilling or refusing to support.[85] Another article argued for a revival of letters of marque and reprisal to

80. *See* H.R. 3076, 107th Cong. (1st Sess. 2001); H.R. 3216, 110th Cong. (1st Sess. 2007). Congressman Paul's proposed legislation is discussed in Part IV(B), *infra*.

81. Cooperstein, *supra* note 31, at 221.

82. *See* H.R. 3076, 107th Cong. (1st Sess. 2001). Congressman Paul introduced a similar bill in 2007. H.R. 3216, 110th Cong. (1st Sess. 2007).

83. H.R. 3076, 107th Cong. (1st Sess. 2001). Congressman Paul introduced a similar bill in 2007. H.R. 3216, 110th Cong. (1st Sess. 2007).

84. H.R. 3076, 107th Cong. (1st Sess. 2001).

85. *See* Young, *supra* note 29, at 899.

authorize privateering in armed conflict with non-state belligerents.[86] Congressman Paul also suggested that letters of marque and reprisal could be used to authorize individuals to target Somali pirates.[87] The feasibility of Congressman Paul's Somali pirates idea was again addressed in legal commentary.[88]

Identified within the literature are some of the reasons why letters of marque and reprisal have not been revived. These reasons include that privateers could undermine the U.S. military or undermine foreign relations.[89] These are plausible concerns that have likely contributed to the fact that contemporary letters of marque and reprisal have failed to captivate the majority of Congress. There is, however, another compelling reason that should not be overlooked: the United States has attained a level of military supremacy in all of the domains that these articles (or legislation) have suggested, so the United States has no need for a privateer supplement.[90] The U.S. military supremacy is of such a level that one would have to seriously scrutinize the decision to pass off to individuals such an important role when they would lack the expertise, training, and proper understanding of the ramifications of their actions.

For example, privateers would not have been desirable to hunt for Osama bin Laden. The United States was able to find and kill Osama bin Laden through military action.[91] Put another way, our military did what it was designed to do, which undercuts the need for private individuals competing with the military. If a bounty hunter, authorized through a letter of marque and reprisal, would have attempted the bin Laden mission, they could very well have irreparably damaged United States–Pakistani relationships or killed innocent civilians. Or worse yet, they could have failed.

There is simply no guarantee that private individuals would or should be trusted with such delicate operations, particularly when the international political stakes are so high. While it is true that there is no guarantee that our military could not have also botched the operation, the fact that the U.S. military specifically trains daily for such operations seems support enough to let it continue to do what it is designed to do.

---

86. *See* Robert P. DeWitte, *Let Privateers Marque Terrorism: A Proposal for a Reawakening*, 82 IND. L.J. 131, 132 (2007).

87. Erika Lovley, *Ron Paul's Plan to Fend Off Pirates*, POLITICO (Apr. 15, 2009), http://www.politico.com/news/stories/0409/21245.html.

88. *See generally* Todd Emerson Hutchins, *Structuring a Sustainable Letters of Marque Regime: How Commissioning Privateers Can Defeat the Somali Pirates*, 99 CAL. L. REV. 819 (2011).

89. *See* DeWitte, *supra* note 86, at 149–53.

90. *See supra* note 73.

91. Macon Phillips, *Osama Bin Laden Dead*, WHITE HOUSE BLOG (May 2, 2011), http://www.whitehouse.gov/blog/2011/05/02/osama-bin-laden-dead.

That the operation was executed successfully speaks to the reason why the United States entrusts the military to do this mission, as opposed to private citizens.

Another example related to modern day piracy is illustrative. In April 2009, Somali pirates attempted to seize a U.S. cargo ship that was delivering aid supplies to Africa.[92] The crew was able to fight off the pirates, but not before the pirates managed to abduct the ship's skipper, Richard Phillips.[93] The pirates demanded a ransom from the United States for Phillips, but instead they received a response from a U.S. Navy Seal sniper team.[94]

Of particular interest in this operation was the manner in which the Navy Seal team was able to execute its mission. With a high degree of accuracy, the Seal team was able to eliminate the pirates simultaneously through sniper rounds to the head.[95] It seems doubtful that a private individual (or individuals) having been issued a letter of marque and reprisal, as Congressman Paul suggested, would have reached the same result. U.S. Special Forces are specifically designed for these sorts of capabilities, and they go through extensive training for this objective.[96] Private individuals simply do not match U.S. military capabilities, at least in most regards.

In summary, the problem with prior revivals to prize law was that they argued for a system that would compete with the U.S. military and not provide a useful supplement. While Congressman Paul's idea is an interesting thought, it simply would not be practical or desirable. It is perhaps refreshing, though, to see Congressional leaders considering all available options within their constitutionally granted authority to protect and defend the United States.

Just because letters of marque and reprisal would not work to combat pirates, terrorists, or any other land- or sea-based belligerent does not mean that they would not have some applicability in another context. But, it has to be in a context in which the U.S. military lacks superiority—i.e. in the cyber domain.

---

92. Max Boot, *Pirates, Then and Now: How Piracy Was Defeated in the Past and Can Be Again*, FOREIGN AFFAIRS (July–Aug. 2009), http://www.foreignaffairs.com/articles/65156/max-boot/pirates-then-and-now.

93. *Id.*

94. *See id.*

95. Ann Scott Tyson, *After Brief Countdown, SEALs Fired In Synchrony*, WASH. POST (Apr. 14, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/04/13/AR2009041302694.html ("The snipers' pinpoint accuracy—firing from one moving ship onto the bobbing lifeboat after a split-second decision—was perhaps the main factor in keeping Phillips, 53, alive . . . .").

96. *See id.* ("Becoming a Navy SEAL sniper requires at least five years of experience on a SEAL team. SEALs must pass a marksmanship test, undergo psychological testing and compete for the positions.").

V. MODERN-DAY PRIZE LAW TO TAME THE WILD WILD WEB

The United States' military capabilities for combating cyber-attacks are woefully inadequate. Prime indication of this reality is that the United States is attacked daily without repercussion to the perpetrators.[97] Unless and until the United States can achieve superiority in the internet environment, something must be done. Congress should recognize that prize law has a history of incentivizing private assistance that protected our nation when the military needed a supplement. Before it was on the oceans, but today it can be on the internet. If prize law, authorized through Congress's letters of marque and reprisal power, is to have relevance in contemporary times, then its utility will not be found in fighting Somali pirates or al-Qaeda in Afghanistan, but in filling a particular niche that the United States and its military needs filled *at this time*.

Discussed below are some of the arguments for why twenty-first century prize law could be a solution to the current cyber-attack problem, including: (1) prize law could overcome the current market failure afflicting the U.S. military; (2) the prize law framework lends itself well to the hacking community; (3) specifically tailored letters of marque and reprisal would supplement military needs and reduce vigilantism; and, (4) prize law fits within the U.S. military's cyberspace strategy. Each is discussed in turn.

A. Prize Law Could Overcome the Current Market Failure Afflicting the U.S. Military

There exists a market failure for individuals with specialized computer hacking skills within the U.S. military that has led to the lack of U.S. military cyber-strength. While there are numerous individuals with hacking or other computer-savvy abilities, most of these individuals are not within the U.S. military.[98] The market failure for computer hackers is a result of the fact that computer hacking is largely

97. *See* Scott J. Shackelford, *Estonia Three Years Later: A Progress Report on Combating Cyber Attacks*, 13 J. INTERNET L. 22, 22 (2010) ("Literally thousands of largely unreported major and minor cyber attacks occur daily."); *accord* Commander Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict During A Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1, 1 (2010) ("Cyber attacks against U.S. government systems, critical infrastructure, and private networks are now reported in the media on an almost daily basis.").

98. *See* Eric Beidel & Stew Magnuson, *Government, Military Face Severe Shortage Of Cybersecurity Experts*, NAT'L DEF. (Aug. 2011), http://www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx ("There is an acute shortage of Internet security experts in the government, and no large pool of applicants waiting in the wings to join the fight.").

a back-room sort of affair.[99] Universities have not widely endorsed the behavior, and the law has fostered a disdain towards hackers by not distinguishing between malicious and non-malicious hacking.[100]

An additional contribution to the market failure is that Americans in general perform poorly when it comes to math and sciences,[101] two fields which computer-savvy individuals find important. While the military has sought to expand its base of computer savvy individuals, the effects of the market failure have become so entrenched that it will take time to solve this problem.

It is also quite possible that those who actually possess skills related to computer hacking are ineligible for military service. A 2009 military study found that more than one-third of Americans aged seventeen to twenty-four were unqualified for military service, largely on account of obesity.[102] Setting aside the stereotype of a typical hacker, it is at least likely that someone who is spending the amount of time required to learn how to hack is likely not spending other time engaged in activities such as running or physical fitness, which is a critical component of military readiness.

Fortunately, the U.S. military can start recruiting hackers, and is starting to do so, even if not for enlistment purposes. Many within the hacking community are willing to cooperate with companies and government agencies if monetary rewards and public recognition were offered for their knowledge and skills.[103]

There is already an established cohort of individuals who collectively use their computer hacking skills for specific political or otherwise motivated aims. A group known as "Telecomix, a loose-knit team of international hacktivists, has been scanning" the internet looking to expose companies that use their software or internet-service providing capabilities to censor or survey the internet.[104] Other similar groups are continuing to develop. One blogger has even gone so far as to promote the idea of Congress authorizing letters of marque and reprisal on a

99. *See id.* (stating that the impressive cybersecurity hires for Raytheon, a defense contractor, have not "come from the campus culture" and discussing that some have suggested a four year degree with a more defined career path for hackers).

100. *See* Michael Lee et al., *supra* note 65, at 883 ("Moreover, the sweeping criminalization of all hacking activities has bred within the hacking community a strong distrust and resentment of computer security professionals and government agents.").

101. *See* Bill Clinton, *Priority Issues for the States As Educational Reform Continues*, 1 STAN. L. & POL'Y REV. 5, 6 (1989) ("American scores on science and math exams are still below those of students in other industrialized countries.").

102. William H. McMichael, *Most U.S. Youths Unfit to Serve, Data Show*, ARMY TIMES (Nov. 3, 2009), http://www.armytimes.com/news/2009/11/military_unfityouths_recruiting_110309w/.

103. Michael Lee et al., *supra* note 65, at 883.

104. Andy Greenberg, *Web Vigilantes*, FORBES MAG. (Jan. 3, 2012), http://www.forbes.com/forbes/2012/0116/technology-telecomix-hackers-syria-web-vigilantes.html.

dedicated blog, which includes among other content a proposed doctrine, "The Morgan Doctrine" setting forth a code for cyber privateers.[105] Other blogs and scholars have addressed the idea.[106]

The point is that a small, but significant amount of interest has arisen where hackers would assist in the protection of the United States from cyber-attacks if granted letters of marque and reprisal. Prize law, through market forces, would motivate these hackers to assist the government in its objectives and could thereby help solve the problems of the current market failure afflicting the military.

B. The Prize Law Framework Fits Within the Existing Framework of the Hacking Community

The dichotomy that prize law creates is between illegal piracy and legitimate privateering. Privateers had justification under international law for their actions pursuant to letters of marque and reprisal, while pirates did not.[107] Although distinct, it is quite possible for one to start in the profession as a legitimate privateer and then become a pirate. In 1696, Captain William Kidd did just that.[108]

Captain Kidd had received a letter of marque and reprisal from King William III of England to bring "Pyrates, Free Booters and Sea Rovers to Justice."[109] When he set out with his crew on the ship *Adventure Gallery* he may have had good intentions, but things changed within a few months.[110] Captain Kidd murdered one of his own crewmembers and the *Adventure Gallery* began engaging in piracy by attacking innocent trading ships.[111] Kidd was eventually captured and returned to England where he was tried and hung for his derelictions.[112]

While tales about Kidd and other famous pirates such as Black Bart,

105. *See* THE MORGAN DOCTRINE, http://www.themorgandoctrine.com (last visited Apr. 26, 2013).

106. *See* Susan Brenner, *Marque and Reprisal*, CYB3RCRIM3 (May 18, 2009), http://cyb3rcrim3.blogspot.com/2009/05/marque-and-reprisal.html; *see also* WILLIAM A. OWENS ET AL., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 208 (2009).

107. *See* PRIZE GAME, *supra* note 27, at 69 ("[A] pirate was clearly defined as a person at war with all the world and engaged in criminal depredations at sea against any vessel which could be victimized. Commissioned privateers followed a far different course of action. Their hostilities were directed solely against the declared enemies of the sovereign whose commission they held or, subject to the control of a prize court, neutral vessels carrying troops or cargo in aid of such enemies.").

108. *See* Theodore T. Richard, *Reconsidering the Letter of Marque: Utilizing Private Security Providers against Piracy*, 39 PUB. CONT. L. J. 411, 412 (2010).

109. *Id.*

110. *Id.*

111. *Id.*

112. *See id.*

Calico Jack, and Blackbeard have captivated our attention because of their dramatic lifestyles, there were many who earned an honest living as a privateer.[113] For example, Frenchman Jean Bart was so successful at disrupting Dutch shipping in the late seventeenth century that he was ennobled and given a captain's commission in the French navy.[114] Sir Francis Drake, Sir Walter Raleigh, and Sir John Hawkins all served as English privateers attacking Spanish trading vessels.[115] They were able to raise a formidable amount of wealth and protection by virtue of their roles as privateers sharing their bounty with the English crown.[116]

This dichotomy between pirate and privateer is an analogous to a distinction already found within the hacking community. There are hackers, commonly referred to as "Black Hats," that use their craft on their targets with a malicious intent.[117] For example, a Black Hat hacker is likely to take advantage of a computer break-in by destroying files or stealing data.[118] These Black Hats can be thought of as the pirates of the internet. There are also hackers, commonly referred to as "White Hats" or "Ethical Hackers" who use their powers for good and legitimate ends.[119] White Hats or Ethical Hackers are more likely to locate or repair vulnerabilities in computer networks, spy on behalf of their own country, or catch other hackers for government authorities.[120] These White Hats are the privateers of our internet age.

Just like Captain Kidd, it is conceivable that a White Hat hacker could become a Black Hat hacker. There are solutions proposed later in this Comment in Part VI(C) to address that concern. The point raised here is that the pirate/privateer framework is a lot like the framework that currently exists between Black Hat/White Hat hackers, which suggests the two could fit together easily.

C. Specifically-Tailored Letters of Marque and Reprisal Would Supplement Military Needs and Reduce Vigilantism

As identified earlier in this Comment, there are concerns associated

113. This is not to suggest that even the most lawful privateer was not without moral shortcomings. *See* PRIZE GAME, *supra* note 27, at 69 ("Privateers were not plaster saints but, in most of them, a decent civilized greed outweighed vainglory and blood lust.").

114. *See* Boot, *supra* note 92, at 98.

115. *Id.*

116. *Id.*

117. Susan W. Brenner et. al., *The Trojan Horse Defense in Cybercrime Cases*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1, 23 n.74 (2004).

118. *Id.*

119. *See* Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 172 n.4 (2000).

120. *See id.*

with a government authorizing individuals to carry out land or sea based operations.[121] Aside from the fact that the individual is less likely to be trained for the mission, they could needlessly risk innocent lives or disrupt fragile diplomatic relations that they may not understand or appreciate. Land- or sea-based privateers would compete with the military, rather than be a useful supplement. The concerns identified above are either not present, or greatly diminished, with internet privateers, provided that their letter of marque and reprisal authorization narrowly confines the role of internet privateers.

Prize law, authorized through letters of marque and reprisal, should only be used in two limited scenarios—tracking and defense. Privateers could provide support for tracking the location of hackers and providing evidence that would ultimately lead to the successful prosecution of that hacker by military tribunal or courts. Privateers could also be used to detect and deter incoming attacks by acting in a defensive manner. Outside of these two contexts, the potential for the hacker to do damage likely outweighs their benefit. Privateers with offensive capabilities may not be prudent, as the privateer could damage or disrupt overzealously, or create collateral damage.

Both tracking and defense are the critical areas where cyber-security is lacking. By not authorizing the hackers to engage in hostilities by offensive hacking, their resources can be targeted at the needs of the United States, and likely would not raise any use of force issues under international law, as every nation has the inherent right to self-defense under international law.[122] Furthermore, the limited scope of internet prize law would reduce the opportunity for vigilantism by privateer hackers.

D. Prize Law Fits Within the U.S. Military's Cyberspace Strategy

In July 2011, the DOD released a summary of its strategy for operating within cyberspace.[123] The plan recognized that cyberspace had become "a defining feature of modern life" in which individuals, companies, and the DOD heavily relied upon.[124] The introduction to the strategy acknowledged that "the [DOD] and the nation have vulnerabilities in cyberspace."[125] The strategy plan continued, "[United

121. *See supra* Part IV(B).

122. *See* U.N. Charter art. 51 (recognizing an "inherent right of individual or collective self-defence [sic]").

123. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING WITHIN CYBERSPACE, July 2011, *available at* http://www.defense.gov/news/d20110714cyber.pdf.

124. *Id.* at 1.

125. *Id.*

States'] reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity . . . ."[126] Against this backdrop, the DOD sets forth five strategic initiatives that will allow the United States to "operate effectively in cyberspace, defend national interests, and achieve national security objectives."[127]

"Strategic Initiative 3" is of particular relevance as it states that the "DoD will partner with other U.S. government departments and agencies and *the private sector* to enable a whole-of-government cybersecurity strategy."[128] Strategic Initiative 3 calls for increased use of the private sector.[129] According to the DOD, success will require additional pilot programs, business models, and policy frameworks to foster public–private partnerships.[130] The plan further states, "in some cases, incentives or other measures will be necessary to promote private sector participation."[131] "A collaborative national effort will develop common and workable solutions to policy problems that both increase cybersecurity and further the public good."[132]

There have been two significant events thus far by the DOD that show action in line with Strategic Initiative 3. First, the Defense Advanced Research Projects Agency (DARPA), which commissions advanced research for the DOD, has begun funding hackers to protect against cyber-attacks.[133] Second, General Alexander has testified before Congress in support of legislation that would require private companies to report incoming attacks to the U.S. government before the attack is completed.[134]

While not mentioning privateers or prize law directly, implicitly the military's cyber-warfare strategy indicates that prize law could fit well into the military's plans. The DOD, through DARPA, is already funding hackers to help protect against cyber-attacks. Prize law would essentially be the same sort of program, but on a much greater scale and with explicit Congressional approval.

126. *Id.*

127. *Id.* at 13.

128. *Id.* at 8 (emphasis added).

129. *Id.*

130. *Id.* at 10.

131. *Id.* at 9.

132. *Id.*

133. *See* Spencer Ackerman, *Darpa Begs Hackers: Secure Our Networks, End 'Season of Darkness'*, WIRED (Nov. 7, 2011), http://www.wired.com/dangerroom/2011/11/darpa-hackers-cybersecurity/; *see also* CYBER FAST TRACK, http://www.cft.usma.edu/ (last visited Apr. 26, 2013).

134. Lisa Daniel, *DOD Needs Industry's Help to Catch Cyber Attacks, Commander Says*, AM. FORCES PRESS SERVICES (Mar. 27, 2012), http://www.defense.gov/news/newsarticle.aspx?id=67713.

VI. CHALLENGES ASSOCIATED WITH MODERN-DAY PRIZE LAW USED TO COMBAT CYBER-ATTACKS

There are several surmountable issues that would need to be addressed if Congress revived prize law for hackers to combat cyber-attacks. These issues include: (1) international and domestic reluctance to revive prize law, (2) the lack of readily ascertainable economic incentives, and (3) the practicalities of regulating a prize law system. Each of these issues and some potential responses are discussed in turn.

A. International and Domestic Reluctance to Revive Prize Law

Letters of marque and reprisal and the practice of prize law were abandoned by many nations in 1856.[135] The United States has not issued a letter of marque and reprisal since the War of 1812.[136] Undoubtedly, any revival of the practice of prize law is going to be met with resistance just based on fear of the unknown or a desire to maintain the status quo.

In order to remedy this concern, proponents of reviving prize law could focus on the fact that the U.S. military has sought and utilized private individuals to assist in wartime operations in contemporary times. For example, the U.S. military engagement within Iraq utilized countless private security firms. The most commonly known private security firm was Blackwater, which was the largest of the security firms in Iraq in 2007.[137] So, the U.S. military has engaged privateers in wars since the War of 1812, but has not done so under the auspices of letters of marque and reprisal or prize law. Therefore, a reasonable conclusion is that U.S. officials do not oppose allowing private citizens to engage in some limited form of combat engagement or support.

Blackwater and other firm were engaged by the U.S. military through contracts. Letters of marque and reprisal also operate as contracts. They authorize an individual to act in a manner that is allowed by virtue of the document. It is also a promise that in the event that the privateer is able to accomplish a specific task, like capturing an enemy combatant's ship, the privateer would be entitled to a portion of the capture.

The lack letters of marque and reprisal being used in recent years is a concern. However, given that the military has the capability and has successfully teamed with private individuals in the more recent past, the

135. *See* PRIZE GAME, *supra* note 27, at 141.

136. Marshall, *supra* note 76, at 954.

137. *See* Gable F. Hackman, *Slipping Through the Cracks: Can We Hold Private Security Contractors Accountable for Their Actions Abroad?*, 9 LOY. J. PUB. INT. L. 251, 251 (2008).

resistance to a modern day prize law system on grounds that privateering is no longer an international or domestic practice could be argued to be misplaced.

B. The Lack of Readily Ascertainable Economic Incentives

Privateers of the past were incentivized by the ability to keep a share of the "prize" of their capture. They had clear economic advantages to carry out their voyages on the seas. Prize law was a business. If Congress were to revive prize law for hackers, the question would arise: what economic incentives would hackers receive for preventing cyber-attacks? Put another way: what would be the hacker's bounty?

There are several potential solutions to this problem. There would be inherent value to the material that these hackers could gain access to. It is recognized that information has inherent value that could be sold to others for value.[138] Despite the fact that such material is intangible, it still could be resold or be of value to someone else. This solution is not desirable, however, because it would create a secondary market for state secrets, critical military targets, or other confidential information.

Perhaps the best solution for modern day prize law would be Congressional funding. Cash bounties provided by the U.S. government to encourage hackers to make patriotic use of their skills would provide an incentive. Furthermore, the bounty would decrease the chances of a secondary market being created for the information.

Congressman Paul's letter of marque and reprisal bill would have authorized Congress to expend funds from the $40 billion set aside by the Emergency Supplemental Appropriations Act in order to provide a bounty for Osama bin Laden or members of al-Qaeda.[139] Congress could apportion funds from the treasury to fund modern day letters of marque and reprisal. Funding from Congress is already used to finance hackers to protect against cyber-attacks in the "Cyber Fast Track" program.[140]

C. The Practicalities of Regulating Modern-Day Prize Law

One of the hallmarks defining prize law was specific courts with admiralty jurisdiction that specialized in capture cases. These courts

138. Commissioner Pamela Jones Harbour, Remarks Before FTC Exploring Privacy Roundtable (Dec. 7, 2009), *available at* http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf ("Data is currency. The larger the data set, the greater potential for analysis—and profit.").

139. *See* September 11 Marque and Reprisal Act of 2001, H.R. 3076, 107th Cong. (1st Sess. 2001).

140. *See* CYBER FAST TRACK, *supra* note 133.

made privateering a legitimate business endeavor. A privateer would not have been able to sell the spoils of his prize legally, if it was not adjudicated that the privateer had ownership. If prize law were to be adopted in modern times, there would have to be some regulation of the practice.

The first line of regulation would be with the actual letter of marque and reprisal itself. The drafting of this letter would require specific authorization to particular parties and for a particular amount of time. However, just as a contract would have little value if parties could not adjudicate the terms through a court in the event of a dispute, letters of marque and reprisal would have little value if privateers could not ensure a proper adjudication to reward them for their work in preventing or detecting a cyber-attack.

It would seem to follow that prize law courts or some other monitoring body would be required in the system. Disputes are likely to arise as to the scope of the letter itself. Once a hacker has acted, there may be a temptation to go further than what was authorized. Worse yet, there is the potential for the hacker to engage in malicious conduct. Just as Captain Kidd set out lawfully under a letter of marque and reprisal before turning to piracy, it is quite possible that an Ethical Hacker would set out lawfully and then switch to being a Black Hat. Already, there is a third group of hackers, aptly named "Grey Hats" whose actions and moral conduct lie somewhere in between those of the White and Black Hats. These hackers possess a powerful set of skills, but their conduct has to be watched just like any other profession with power.

Specialty courts have been utilized in a number of different contexts, such as the U.S. Foreign Intelligence Surveillance Act (FISA) Courts, Bankruptcy Courts, and Tax Courts, among others.[141] Given the complexities involved in computer hacking and the confidential nature of the information targeted, a special court with jurisdiction over the prize law system makes sense. Indeed, a successful prize law system needs court access or regulation of some kind.

VII. CONCLUSION

The United States is currently failing to protect its citizens and interests on the internet, but this Comment provides a viable solution to this problem. Unless and until the U.S. military maintains domain control over the internet as a strategic environment in the way that it maintains control over the land, air, and oceans of the world, Congress

141. *See* 50 U.S.C. § 1803 (2012) (FISA courts); 28 U.S.C. § 1334(a) (2010) (bankruptcy courts); 26 U.S.C. § 7441 (2012) (tax courts).

should evaluate all constitutionally granted authority within its control to protect and defend the United States.

The use of privateers is not a novel idea, and they have been utilized in the most recent military operations carried out by the U.S. military. Although not explicitly labeled privateers and prize law, the practice has long been around, and is currently practiced to this day.

Like the (nonexistent) capabilities of the U.S. Navy in the 1700s, the U.S. military's ability to engage in cyber-warfare is virtually nonexistent. Congress had the foresight back in those days to recognize the shortcomings of its Navy, and turned to privateers to fill the void. Today, Congress should recognize that the U.S. military is not adequately equipped for the perils of the internet. The warning signs are ubiquitous, with daily cyber-attacks and public announcements from key government officials in the cyber-warfare field.

Strategic partnerships with individual citizens are one solution that has both constitutional and historical support. However, prize law is likely just a short-term solution to the broader problems associated with the internet and the future of war-fighting. Even if the United States were to implement a prize law system, it should move quickly to strengthen its military to be a stand-alone fighter in the cyber domain. Additionally, international support must be garnered. It will not be enough for the United States to act alone. One of the hallmarks of the prize law systems of the sixteenth and seventeenth centuries was that a great majority of the international powers had bought into the idea. Because the internet spans nearly every geographical jurisdiction, collective solutions are required.