THE ARMY LAWYER

Headquarters, Department of the Army

August 2013

ARTICLES

TJAGLCS FEATURES

Lore of the Corps

New Developments

Administrative & Civil Law

BOOK REVIEWS

CLE NEWS

CURRENT MATERIALS OF INTERESTS

Department of the Army Pamphlet 27-50-483

Editor, Captain Marcia Reyes Steward
Assistant Editor, Captain Laura A. O'Donnell
Assistant Editor, Major Keirsten H. Kennedy
Technical Editor, Charles J. Strong

The Army Lawyer (ISSN 0364-1287, USPS 490-330) is published monthly by The Judge Advocate General's Legal Center and School, Charlottesville, Virginia, for the official use of Army lawyers in the performance of their legal responsibilities. Individual paid subscriptions to *The Army Lawyer* are available for $45.00 each ($63.00 foreign) per year, periodical postage paid at Charlottesville, Virginia, and additional mailing offices (see subscription form on the inside back cover). POSTMASTER: Send any address changes to The Judge Advocate General's Legal Center and School, 600 Massie Road, ATTN: ALCS-ADA-P, Charlottesville, Virginia 22903-1781. The opinions expressed by the authors in the articles do not necessarily reflect the view of The Judge Advocate General or the Department of the Army. Masculine or feminine pronouns appearing in this pamphlet refer to both genders unless the context indicates another use.

The Editor and Assistant Editor thank the Adjunct Editors for their invaluable assistance. The Board of Adjunct Editors consists of highly qualified Reserve officers selected for their demonstrated academic excellence and legal research and writing skills. Prospective candidates may send Microsoft Word versions of their resumes, detailing relevant experience, to the Technical Editor at TJAGLCS-Tech-Editor@conus.army.mil.

The Editorial Board of *The Army Lawyer* includes the Chair, Administrative and Civil Law Department; and the Director, Professional Writing Program. The Editorial Board evaluates all material submitted for publication, the decisions of which are subject to final approval by the Dean, The Judge Advocate General's School, U.S. Army.

The Army Lawyer accepts articles that are useful and informative to Army lawyers. This includes any subset of Army lawyers, from new legal assistance attorneys to staff judge advocates and military judges. *The Army Lawyer* strives to cover topics that come up recurrently and are of interest to the Army JAG Corps. Prospective authors should search recent issues of *The Army Lawyer* to see if their topics have been covered recently.

Authors should revise their own writing before submitting it for publication, to ensure both accuracy and readability. The style guidance in paragraph 1-36 of Army Regulation 25-50, *Preparing and Managing Correspondence*, is extremely helpful. Good writing for *The Army Lawyer* is concise, organized, and right to the point. It favors short sentences over long and active voice over passive. The proper length of an article for *The Army Lawyer* is "long enough to get the information across to the reader, and not one page longer."

Other useful guidance may be found in Strunk and White, *The Elements of Style*, and the Texas Law Review, *Manual on Usage & Style*. Authors should follow *The Bluebook: A Uniform System of Citation* (19th ed. 2010) and the *Military Citation Guide* (TJAGLCS, 18th ed. 2013). No compensation can be paid for articles.

The Army Lawyer articles are indexed in the *Index to Legal Periodicals*, the *Current Law Index*, the *Legal Resources Index*, and the *Index to U.S. Government Periodicals*. *The Army Lawyer* is also available in the Judge Advocate General's Corps electronic reference library and can be accessed on the World Wide Web by registered users at http://www.jagcnet.army.mil/ArmyLawyer and at the Library of Congress website at http://www.loc.gov/rr/frd/MilitaryLaw/Army_Lawyer.html.

Address changes for official channels distribution: Provide changes to the Editor, *The Army Lawyer*, The Judge Advocate General's Legal Center and School, 600 Massie Road, ATTN: ALCS-ADA-P, Charlottesville, Virginia 22903-1781, telephone 1-800-552-3978 (press 1 and extension 3396) or electronic mail to usarmy.pentagon.hqda-tjaglcs.list.tjaglcs-tech-editor.

Articles may be cited as: [author's name], [article title], ARMY LAW., [date], at [first page of article], [pincite].

Lore of the Corps

Articles

TJAGLCS Features

New Developments

Administrative & Civil Law

Book Reviews

The Cease-Fire on the Korean Peninsula: The Story of the Judge Advocate Who Drafted the Armistice Agreement that Ended the Korean War

Fred L. Borch
Regimental Historian & Archivist

Sixty years ago this year, on 27 July 1953, an armistice agreement ended the fighting between United Nations (UN) forces and Chinese and North Korean armies on the Korean peninsula. This armistice, or cease-fire agreement, had been drafted the year before by forty-four-year old Lieutenant Colonel (LTC) Howard S. Levie, a career judge advocate (JA) assigned to the UN Command Armistice Delegation. What follows is the story of how, while "dozens of voices . . . harangued more than nine months in trying to reach an armistice in Korea," the pact itself was "written mostly by one man."[1]

The Korean War started on 25 June 1950 when about 10,000 North Korean People's Army (NPKA) soldiers, supported by artillery, aircraft and tanks, crossed the 38th parallel into the Republic of Korea (ROK). While the ROK army was about the same size as the NPKA, its soldiers lacked combat experience. As a result, ROK resistance collapsed quickly and Seoul, the ROK capital, fell to the Communists on the third day of fighting.[2]

Under a UN Security Council Resolution, however, American air, naval and ground units joined the battle.[3] After General Douglas MacArthur's brilliant amphibious landings at Inchon, UN forces (now including Australian, British, Dutch, Turkish and many other UN member states) drove into North Korea, capturing the North Korean capital, Pyongyang, in October. By the end of 1950, however, Chinese Red Army troops had entered the war and, joining forces with the NPKA, drove the UN forces out of North Korea; the enemy re-captured Seoul. The Eighth U.S. Army, first commanded by Lieutenant General Matthew B. Ridgway and then by Lieutenant General James Van Fleet, pushed back against the Communists. Badly hurt by losses in both men and materiel, the Chinese and North Koreans suggested peace talks on 23 June 1951, and the UN accepted.[4]

In July 1951, then LTC Levie was serving in General MacArthur's Far East Command in Tokyo. A Cornell law school graduate who had transferred from the Coast Artillery Corps to The Judge Advocate General's Department in 1946, Levie had been the Chief, War Crimes Division, since September 1950. In this position, he supervised the review of records of trial in which a death sentence had been adjudged against a Japanese accused. One day, while reviewing a trial record, LTC Levie was informed that he was to report the following day to the UN Command Armistice Delegation, and that he would serve as a "Monitor" on the Delegation Working Group. His superiors—involved in the actual negotiations—included four Americans: Vice Admiral C. Turner Joy; Major General Henry I. Hodes; Rear Admiral Arleigh A. Burke; Major General Laurence C. Craigie; and one ROK officer, Major General Paik Sun Yup.[5]

Negotiations opened on 10 July 1951 in Panmunjom and when Levie arrived there, he learned that while the Communist and UN delegations would approve the principles to be contained in the truce agreement, it was going to be his job—as the only lawyer—to draft proposed provisions for the implementation of those principles. The result was that, over a nine-month period, while dozens of individuals argued about the principles to be contained in the cease-fire, Levie drafted the actual language for those provisions suggested by the UN Command.

After LTC Levie drafted each specific provision, he would "have an in-house review and discussion by the delegation and staff."[6] After any changes or modifications were agreed upon, the proposed Armistice provisions were "sent to Washington [D.C.] for approval."[7] After approval, the provisions were translated into Chinese and Korean. As Levie remembered,

> in the beginning, it was thought that each side would draft the specific provisions; rarely did we receive a draft proposal from

[1] *Dozens Argue at Panmunjom, But One Man is Writing Pact*, EVENING STAR (Wash., D.C.), Apr. 14, 1952, at A7.

[2] CENTER OF MILITARY HISTORY, U.S. ARMY, KOREA—1950, at 9–10, 14 (1997).

[3] S.C. Res. 82, U.N. SCOR, U.N. Doc. S/RES/82 (June 25, 1950). The resolution passed because the Soviet Union's representative was boycotting that organization; had he been present, he could have vetoed the resolution.

[4] JOHN MILLER, JR., OWEN J. CARROLL & MARGARET E. TACKLEY, KOREA 1951–1953, at 3–10, 115–17 (1997).

[5] *Id.* at 115, 160.

[6] Written Questions for Colonel Levie (n.d.) (*The Army News Service* provided a list of questions for Colonel Howard S. Levie to answer in order to publish a story about him in *The Army News Service* in December 2008.) (on file with Regimental Historian).

[7] *Id.*

> the Communists. We quickly learned that no matter how perfect the translation of a proposal would be, the Communists would never accept it without demanding some change or changes; changes that were frequently completely meaningless. We then adopted the practice of deliberately inserting a few more or less obvious errors. The Communists would insist on correcting those errors and would otherwise accept the document.[8]

This drafting job was without precedent, as no JA had previously been tasked with authoring a truce agreement. Lieutenant Colonel Levie, however, was familiar with the 1936 cease-fire agreement between Bolivia and Paraguay, and he borrowed paragraphs from this agreement for the Korean armistice.[9] He also looked at "other armistice agreements of modern times on the paragraphs dealing with a demilitarized zone."[10]

By April 1952, LTC Levie's armistice agreement had "been overhauled seven times" and was "26 legal size typewritten pages containing 63 paragraphs, many with subparagraphs."[11] Provisions in the document covered a variety of purely military topics, including the creation of a military demarcation line and demilitarized zone, the establishment of a military armistice commission, and specific details governing the implementation of the cease fire. When negotiations stalled over the issue of repatriating prisoners of war (POWs),[12] the original members of the delegation and staff departed Panmunjom in May 1952. Lieutenant Colonel Levie left the following month but his precise, clear, grammatically correct agreement remained in place. Consequently, when negotiations resumed the following year—with an agreement on POW exchanges—what both sides signed on 27 July 1953 essentially was what Levie had written.[13] It was a remarkable achievement by any measure. At the time, no one realized that this truce document would be so important, since there was every reason to believe that the parties subsequently would sign a formal peace treaty ending the Korean War. But this has never occurred and, as a result, Levie's agreement—which required both sides to withdraw two kilometers from the truce line to establish a Demilitarized Zone—is what maintains a sometimes uneasy peace today.[14]

As for LTC Levie? After leaving Korea in July 1952, he returned to Japan until the following year when he departed for the United States. After briefly serving as the Staff Judge Advocate (SJA), Fort Leavenworth, Kansas, LTC Levie was transferred to the Pentagon, where he served as the first chief of the newly created International Affairs Division (IAD) in the Office of The Judge Advocate General. Promoted to colonel shortly after becoming the head of IAD, Levie remained in the Pentagon until 1958, when he was transferred to Europe. He served first as the SJA, Southern European Task Force, and subsequently as the Legal Advisor, U.S. European Command. After retiring in 1963, COL Levie began a second—and extraordinarily successful—career as professor of international law at St. Louis University and at the Naval War College.[15]

---

[8] *Id.*

[9] From 1932 to 1935, Bolivia and Paraguay fought a territorial war over the Gran Chaco region, an area over which both countries claimed ownership. At least 90,000 to 100,000 men died, and total casualties may have exceeded 250,000. For more on the Chaco War, which ended with a truce in January 1936, see A. DE QUESADA, THE CHACO WAR 1932–1935: SOUTH AMERICA'S GREATEST CONFLICT (2011).

[10] *Supra* note 1.

[11] *Id.*

[12] The UN Command insisted on "voluntary repatriation"—insisting that every POW had the right to make a personal, voluntary decision to return to the country in whose armed forces he had been serving at the time of his capture. The Communists, however, were adamant that all Chinese and North Korean POWs must be returned to their control, regardless of their personal desires. Howard S. Levie, *How It All Started—And How It Ended: A Legal Study of the Korean War*, 35 AKRON L. REV. 205, 223 (2002).

[13] The 27 July 1953 Armistice Agreement was signed by Lieutenant General William K. Harrison, Jr., Senior Delegate, UN Command Delegation and General Nam Il, Senior Delegate, Korean People's Army and Chinese People's Volunteers. For the full text of the Korean War Armistice Agreement, see http://news.findlaw.com/cnn/docs/ korea/kwarmagr072753. html (last visited Aug. 15, 2013).

[14] In the late 1990s, there were attempts to convene a conference in Geneva in order to negotiate a final peace treaty but nothing was achieved. Levie, *supra* note 10, at 225. In fact, starting in 1996, North Korea has announced its withdrawal from the Armistice Agreement on at least six occasions. *Chronology of Major North Korean Statements on the Korean War Armistice*, YONHAP NEWS, May 28, 2009, *available at* http://english.yonhapnews.co.kr/northkorea/2009/05/28/46/0401000000AEN20090528004200315F.HTML.

[15] Richard J. Grunawalt, *Professor Howard Levie and the Law of War*, *in* MICHAEL N. SCHMITT & LESLIE C. GREEN (EDS.), LEVIE ON THE LAW OF WAR, at xv (1998), *available at* https://www.usnwc.edu/getattachment/f70ec02c-8f8e-4f54-aa15-3c71030c6231/Professor-Howard-Levie-and-the-Law-of-War.aspx.

Howard Levie's many writings on the Law of Armed Conflict—he wrote seven books and more than fifty articles and edited thirteen volumes—continue to be used by international legal scholars. The Corps recognized his many contributions when it made him a Distinguished Member of the Regiment in 1995. But COL Levie has yet another unique place in our history: he is the first and only member of the Corps to reach the 'century' mark, and he later celebrated his 101st birthday on 19 December 2008. Levie died at his home in Rhode Island the following year.[16]

More historical information can be found at

The Judge Advocate General's Corps
Regimental History Website

Dedicated to the brave men and women who have served our Corps with honor, dedication, and distinction.

https://www.jagcnet.army.mil/History

[16] Elizabeth M. Collins, *Armistice Author Turns 101*, ARMY NEWS SERV., Dec. 29, 2008.

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 alone[2]; 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 websites[4] 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 dysfunctional[11] 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 allies[14] 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.fco.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.busninessweek.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.scientificamerican.com/article.cfm?id=auto-immune-symbiotes-could-be-deployed-to-thwart-cyber-attacks.

historically effective and constitutional[17] 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/word-press.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 marque[27] 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 or marque authorized private merchant ships to carry arms in self-defense.[34]

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

[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.

[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]

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

---

[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.'").

[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. 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 navy[76] 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

[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.

[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 marque[84] 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 objection[102] 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]

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]

---

[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-11e2-9940-6fc488f3fecd_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=; 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 Fontevecchia, *Standard Chartered Hid 60,000 Transactions With Iranian Banks Worth $250B*, FORBES (Aug. 6, 2012 12:38 PM), http://www.forbes.com/sites/afontevecchia/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 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 Unites 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 stream[126] 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

[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.

[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 he[128] planned to attack 30 Unites 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 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

[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 vorKzakone is unknown, he is believed to be a male, as shown by alleged photographs of vorKzakone online.KREBSONSECURITY.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 Perlroth & 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.*

[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, 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

[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.

[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 laws[163] 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 sufficiently "mainstream" in the United States that industry trade associations[169] 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 individual[171] 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 marque is the antiquated CFAA prohibition.

Indeed, other scholars have posited the use of bounty hunting letters of marque.[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 marque. 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 marque.[173] However, this concern in a cyber letter of marque 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 marque 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 marque

Wanted, *available at* FED. BUREAU 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).

[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 expanded[180] to include civil liability by prohibiting anyone from "intentionally access[ing] a protected computer without authorization or exceed[ing] authorized access . . . [and recklessly causing damage[181] involving a loss[182] of] at least $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 CFAA[189] 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

---

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).

[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.

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 target[201] 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 over-blown.[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

[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-forbescso/ (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.

[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 argue[219] 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 ban[223] 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-Crime[231]

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 to[244]: 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]

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 agency[257] 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

[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.

[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 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]

---

[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-72255 9; 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.

[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-wikileaks-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 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]

securitylaw.us/2012/11/30/steven-chabinsky-crowdstrike-ex-fbi-cyber-division-talks-pprivate-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. W*hether 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).

[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/#ixzzz2EWE5mlfa.

[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/utils/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 Neworks*, 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.

When Did Imminent Stop Meaning Immediate?
Jus In Bello Hostile Intent, Imminence, and Self-Defense in Counterinsurgency

Major Eric D. Montalvo[*]

The application of the principles of psychology in small wars is quite different from their normal application in major warfare or even troop leadership. The aim is not to develop a belligerent spirit in our men but rather one of caution and steadiness. Instead of employing force, one strives to accomplish the purpose by diplomacy. A Force Commander who gains his objective in a small war without firing a shot has attained far greater success than one who resorted to the use of arms.[1]

I. Introduction

Notwithstanding the recipe for success detailed in the quotation above, the United States military has been involved in counterinsurgency (COIN) operations in Iraq and Afghanistan for more than ten years.[2] With the end of major operations in Iraq, and the impending 2014 withdrawal deadline for Afghanistan, it is time for both military and civilian leadership to analyze the lessons learned from those conflicts and integrate them into training methods for U.S. forces going forward. This type of critical analysis is important because Marine Corps and Army doctrine states, and many commentators agree, that COIN will be the prevailing operating environment for the foreseeable future.[3] Within this context, it is important to identify operational law-related doctrine and practice that COIN has frustrated. One such area is the Rules of Engagement (ROE),[4] specifically the Chairman of the Joint Chiefs of Staff Standing Rules of Engagement (SROE) regarding self-defense.[5] Department of Defense (DoD), Joint Publication 1-02, *Dictionary of Military and Associated Terms (JP 1-02)*, defines ROE as "directives issued by competent military authority that delineate the circumstances and limitations under which U.S. forces will initiate and/or continue combat engagement with other forces encountered."[6] Specific to the SROE, the Chairman stated that it "establishes fundamental policies and procedures governing the actions to be taken by U.S. commanders and their forces during all military operations . . . occurring outside U.S. territories."[7]

Rules of Engagement are magnified in COIN operations because the nature of COIN warfare is much different from the type of conventional warfare that served as the impetus for the Geneva Conventions.[8] Many COIN principles are counterintuitive to military leaders, and require an alternative tactical mindset. These differences present what the *Counterinsurgency* field manual calls paradoxes for U.S. servicemembers trained on the conventional use of force. The field manual lists nine paradoxes that distinguish COIN from conventional operations, and four of those paradoxes are specifically applicable to the use of force in self-defense: (1) Sometimes, the more you protect your force, the less secure you may be; (2) Sometimes, the more force is used, the less effective it is; (3) Sometimes doing nothing is the best reaction; and (4) Some of the best weapons for counterinsurgency do not shoot.[9] For the traditionally trained warfighter, these concepts require additional reinforcement to make the mindset of restrained force second nature before deploying to a COIN environment.

Compounding the problem of differences in tactics between a conventional and COIN fight, the enemy in a

---

[*] Judge Advocate, U. S. Marine Corps. Presently assigned as the Staff Judge Advocate, 22d Marine Expeditionary Unit, II Marine Expeditionary Force, Camp Lejeune, North Carolina.

[1] U.S. MARINE CORPS, SMALL WARS MANUAL para. 1-10d (1940).

[2] Nat'l Def. Res. Inst., *Preface to How is Deployment to Iraq and Afghanistan Affecting U.S. Service Members and Their Families*, at iii (James Hosek ed., 2011).

[3] *See* U.S. DEP'T OF ARMY, FIELD MANUAL 3-24, COUNTERINSURGENCY para. 1-8 (15 Dec. 2006) [hereinafter FM 3-24] (concluding that "[t]he recent success of U.S. military forces in major combat operations undoubtedly will lead many future opponents to pursue asymmetric approaches"); Commander Albert S. Janin, *Engaging Civilian Belligerents Leads to Self-Defense/Protocol I Marriage*, ARMY LAW., July 2007, at 82, 83 (recognizing that "[t]he lethal problem of civilian-belligerents is now the customary trend in warfare rather than the exception to the rule").

[4] *See* GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 127, 193 (2012) (stating that "ROE have become a key issue in modern warfare and a key component of mission planning for U.S. and many other armed forces" and "self-defense . . . is a significant purpose of the ROE and accounts for much of the force applied in current military operations"); Major Winston S. Williams, *Training the Rules of Engagement for the Counterinsurgency Fight*, ARMY LAW., Jan. 2012, at 42 (finding that U.S. Armed Forces have struggled with achieving the goals of counterinsurgency while not undermining the right to self-defense").

[5] CHAIRMAN OF THE JOINT CHIEFS OF STAFF, INSTR. 3121.01B, STANDING RULES OF ENGAGEMENT/STANDING RULES FOR THE USE OF FORCE FOR U.S. FORCES app. A (13 June 2005) [hereinafter CJCSI SROE 3121.01B].

[6] JOINT CHIEFS OF STAFF, JOINT PUB. 1–02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 270 (15 Aug. 2012) [hereinafter JP 1–02].

[7] INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., U.S. ARMY, JA422, OPERATIONAL LAW HANDBOOK 84 (2012) [hereinafter OPLAW HANDBOOK].

[8] *See* Trevor A. Keck, *Not All Civilians are Created Equal: The Principle of Distinction, the Questions of Direct Participation in Hostilities and Evolving Restraints on the Use of Force in Warfare*, 211 MIL. L. REV.115 (2012) ("Warfare is fundamentally different today than in 1949 when states convened to draft and sign the four Geneva Conventions.").

[9] FM 3-24, *supra* note 3, para. 1-148–53.

COIN environment does not comply with the Law of Armed Conflict (LOAC) principle of distinction. This allows the insurgent to blend in with the civilian population, operate more freely within the battlespace, and use U.S. adherence to LOAC against American servicemembers.[10] In addition, the expanding presence of the media within military operations has further scrutinized self-defense SROE in the eyes of the American public, commonly characterizing it as ineffective and limiting the ability of servicemembers to defend themselves.[11] The above factors lead to a situation in which self-defense ROE comes under the microscope by servicemembers, political leadership, and the public writ large. This scrutiny places an increased burden on military leadership to ensure that self-defense ROE is effective, clear, and continually trained in order to mitigate or avoid potential problems.

Prolonged COIN operations in Iraq and Afghanistan have distorted the U.S. view of anticipatory self-defense, hostile intent, and imminence as they relate to the use of force in a COIN environment, and have negatively shaped the use of force in self-defense, creating greater accompanying risks. More specifically, the expansion of what U.S. forces consider an imminent threat does not comport with the United States' coalition partners, and has frustrated the application of the common self-defense formula (hostile act or hostile intent + positive identification = authority to use force).[12] The result has been (1) an increased risk of civilian casualties and (2) a self-defense targeting model that in practice looks more like status-based targeting vice the conduct-based model required in COIN. These problems can be mitigated if the SROE's definitions of hostile intent and imminence return to the form that existed prior to the 2005 SROE.[13] This shift would require commanders and judge advocates to apply a narrower concept of imminence, defined later in this article. In addition, servicemembers must apply the self-defense formula correctly by first establishing an individual's hostile intent before obtaining positive identification (PID) of a legitimate military target.

Part II of this article illustrates some of the inherent problems in applying a broad definition of imminence. This analysis calls for a brief review of the historical support for and development of the inherent right to self-defense, the influence of the Bush Doctrine on the concept of imminence, and the codification of anticipatory self-defense in the SROE through the concept of hostile intent. Part II then summarizes the main points of status- and conduct-based targeting, and discusses how those concepts relate to the commonly taught self-defense formula. Next, Part III argues that returning to a narrower definition of imminence and correctly applying the self-defense formula will mitigate the three problems identified in this article. The article concludes with recommendations as to how commanders and judge advocates can shape ROE philosophy, training,

[10] *See* OPLAW HANDBOOK, note 7, at 21 (declaring that insurgents "deliberately and illegally use the civilian population . . . to conduct or conceal their attacks as a strategy of war"); GARY D. SOLIS, THE LAW OF ARMED CONFLICT (2010) (stating that terrorists in Iraq and Afghanistan do not comply with (LOAC) principle of distinction, making hostile intent and hostile act the only methods to differentiate between combatants and non-combatants); CORN ET AL., *supra* note 4, at 132–33 ("Exercising [distinction] is increasingly difficult on the asymmetric battlefield. No longer are wars fought on battlefields far from concentrations of civilians . . . [t]he soldier is faced with combatants masquerading as civilians, in order to take advantage of the humanity of the warrior, to use the law as a shield of protection against attack."); Sarah Sewall, *Introduction* to FM 3-24, *supra* note 3, at xxi, xxvii ("[Counterinsurgency (COIN)] is more difficult because insurgents exploit civilians by dress in civilian clothes, hide behind women, use children as spotters, and store weapons in school and hospitals."); Keck, *supra* note 10, at 115 (finding that "states primarily fight wars against non-state armed groups (NASG) that often violate IHL, and more specifically the principle of distinction. Blending in with noncombatants is often a critical part of the NASG's strategy in places such as Afghanistan"); Janin, *supra* note 3, at 83 (finding that in today's insurgencies the "combatants appear to be civilians and base their operations amongst non-combatants").

[11] *See* Major Mark S. Martins, *Rules of Engagement for Land Forces: A Matter of Training, Not Lawyering*, 143 MIL. L. REV. 3, 35 (1994) (finding that "an aggressive and skeptical news media has emerged, willing to question the use of military force . . . and prepared to focus the wrath of the American people on a political leader who appears to have lost control"). *See, e.g.*, Sara A. Carter, *Marine's Career Threatened by Controversial Rules of Engagement*, WASH. EXAM'R (Jan. 23, 2012), http://washingtonexaminer.com/marines-career-threatened-by-controversial-rules-of-engagement/article/167369#.UGec0EJOTdk (reporting on an incident involving the use of force in self-defense the reporter stated that some experts believed the Marine involved was placed "in a difficult, if not impossible, situation by unreasonable rules of engagement foisted upon the military by politically sensitive commanders in the Pentagon," and the Marine's lawyer asserts that he is "just one of hundreds of cases of troops who have suffered under stringent rules of engagement"); Jason Motlagh, *Petraeus Toughens Afghan Rules of Engagement*, TIME (Aug. 6, 2010) http://www.time.com/time/world/article/0,8599,2008863,00.html (responding to General Patraeus's revision of the tactical directive in 2010, the reporter stated that "servicemen say that the strict rules put them in greater danger, even as they aim to avoid civilian casualties"); Kim Murphy, *Officer Advises Against Court-Martial in Afghanistan Shooting Death*, LA TIMES (Aug. 3, 2012), http://www.afghanistannnewscenter.com/news/2012/august/aug32012.html#a13 (reporting on a shooting incident that involved the death of an Afghan physician the reporter classified the rules of engagement as "strict . . . in attempting to minimize civilian casualties." In addition, she summarized some soldiers' comments about "rules of engagement that make it increasingly difficult for soldiers to defend themselves"); Paul Szoldra, *Marine: Strict Rules of Engagement Are Killing More Americans Than Enemy in This Lost War*, BUS INSIDER (Aug. 24, 2012) http://www.businessinsider.com/one-marines-views-on-afghanistan-2012-8 (A former Marine officer states that the rules of engagement result in servicemembers fighting with "their hands tied behind their back" due to the restrictive nature of the rules of engagement and that "enemy fighters use our rules of engagement and restrictions . . . against us.").

[12] A search of all relevant manuals, orders, directives, regulations, doctrinal publications, and training manuals reveals no official adoption of this self-defense formula. However, based on personal experience of both receiving and providing instruction on self-defense Rules of Engagement (ROE), and after interviewing judge advocates from other services, it is the author's conclusion that this formula is widely employed as a teaching tool by U.S. forces. The best implied reference to this self-defense formula can be found in Gary Solis's book, THE LAW OF ARMED CONFLICT, *supra* note 10, at 502, where he states that most "ROE . . . contain other common elements addressing hostile acts, enemy hostile intent . . . and a positive identification requirement." *Id.*

[13] The Appendix to this article provides the SROE definition for hostile intent and imminence for all SROEs dating back to 1981.

and employment within the unit to ultimately better support the COIN mission.

II. Laying the Foundation

As it relates to this article, it is important to first frame the problem[14] created by an expanded view of imminence when determining if an individual or group is demonstrating hostile intent. Once the reader understands the parameters of the problem, he might then consider how the inherent right to self-defense, the Bush Doctrine, and the CJCS's definition of hostile intent and imminence have all served to further develop the issue, and can relate those developments to status-and conduct-based targeting, as well as the self-defense formula.

A. Framing the Problem

1. Imminent No Longer Requires an Immediate or Instantaneous Threat

The current SROE defines hostile intent as "[t]he threat of imminent use of force against the United States, U.S. forces or other designated persons or property. It also includes the threat of force to preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital USG property."[15] The SROE attempts to further clarify the phrase "imminent use of force" by providing that "[t]he determination of whether the use of force against U.S. forces is imminent will be based on an assessment of all facts and circumstances known to U.S. forces at the time and may be made at any level. *Imminent does not necessarily mean immediate or instantaneous.*"[16] The SROE successfully provides a definition that can be taught in classrooms and recited in a deployed setting; however, there is no further explanation to help Marines and Soldiers apply it in a fast-paced combat environment. Combined with certain aggravating factors inherent in COIN operations, the SROE's definition creates more problems than it attempts to solve. One very real problem facing U.S. forces is the risk of civilian casualties.

2. The Ultimate Problem in COIN: Civilian Casualties

A primary contributor to the civilian casualty problem is the difficulty in assessing hostile intent within a fast-paced combat environment using the SROE's limited explanation of imminence.[17] Compounding the time and space problem, the SROE's definition of imminent use of force does not comport with our U.S. coalition and NATO partners,[18] making it more difficult to justify some U.S. actions. Overall, the ambiguous standards of hostile intent and imminence, and the resulting broad application by U.S. forces, lead to problems at the tactical and strategic level. However, these issues can be mitigated, and in some cases eliminated, if commanders and judge advocates take deliberate actions to continually reinforce a narrow view of hostile intent and imminence within self-defense ROE.

How U.S. forces view the concepts of hostile intent and imminence within anticipatory self-defense is pivotal because it informs the actual employment of force. In a COIN environment, a narrow view of hostile intent and imminence results in a more restrained use of force, a stated goal in COIN. On the other hand, a broad application of hostile intent and imminence gives a servicemember greater authority to engage perceived threats, which increases the risk of civilian casualties. Recognizing that the civilian population is the center of gravity[19] in COIN operations,[20]

---

[14] The first step in the Marine Corps planning process is to frame the problem the staff or operational planning team will address. Once accomplished, there is common understanding of what foundational information will be required to conduct meaningful analysis and propose a well-supported decision. U.S. MARINE CORPS, MARINE CORPS WARFIGHTING PUB. 5-1, MARINE CORPS PLANNING PROCESS 2-1 (Aug. 24, 2010).

[15] CJCSI SROE 3121.01B, *supra* note 5, at A-3.

[16] *Id*. (emphasis added).

[17] *See* CORN ET AL., *supra* note 4, at 193 (concluding that the concept of hostile intent is "difficult to put into practice"); YORAM DINSTEIN, WAR AGGRESSION AND SELF-DEFENCE 205 (5th ed. 2011) (finding that there the term imminence "may mean different things to different people" and that "[t]here is no authoritative definition of imminence in the context of an armed attack"); SOLIS, *supra* note 10, at 506 (declaring that a "bright-line" cannot exists for determining hostile intent); Lieutenant Colonel Mark S. Martins, *Deadly Force is Authorized, But Also Trained*, ARMY LAW., Oct. 2001, 1, at 5 (stating that concept of hostile intent is difficult to define "require[ing] elaboration and further definition . . ."); Major John J. Merriam, *Natural Law and Self-Defense*, 206 MIL. L. REV. 43, 64 (2010) (quoting John Yoo as stating that "international law does not supply a precise or detailed definition of what it means for a threat to be sufficiently imminent to justify the use of force in self-defense as necessary").

[18] *See* SOLIS, *supra* note 10, at 506 (stating that America's aggressive stance on hostile intent embodied in the U.S. SROE is not shared by many countries); Janin, *supra* note 3, at 93 (recognizing that the British operate under ROE that are "not as aggressive as, the U.S. SROE, with respect to hostile intent); Merriam, *supra* note 19, at 78–80 (finding that the U.S. SROE on anticipatory self-defense are "dramatically different" than the NATO equivalents and the British were unwilling to follow the United States after if revised the definition of imminence in the 2005 SROE); David A. Sadoff, *A Question of Determinacy: The Legal Status of Anticipatory Self-Defense*, 40 GEO. J. INT'L L. 523 (2009) (placing the United Stated in a small group of States, which includes Israel, that subscribes to an expansive view of anticipatory self-defense); Lieutenant Colonel W. A. Stafford, *How to Keep Military Personnel from Going to Jail for Doing the Right Thing*, ARMY LAW., Nov. 2000, 1, at 5–6 (stating that differing views on what constitutes hostile intent and imminence leads other countries to view our actions as excessive).

[19] JP 1–02, *supra* note 6, at 39 (defining center of gravity as "[t]he source of power that provides moral or physical strength, freedom of action, or will to act").

[20] FM 3-24, *supra* note 3, para. 3-76.

civilian casualties become a real problem when imminence is applied in an overly broad manner.[21] The prevention of civilian casualties is such an important issue in a COIN fight that even Mullah Omar, the recognized leader of the Taliban in Afghanistan, issued guidance to his fighters to limit the indiscriminate use of force.[22]

3. Status-Based Targeting in a Conduct-Based Environment

An important factor that has influenced the application of anticipatory self-defense is the length of time U.S. forces have been involved in COIN operations in Iraq and Afghanistan. The last ten years have marked the longest sustained period U.S. ground forces have been involved in COIN-centric operations.[23] This prolonged exposure to an environment filled with uncertainty has made servicemembers hyper-vigilant, leading to the engagement of targets that do not meet the definition of hostile intent under the SROE.[24] The result of this practice is movement toward a targeting model that looks more like status-based targeting vice conduct-based targeting. Stated another way, servicemembers are engaging targets in self-defense based on physical characteristics and a perceived threat, not on the individual's conduct. This leads to the unintentional killing of civilians because, for example, they meet the description of a military-aged-male, or MAM.[25] Further aggravating the problem, improper engagements are justified after the fact by commanders and judge advocates under an expanded self-defense model in an attempt to "protect" the individual Marine or Soldier. While the above is best classified as a mind-set problem in how Marines and Soldiers process information on the battlefield, it further increases the risk of civilian casualties when put into practice.

B. Inherent Right of Self-Defense, the Bush Doctrine, and the Chairman of the Joint Chiefs of Staff Definition of Hostile Intent

1. Development of Individual Self-Defense

Any meaningful discussion of anticipatory self-defense and imminence must involve an understanding of their historical development as concepts within customary international law, and then as policy within U.S. SROE. While there is some disagreement among scholars, it is a commonly held belief that self-defense derives from natural law and "is as old as history and has long been founded on the simple notion that every rational being . . . must conclude that it is permissible to defend himself when his life is threatened with imminent danger."[26] The origins of self-defense date back to Roman jurists who believed a natural law existed "that was universal and derived from reason."[27] While Roman society was one of the first to address natural law self-defense principles, it was Saint Thomas Aquinas's *Summa Theological* that framed self-defense as a concept rooted within a moral code that was "not derived but rather self-evident."[28] With the development of self-defense in natural law, the next historical step was a connection between theoretical belief and application to individual or State action.

Hugo Grotius, a Dutch jurist and student of Aquinas's early work, furthered the concept of self-defense in his book "*De Jure Belli ac Pacis*, which earned him the title of the 'father of international law,'" because he began applying the concept of self-defense to the "nation-state and internal order organized around it."[29] Although absent from Aquinas's writings, Grotius specifically addressed the concepts of anticipatory self-defense and the accompanying immanency requirement:

[21] Martins, *supra* note 11, at 4 (stating that a danger of not properly training Marines and Soldiers in ROE can lead to an overly aggressive use of force that could harm civilians.); Merriam, *supra* note 17, at 82 (2010) (arguing that an "expanded standard if imminence" may increase the chance for the mistaken killing of civilians).

[22] Katharine Fortin, *Mullah Omar Urges The Taliban to Avoid Civilian Deaths*, ARMED GROUPS & INT'L L. BLOG (Aug. 21, 2012) http://armedgroups-internationallaw.org/2012/08/21/mullah-omar-urges-the-taliban-to-avoid-civilian-deaths-a-cause-to-celebrate/ (quoting Mullah Omar's decree directed towards other Taliban fighters to "employ tactics that do not cause harm to life and property of the common countrymen. The instructions given to you for the protection of civilian losses are, on you, a religious obligation to observe.").

[23] INST. OF MED., RETURNING HOME FROM IRAQ AND AFGHANISTAN 17 (2010) (finding that OIF and OEF are the "longest sustained U.S. military operation").

[24] *See* SMALL WARS MANUAL, *supra* note 1, at 1-16b ("Uncertainty of the situation and the future creates a certain psychological doubt or fear in the minds of the individual concerned . . . ."); e-mail from Colonel Eric M. Smith, Dir., Capabilities Development Directorate, Marine Corps Combat Dev. Command & former Commanding Officer, Regimental Combat Team 8, Afghanistan (Nov. 26, 2012) [hereinafter Colonel Smith e-mail] (on file with author) (responding to a question about the effect of prolonged COIN operations, he explained that "[t]he wars in Iraq and Afghanistan have heavily influenced the current military view of hostile intent and imminent threat. For the main, the impact is negative.").

[25] The term military-aged-male, or MAM, was both formally and informally used in Iraq as a means of identifying potential insurgent(s) or threats to U.S. forces. This term was eliminated from the military vernacular because it was applied too broadly by servicemembers, which led to unnecessary detentions and the unsupportable use of deadly force.

[26] Merriam, *supra* note 17, at 44–46. *Contra* DINSTEIN, *supra* note 17, at 191 (asserting that referencing natural law as the source of the right to self-defense, while "common in popular publications and even in some official pronouncements—is unwarranted").

[27] *Id*. at 48.

[28] *Id*. at 49.

[29] *Id*. at 54 (quoting EDWARD DUMBAULD, THE LIFE AND LEGAL WRITINGS OF HUGO GROTIUS 59 (1969)).

> When our lives are threatened with immediate danger, it is lawful to kill the aggressor . . . [however] the danger must be immediate, which is one necessary point. Though it must be confessed, that when an assailant seizes any weapon with an apparent intention to kill me I have a right to anticipate and prevent the danger. For in the moral as well as the natural system of things, there is no point without some breadth.[30]

Fast-forwarding more than 200 years, the concept of anticipatory self-defense was again at the forefront of international law in the famous Caroline Case. The Caroline Case involved the British burning and sinking of a U.S.-flagged ship suspected of providing personnel and arms to Canadian rebels.[31] In a series of letters between Daniel Webster, the U.S. Secretary of State, and the British government, Webster "asserted that the right to self-defense does not exist unless one can show a *necessity of self-defense, instant, overwhelming, leaving no choice of means, and no moment for deliberation*."[32] This statement by Secretary Webster is widely held to be the "modern formulation of the right to anticipatory self-defense in international law."[33] It also serves as the primary basis for the concept of hostile intent and imminence within U.S. doctrine and policy. However, while the Caroline Case provided a theoretical standard for the right to anticipatory self-defense, the principles articulated by Secretary Webster were not immediately operationalized. This issue was remedied by the development of ROE.

2. Rules of Engagement and the Chairman's Standing Rules of Engagement

Rules of Engagement are "intended to give operational and tactical military leaders greater control over the execution of combat operations."[34] It is important to recognize that ROE are "not LOAC or International Humanitarian Law, nor are they mentioned in the Geneva Conventions or Additional Protocols. They are also not domestic law. They are military directives."[35] Many considerations inform ROE development, including customary international law, treaty obligations, domestic law, and policy in order to provide Marines and Soldiers with a framework on the use of force in combat operations and military operations other than war.[36] Recognizing that ROE can come in varying forms within the chain-of-command, U.S. forces are issued common baseline ROE through the SROE.

As compared to the history of U.S. involvement in armed conflict, the regulation of the use of force through SROE is a relatively new concept.[37] The first SROE-like document was the *Worldwide Peacetime ROE for Seaborne Forces*, published in 1981, which focused on a naval ship's ability to fire a first strike against foreign flagged vessels.[38] As the SROE concept continued to develop, military leadership realized that ground forces needed their own specific guidance on the use of force in self-defense.[39] While the title and substance of the SROE has changed since 1981, a constant was the continued restatement of the inherent right to self-defense.[40] In addition, also dating back to the 1981 SROE was the authority to use deadly force against a person or group demonstrating hostile intent.[41] In defining hostile intent the 1981, 1986, 1994, and 2000 SROEs all required an imminent threat of force, with no further explanation or definition.[42] However, relevant to this article is the additional definition of imminence found in the current 2005 SROE eliminating the requirement for an imminent threat to be immediate, which was based on a concurrent change in national self-defense policy.

---

[30] *Id*. at 56–57 (quoting HUGO GROTIUS, DE JURE BELLI AC PACIS 76–77 (1625)).

[31] *Id*. at 59.

[32] *Id*. at 60 (emphasis added).

[33] *Id*. at 59.

[34] CORN ET AL., *supra* note 4, at 126.

[35] SOLIS, *supra* note 10, at 490.

[36] *See id.* at 498 ("SROE apply in common Article 2 and common Article 3 conflicts and in peace-keeping mission, and anti-terrorist mission. They also apply in military operations other than war."); Janin, *supra* note 3, at 91 (Rules of Engagement "coordinate political, military, and legal purposes and . . . ensure law of war compliance").

[37] W. Hays Parks, *Deadly Force Is Authorized*, U.S. NAVAL INST. PROC. 32 (Jan. 2001) (stating that "rules of engagement have been with us for some time, [but,] their formulation is recent").

[38] *Id*. at 33.

[39] *See* SOLIS, *supra* note 10, at 491–94. After a full review of use of force incidents in Vietnam there was a recognition by military leadership that there needed to be a specific ground force ROE, therefore, the JCS issues ROE for ground forces in 1988 designated the Peacetime ROE. The next revision of the ROE came in 1994 and was formerly designated by the JCS as the Standing ROE. Since 1994, there have been two additional revisions of the SROE with publishing in 2000 and 2005. *Id.*

[40] The author, in conjunction with a researcher from the Pentagon Library, Information Management Division, conducted a review of the SROE directives from 1981 to the present and found a statement in all five documents that declared a right to self-defense.

[41] The author, in conjunction with the a researcher from the Pentagon Library, Information Management Division, conducted a review of the SROE directives from 1981 to the present and found all documents contained the concept of hostile intent.

[42] The author, in conjunction with the a researcher from the Pentagon Library, Information Management Division, conducted a review of the SROE directives from 1981 to the present and found that they all contained a definition of hostile intent that required a threat of the imminent use of force.

3. The Bush Doctrine's Influence on the Standing Rules of Engagement

A primary source for determining the national policy on self-defense is the National Security Strategy (NSS). Under federal law, the President is responsible for submitting his NSS to Congress, which, among other things, must describe "the . . . national defense capabilities of the United States necessary to deter aggression and to implement the national security strategy of the United States."[43] While not specifically addressed in every NSS, world events have required the president to explain the nation's policy on the use of force in self-defense. Dating back to 1950, at the beginning stages of the Cold War, President Truman issued National Council Report 68 (NSC-68),[44] which asserted America's anticipatory self-defense policy of not striking first "unless it is demonstrably in the nature of a counter-attack to a blow . . . *about to be delivered*."[45] A more expansive view of anticipatory self-defense was promulgated by President Bush in his 2002 NSS after the terrorist attacks on September 11th.[46] The "Bush Doctrine" took a clear stance on the use of force in response to anticipated developing threats:

> For centuries, international law recognized that nations need not suffer an attack before they can lawfully take action to defend themselves against forces that present an imminent danger of attack. Legal scholars and international jurists often conditioned the legitimacy of preemption on the existence of an imminent threat . . . [w]e must adapt the concept of imminent threat to the capabilities and objectives of today's adversaries . . . . The greater the threat, the greater the risk of inaction—and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack.[47]

Prior to President Bush's 2002 NSS, the 2000 SROE defined hostile intent as "the threat of imminent use of force against . . . U.S. forces . . . ."[48] There was no further definition of imminence. However, after President Bush promulgated his 2002 NSS, the SROE was revised and included a definition of imminence that did not require an immediate or instantaneous theat.[49] It is important to recognize that President Bush's statement in the 2002 NSS was referencing the use of force in a *jus ad bellum* context—"the law dealing with . . . how States initiate armed conflict"[50]—however, the expansion of imminence and national anticipatory self-defense by the President had a direct influence on the changing definition of imminence and hostile intent in the 2005 SROE, [51] which are *jus in bello* policies—the "law governing the conduct, [or means and methods,] of hostilities."[52] Stated another way, the flexibility President Bush needed to defend the nation against developing asymmetrical threats bled over to the individual Marine and Soldier making real-time self-defense targeting decisions in a COIN environment. This leads to the question: What type of targeting model are U.S. servicemembers employing under an expanded view of imminence and anticipatory self-defense in a COIN environment? While it should be conduct-based targeting, it may, in practice, look more like status-based targeting, which is impermissible within a self-defense context and contrary to U.S. and international law.

C. Status- versus Conduct-Based Targeting and the Self-Defense Formula

Every decision to use force is based upon either a status- or conduct-based targeting model. The established process within which targeting decisions are made will differ from one theatre or unit to another,[53] but a commander's decision to use force, at its core, is based on a potential target's status

[43] 50 U.S.C. § 404a (2012).

[44] THE EXECUTIVE SEC'Y ON UNITED STATES OBJECTIVES AND PROGRAMS FOR NAT'L SECURITY, NSC 68, A REPORT TO THE NATIONAL SECURITY COUNCIL (14 Apr. 1950) (this document was previously classified Top Secret, but was declassified on 27 February 1975), *available at* http://www.trumanlibrary.org/whistlestop/study_collections/coldwar/documents/pdf/10-1.pdf (This document was previously classified Top Secret, but was declassified on 27 February 1975.).

[45] *Id*. at 53 (emphasis added).

[46] Sadoff, *supra* note 18, at 560–61.

[47] THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 15 (Sept. 17, 2002) [hereinafter NSS 2002].

[48] CHAIRMAN OF THE JOINT CHIEFS OF STAFF, INSTR. 3121.01A, STANDING RULES OF ENGAGEMENT FOR U.S. FORCES encl. A (15 Jan 2000).

[49] *Supra* note 16.

[50] INT'L & OPERATIONAL LAW DEP'T, THE JUDGE ADVOCATE GEN.'S LEGAL CTR. & SCH., U.S. ARMY, JA 422, LAW OF ARMED CONFLICT DESKBOOK 10 (2012) [hereinafter LOAC DESKBOOK].

[51] *See* Janin, *supra* note 3, at 90 (asserting that "the law governing the use of force in self-defense is a macrocosm of the choices to be made at the tactical level of warfare"); Merriam, *supra* note 17, at 80 (finding that the expansion of imminence and anticipatory self-defense in President's Bush's 2002 NSS is reflected in the 2005 SROE revised definition of imminence with respect to hostile intent); Sadoff, *supra* note 18, at 561 (stating that a nation's application of anticipatory self-defense may influence that same nation's ROE).

[52] LOAC DESKBOOK, *supra* note 50, at 135.

[53] *See* SOLIS, *supra* note 10, at 530 (recognizing that "military forces employ strict protocols in making targeting decisions . . . [which] improve and mature, change to meet conflict circumstances, and seldom remain static for long").

or conduct.[54] Article 4 of the Third Geneva Convention[55] and Article 51 of the Additional Protocol 1 to the Geneva Conventions[56] do not use the formal terms of status- and conduct-based targeting, but both serve to codify customary international law relating to these two targeting methods.

1. The Basics of Status-Based Targeting

Status-based targeting is the use of force against (1) an individual serving in a nation's armed force, (2) a member of an organized armed group, or (3) a declared hostile force.[57] Commonly, members of a nation's armed force are classified as combatants,[58] while members of an organized armed group are comprised of non-state actors classified as either unprivileged belligerents or unlawful combatants.[59] Article 4 of the Third Geneva Convention provides the framework definitions for individuals categorized as combatants.[60] Specifically, Article 4(A)(1), (2), (3), and (6) classify as combatants those individuals who are members of an armed force, militia, volunteer corps, or spontaneous organized resistance.[61] The SROE also addresses status-based targeting within the context of a declared hostile force.[62] The current 2005 SROE defines a declared hostile force as "any civilian, paramilitary or military force or terrorist(s) that has been declared hostile by appropriate U.S. authority."[63] The authority referenced in the SROE remains at "the National Command Authority, the Joint Chiefs of Staff, or regional command"[64] levels, and once declared hostile, an individual or group can be attacked anywhere they are found without having to commit a hostile act or demonstrate hostile intent.[65] However, it is important to recognize that even if a commander is conducting status-based targeting he must first obtain positive identification (PID) of the target before engaging,[66] and in many instances the basis of PID is the target's conduct.

2. Conduct-Based Targeting and Self-Defense in Counterinsurgency

Conduct-based targeting is the use of force against individuals engaged in activities deemed hostile by the servicemember observing the conduct.[67] This targeting method is recognized in Article 51(3) of Additional Protocol I, which permits the targeting of noncombatants, otherwise known as civilians, "for such time as they take a direct part in hostilities."[68] While the definitions of "for such time" and "direct participation" are widely debated within the international community,[69] an exact definition is not necessary. The significant principle within Article 51(3) is that an individual's conduct can make them a legitimate military target.

Like Article 51(3), the SROE also recognizes the concept of conduct-based targeting through its self-defense

---

[54] While the concepts of status- and conduct-based targeting applies to the use of force against individuals and inanimate objects (buildings, bridges, etc.), this article focuses exclusively on the targeting of individuals.

[55] Geneva Convention Relative to the Treatment of Prisoners of War, art. 4, Aug. 12, 1949, 6 U.S.T 3114, 75 U.N.T.S. 31 [hereinafter GC III].

[56] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), annex I, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

[57] *See* LOAC DESKBOOK, *supra* note 520, at 138.

[58] *See* CORN ET AL., *supra* note 4, at 165 (stating that combatants are those individuals described in Article 4(A)(1), (2), (3), and (6) of the Third Geneva Convention and that combatant status is granted exclusively by the State).

[59] *Id.* at 170 (stating that "modern armed conflict is driving a reevaluation of the idea and even the ICRC seems to recognize the need to make special allowances for organized armed groups that are taking a part in hostilities as structured participants").

[60] *See id.* at 165.

[61] GC III, *supra* note 55, art. 4(A) (categorizing as combatants those individuals that are

> (1) members of the armed force of a Party to the conflict; (2) members of other militias and member of other volunteer corps . . . belonging to a Party to the conflict and operating in or outside their own territory . . . provided that such militias or volunteer corps . . . fulfill the following conditions: (a) commanded by a person responsible for his subordinates, (b) [have] a fixed distinct sign recognizable from a distance, (c) carry arms openly, (d) conduct their operations in accordance with the laws and customs of war; (3) members of regular armed forces who profess allegiance to a government or an authority no recognized as the Detaining Power . . . [and] (6) inhabitants of a non-occupied territory, who on approach of the enemy spontaneously take up arms to resists the invading force.

Id.

[62] *See* LOAC DESKBOOK, *supra* note 520, at 138.

[63] CJCSI SROE 3121.01B, *supra* note 5, para. 3d.

[64] *See* SOLIS, *supra* note10, at 597.

[65] CJCSI SROE 3121.01B, *supra* note 5, para. 2b (stating that "[o]nce a force is declared hostile by appropriate authority, U.S. units need not observe hostile act or demonstration of hostile intent before engaging that force"). *See* CORN ET AL., *supra* note 4, at 165 (stating that combatants are "targetable anywhere and anytime").

[66] *See* SOLIS, *supra* note 10, at 508 (finding that friendly forced must first positively identify a target's status before engaging with deadly force).

[67] LOAC DESKBOOK, *supra* note 520, at 138.

[68] AP I, *supra* note 56, art. 51(3).

[69] While outside the scope of this article, see LOAC DESKBOOK, *supra* note 50, at 20–21, for a further discussion of the direct participation in hostilities debate.

policies and accompanying concepts of hostile act and hostile intent.[70] As stated in the SROE, "[u]nit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstration of hostile intent."[71] Targeting decisions shift when employing force in self-defense because "immediate firing on the opposing force or individual is permitted because of the opponent's *conduct*, rather than his *status*."[72]

When operating in a COIN environment, Marines and Soldiers almost exclusively employ a conduct-based targeting model when deciding whether to use deadly force.[73] As discussed earlier in this article, the center of gravity in a COIN environment is the civilian population; however, as a deliberate tactic, insurgent fighters violate the principle of distinction in order to disguise themselves as noncombatants. This presents an obvious identification problem for U.S. forces. Even if the appropriate authority declared insurgent forces hostile, shifting U.S. forces to a status-based targeting model, the only method to PID an insurgent who does not wear an identifiable uniform is to observe his conduct. [74] As a result "[t]he practical and legal constraints of PID make status-based engagements very rare . . . [placing] U.S. armed forces in a reactive posture"[75] based on the conduct they observe. Recognizing the necessity to employ a conduct-based targeting model in COIN operations, Marines and Soldiers require a practical, useful framework to process their observations and determine if deadly force is authorized.

The self-defense formula—hostile act or demonstrated hostile intent plus positive identification of the enemy permits the use of deadly force (HA/HI + PID = Use of Force)—is the framework used by Marines and Soldiers to make conduct-based self-defense decisions.[76] Separating the two elements of the equation, the presence of a hostile act and/or hostile intent satisfies the military necessity principle of LOAC, and the requirement to have PID of the enemy satisfies the distinction principle under LOAC.

While the SROE defines both hostile act and hostile intent for the servicemember, it fails to provide an operational definition for PID.[77] Joint Publication 1-02 defines PID as "identification derived from observation and analysis of target characteristics including visual recognition, electronic support systems, non-cooperative target recognition techniques, identification friend or foe systems, or other physics-based identification techniques."[78] As is evident from an initial reading, this definition is not useful for the individual Marine or Soldier patrolling the streets of Iraq and Afghanistan. With references to electronic support systems and physics-based identification techniques in the Joint Publication, it is clear the definition is more practical for deliberate targeting in a command operations center, not for Marines and Soldiers on patrol. However, a more pragmatic standard has developed based on the "international criminal law general intent standard of honest and reasonable belief."[79] As it relates to the use of force in self-defense, positive identification is "a reasonable certainty that the proposed target is a legitimate military target."[80] Stated another way, "PID is about recognizing hostile intent and hostile acts."[81]

III. The Way Forward

As demonstrated in Parts I and II of this article, the COIN environment presents the individual Marine and Soldier with difficult targeting scenarios without the benefit of clear, tangible guidance from the SROE. The practical result has been a broadening of what constitutes hostile intent and an imminent threat, as well as a confused application of the self-defense formula. This has led to an increased risk of civilian casualties and a targeting process that looks more like status-based targeting than the required conduct-based model. This article makes three recommendations to correct these problems: (1) return to a more traditional, narrow definition of hostile intent and imminence; (2) apply the self-defense formula correctly by recognizing hostile intent first and then gaining PID; and (3) require both commanders and judge advocates to forcefully incorporate these two recommendations into their overall ROE philosophy, pre-deployment training packages, and review of combat actions during the deployment.

A. Return to Traditional Imminence

Operating under U.S. SROE in a COIN environment, realistic limitations must be placed upon the meaning U.S. forces apply to the phrase "threat of imminent use of

[70] CJCSI SROE 3121.01B, *supra* note 5, app A to encl A.

[71] *Id*. para. 2a.

[72] SOLIS, *supra* note 10, at 505.

[73] Janin, *supra* note 3, at 91.

[74] *Id*.

[75] *Id*. at 93.

[76] *Supra* note 12.

[77] *See* SOLIS, *supra* note 10, at 508.

[78] JP 1-02, *supra* note 6, at 245.

[79] SOLIS, *supra* note 10, at 508.

[80] OPLAW HANDBOOK, *supra* note 7, at 103–04 (reprinting the Operation Iraqi Freedom Combined Forces Landing Component Commander ROE card promulgated 311334Z Jan 03 & the Operations Iraqi Freedom Multi-National Coalition – Iraq ROE card promulgated 27 Mar. 2007).

[81] SOLIS, *supra* note 10, at 508.

force."[82] As stated by Dr. Yoram Dinstein, a preeminent operational law scholar,[83] "[t]he use of force in self-defense cannot be based on grounds of assumptions, expectations, or fear of what is sometimes called a latent threat."[84] While any self-defense ROE must give servicemembers the ability to defend themselves before absorbing the "first punch," it cannot be so broad as to permit the use of force against overly anticipated threats. Solving this "quick trigger-finger" problem requires redefining the term imminent.

1. 2005 SROE Definition of Imminent Use of Force Is Not Necessary

The current SROE should be revised by removing the additional definition of "imminent use of force" and returning to the pre-2005 standard. As discussed in Part II, since the inception of the SROE in 1981, hostile intent required the threat of the imminent use of force without any further explanation. This left military leaders and individual servicemembers to apply the plain and traditional meaning of the term imminent. It was not until President Bush espoused his expanded view of national anticipatory self-defense that the explanatory language was added—defining imminent in the negative as "not necessarily meaning immediate or instantaneous."[85] While the expanded definition of anticipatory self-defense was necessary in the *jus ad bellum* use of force based on an uncertain and evolving asymmetrical threat, it was not necessary for the *jus in bello* application by individual Marines and Soldiers on the ground.[86]

2. Support for a Return to Traditional Imminence and Assumption of Greater Risk

Some commanders and judge advocates share the view that an additional definition of imminence was not needed. A former battalion and regimental combat team commander with multiple tours in Iraq and Afghanistan believes "there was no need for the addition" and that it "muddied the waters for no clear gain."[87] Supporting his opinion, the former commander was unaware of "a Marine [operating under the pre-2005 definition of hostile intent] who would not pull the trigger when their life was truly in danger."[88] Expanding the definition tended to "open the door for [individual] ROE to be confused with [deliberate] targeting."[89] A judge advocate with operational experience at division, brigade, and special forces commands believes Soldiers understood their authority to engage people demonstrating hostile intent prior to the 2005 SROE revision. He was "not clear what [the] change accomplished."[90] The judge advocate recommends the United States return to a natural law definition of imminence espoused in the Caroline Case. He believes imminent means immediate and a subsequent return to the traditional definition will "enhance the perceived legitimacy of the defensive use of force . . . ."[91]

The result of requiring "imminent" to mean "immediate" is a necessary burden of COIN operations: the assumption of greater risk. Greater risk assumption, and the resulting reduction in the use of force, will further mitigate the possibility of civilian casualties, which turn tactical gains into strategic losses.[92] The Counterinsurgency Field Manual succinctly states the importance of minimizing civilian casualties: "In COIN, killing a civilian is no longer just collateral damage; it undermines the goal of COIN."[93] Obviously, this is a counterintuitive concept to many military leaders trained in conventional warfare and force protection measures. However, more than ten years of COIN operations in Iraq and Afghanistan have proven that the acceptance of greater risk is a prerequisite to mission accomplishment.[94] The former battalion and regimental

[82] CJCSI SROE 3121.01B, *supra* note 5, app. A.

[83] Dr. Dinstein is currently a professor Emeritus at Tel Aviv University. He has guest-lectured all over the world and delivered a series of lectures at the Hague Academy of International Law. He is a member of the Institute of International Law and was also a member of the Executive Council of the American Society of International Law. Dr. Dinstein has written extensively, including a six-volume treatise on international law and his latest book, *War Aggression and Self-Defence*, is in its 5th edition. His writings have been cited by judges of the International Court of Justice and the International Criminal Tribunal for the Former Yugoslavia.

[84] DINSTEIN, *supra* note 17, at 206.

[85] CJCSI SROE 3121.01B, *supra* note 5, encl. A.

[86] *See* DINSTEIN, *supra* note 17, at 192 (stating that "[s]elf-defence (*sic*) exercised by States (legal entities) is not to be equated with self-defence (*sic*) carried out by physical persons").

[87] Colonel Smith e-mail, *supra* note 24.

[88] *Id*.

[89] *Id*.

[90] Merriam, *supra* note 17, at 87.

[91] *Id*.

[92] U.S. MARINE CORPS CTR FOR LESSONS LEARNED, CIVILIAN CASUALTY MITIGATION: SUMMARY OF LESSONS, OBSERVATIONS AND TACTICS, TECHNIQUES AND PROCEDURES FROM MARINE EXPEDITIONARY BRIGADE – AFGHANISTAN (MEB-A)—APRIL 2010, at 8 (29 July 2010) [hereinafter CIVILIAN CASUALTY MITIGATION AAR] (finding that reducing civilian casualties requires the assumption of additional risk, which is necessary to win the civilian population).

[93] Sewall, *Introduction* to FM 3-24, *supra* note 3, at xxv.

[94] *See, e.g.*, *id*, para. 7-13 ("Combat requires commanders to be prepared to take some risk, especially t the tactical level . . . However, in COIN operations, commanders may need to accept substantial risk to de-escalate a dangerous situation."); Major Trent A Gibson, Hell-Bent on Force Protection: Confusing Troop Welfare with Mission Accomplishment in Counterinsurgency (Apr. 8, 2009) (unpublished Masters of Military Science thesis, Marine Corps University) (on file with author) (concluding that "our military leaders must embrace the unconventional view inherent in out new counterinsurgency doctrine which places the immediate, near-term cost of success upon the shoulders of the Soldiers and Marines executing COIN

combat team commander, referred to previously, views risk in the COIN environment as follows: "In a COIN fight we must accept more risk. We accept it to protect innocents because (1) it is morally imperative and (2) it furthers the mission."[95]

B. The First Step Is Hostile Act or Hostile Intent, Not Positive Identification

The order in which a servicemember applies the self-defense formula is important to its proper application. In a typical addition equation, it does not matter how the values on the left side of the equal sign are combined. Whether the values are added in the order listed, or in a more convenient combination, the answer is always the same. The self-defense formula cannot be treated in the same manner.

Marines and Soldiers must first establish either a hostile act or hostile intent before they move to the PID aspect of the self-defense formula.[96] The consequence of obtaining PID before a hostile act or hostile intent is the employment of an improper targeting model in defensive COIN operations. If a servicemember initially determines an individual is a target based on PID, they are making a status-based targeting decision pursuant to the individual's physical characteristics.[97] Once an individual is positively identified as a "bad guy" under a status-based targeting model, seemingly innocuous conduct is misperceived as a hostile act or hostile intent, permitting the use of deadly force. The result is an increase in alleged self-defense engagements and unnecessary risk to surrounding civilians.

This faulty status-based determination is the result of a hyper-vigilant mental state resulting from the increased number of deployments executed by Marines and Soldiers over the last ten years. The compressed and frequent deployment cycle gives Marines and Soldiers a false sense of familiarity with the local population's culture and enemy techniques, tactics, and procedures.[98] However, as stated earlier, COIN operations require conduct-based targeting because the enemy does not distinguish itself from the civilian population and must be identified based on observed conduct. Commanders and judge advocates must recognize that frequent deployments are creating hyper-vigilant servicemembers and employ ROE training that addresses the potential problems.

C. Influence and Role of the Judge Advocate

1. A Deliberate Command Philosophy

As the principal legal advisor to the commander, judge advocates can exercise a tremendous amount of influence on ROE development, training, employment, and review within military units. Even with this influence, "commanders are solely responsible for the ROE philosophy in their unit, but as the size of the unit increases a commander must use surrogates to convey intent and in many instances that surrogate is the judge advocate."[99] Recognizing these facts, judge advocates must have a conversation with the commander regarding the commander's self-defense philosophy in a COIN environment, specifically with regard to hostile intent and imminence.[100]

In addition, judge advocates should work with their commanders to establish internal orders, rules, and policies to define left and right limits for common situations. Contrary to some opinions, rules can be established in a fluid combat environment that serve as a basis for decision-making in individual circumstances. [101] However, it is also important to realize that "ROE philosophy is not derived from ROE classes, but from constant interaction between the commander and his subordinates. Commanders must try and weave ROE into all of their communications."[102] Commanders and judge advocates should take the additional step of ensuring that members of their units not only understand when they can shoot, but also when they should not shoot even though legally permitted.[103]

---

operations"), *available at* http://www.dtic.mil/dtic/tr/fulltext/u2/a508083.pdf.

[95] Colonel Smith e-mail, *supra* note 24.

[96] CIVILIAN CASUALTY MITIGATION AAR, *supra* note 92, at 8 (requiring an observation of hostile intent or hostile act as imperatives before gaining positive identification).

[97] Physical characteristics that raise a servicemember's awareness and cause them to determine the individual is a legitimate military target include: holding a cell phone, riding on a red motorcycle, wearing a red turban, etc.

[98] Colonel Smith e-mail, *supra* note 24 (Marines "serving for multiple years in one small geographic area leads one to believe that one knows the inner workings of the adversary's mind, when in fact this is not the case. For example, after 2 [sic] deployments to Iraq, a Marine believes that he knows for a fact that 'when a bomb goes off, the only people on the street for the next 30 minutes are bad guys.' This is worsened if the Marine was trained by others who also had multiple deployments. We are smart people, and assume that after years of conflict, we should be able to derive intent, but the fact is that we cannot.").

[99] *Id*.

[100] FM 3-24, *supra* note 3, at 182 (stating that "commanders must ensure Soldiers and Marines understand the rules of engagement, which becomes more restrictive as peace and stability return").

[101] While the author was deployed to Afghanistan as a Command Judge Advocate to a Regimental Combat Team, the commander promulgated fragmentary orders and policies within the regiment that provided definitions and rules on how to deal with individuals suspected of spotting. Spotting was the practice of local national observing the actions of friendly forces and reporting those actions to other insurgents.

[102] Colonel Smith e-mail, *supra* note 24.

[103] CIVILIAN CASUALTY MITIGATION AAR, *supra* note 92, at 10 (A former Battalion Commander in Afghanistan explained, "Commanders on the ground, from the squad leader on up, have to have a complete

2. Reviewing Investigations and Underwriting Good-Faith Mistakes

Finally, when reviewing investigations involving self-defense ROE decisions, commanders and judge advocates must hold all servicemembers to the definition of imminence and hostile intent suggested in this article. At the conclusion of an investigation, commanders should not shy away from finding that a ROE violation occurred, even if the commander believes the Marine or Soldier acted in good faith. Determining that an ROE violation occurred accomplishes two things: (1) provides opportunities for commanders to conduct more focused ROE training based on a substantiated problem and (2) increases the credibility of the commander in the eyes of higher headquarters and the public because he accepts responsibility for a mistake and takes corrective action.

Moreover, prolonged U.S. involvement in COIN operations has demonstrated that leadership is willing to accept good faith misapplications of the ROE and not subject Marines or Soldiers to punishment or even a court-martial for a split-second decision. [104] This is because the Army and Marine Corps must institutionally "underwrite honest [ROE] mistakes and tell [its members] that such mistakes help the entire [unit] improve at performing difficult missions."[105] Ultimately, proactive and integrated involvement in self-defense ROE by the commander and judge advocate will lead to better training, more effective employment, and a commander who retains freedom of movement and maneuver within his battlespace.

IV. Conclusion

After more than ten years of COIN operations in Iraq and Afghanistan, U.S. forces have expanded the application of anticipatory self-defense, imminence, and hostile intent to a point that strains our credibility and, at times, detracts from mission accomplishment. The result is an increased risk of civilian casualties and a targeting model that has shifted away from the conduct-based targeting required in COIN operations and looks more like status-based targeting based on a civilian's physical characteristics. This is a byproduct of the increased number and duration of deployment tours by Marines and Soldiers making them hyper-vigilant to the operating environment. As stated in this article's introductory quotation from the 1940 Marine Corps' Small Wars Manual, small wars, or COIN in modern parlance, requires "principles of psychology . . . different from their normal application in major warfare of even troop leadership."[106]

Marines and Soldiers conducting COIN operations must have clear, understandable authority to use force in self-defense against demonstrations of hostile intent. Specific to the COIN environment, the authority to use force must be delicately balanced against the requirement of restrained force in order to protect and positively influence the civilian population. Compounding the difficulty restrained force presents, insurgents fail to distinguish themselves from the civilian population (usually in the hope of provoking an overly aggressive response from U.S. forces). In many instances, that overly aggressive response produces civilian casualties or destruction of civilian property, which further alienates the civilian population—undermining COIN efforts. The tools provided Marines and Soldiers operating in such an uncertain environment are the SROE concepts of self-defense in response to hostile act or hostile intent, and the self-defense formula that operationalizes the military directive for individual servicemembers.

To combat these problems, both judge advocates and commanders must first recognize a problem exists, and then institute a ROE philosophy as well as a training program that sets left and right lateral limits on what constitutes an imminent threat of force under the SROE. At a national strategic level, the SROE should be revised, returning to the pre-2005 definition of hostile intent. While the president's decisions to use force against asymmetric threats may require broader, more flexible authority, the same is unnecessary for the Marine and Soldier on the ground. At the tactical level, an imminent use of force should mean the threat is immediate and instant. This is the paradigm shift that is required to more effectively conduct COIN operations now and in the future.

---

understanding of the ROE. The ROE answers the question 'Can I do this?', but then you have to ask 'Should I?' Just because I can, doesn't mean I should.").

[104] Martins, *supra* note 17, at 12 (finding that "the facts do not support the assertion" that commanders will court-martial servicemembers for good-faith ROE mistakes); Colonel Smith e-Mail, *supra* note 24 (stating that "mistakes happen in war, and we cannot criminally charge those Marines who fail to meet the standard of performance in determining hostile act or hostile intent").

[105] Martins, *supra* note 17, at 11.

[106] *Supra* note 1.

Appendix

SROE Definitions of Hostile Intent

1. **Worldwide Peacetime ROE for Seaborne Forces, 1981**

Hostile Intent – The threat of the imminent use of force by a foreign force against the United States or U.S. forces. Evidence of hostile intent may lead to the force being declared hostile. Whether or not a force is declared hostile, where the hostile intent amounts to a threat of imminent attack, the right exists to use proportional force in self-defense by all authorized means available.

2**. JCS Peacetime Rules of Engagement, 26 June 1986**

Hostile Intent – Hostile intent is the threat of the imminent use of force by a foreign force or terrorist unit(s)/organization against the United States or U.S. forces, U.S. citizens and their property, or U.S. commercial assets. Where there is preparation for imminent use of armed force, the right exists to use proportional force, including armed force, in self-defense by all authorized means available in order to deter or neutralize the potential attacker or, if necessary, destroy the threat.

3. **CJCSI 3121.01, JCS Standing Rules of Engagement, 1 Oct 1994**

Hostile Intent – Hostile intent is the threat of imminent use of force by a foreign force or terrorist unit (organization or individual) against the United States, U.S. forces, and in certain circumstances, U.S. citizens, their property, U.S. commercial assets, or other designated non-U.S. forces, foreign nationals and their property. When hostile intent is present, the right exists to use proportional force, including armed force, in self-defense by all necessary means available to deter or neutralize the potential attacker or, if necessary, to destroy the threat.

4. **CJCSI 3121.01A, Standing Rules of Engagement for US Forces, 15 January 2000**

Hostile Intent – The threat of imminent use of force against the United States, U.S. forces, and in certain circumstances, U.S. nationals, their property, U.S. commercial assets, and/or other designated non-U.S. forces, foreign nationals and their property. Also, the threat of force to preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital USG property.

5. **CJCSI 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force by US Forces, 13 June 2005**

Hostile Intent – The threat of imminent use of force against the United States, U.S. forces or other designated persons or property. It is also the threat of force to preclude or impede the mission and/or duties of U.S. forces, including the recovery of U.S. personnel or vital USG property.

Imminent Use of Force – The determination of whether the use of force against U.S. forces is imminent will be based on an assessment of all facts and circumstances known to U.S. forces at the time and may be made at any level. Imminent does not necessarily mean immediate or instantaneous.

Readmission Rights of Servicemembers

On 14 August 2008, Congress enacted the Higher Education Opportunity Act (HEOA), which reauthorized the Higher Education Act of 1965.[1] In addition to reauthorizing existing programs, it created new requirements for institutions of higher education.[2] One such requirement is a little known provision pertaining specifically to members of the armed forces.[3] Under 20 U.S.C. § 1091c(b), "a person who is a member of, applies to be a member of, performs, has performed, applies to perform, or has an obligation to perform, service in the uniformed services shall not be denied readmission to an institution of higher education on the basis of that membership."[4] In essence, the HEOA creates readmission rights for servicemembers who are students, similar to the reemployment rights contained in the Uniform Servicemembers Employment and Reemployment Rights Act (USERRA).[5]

Under 20 U.S.C. § 1091c(c), student-Soldiers must satisfy three prerequisites to qualify for readmission rights.[6] First, the student must give advance written or verbal notice of military service to the appropriate official at the institution of higher education.[7] Second, the cumulative length of the absence (and of all previous absences) from the institution of higher education by reason of service cannot exceed five years.[8] Finally, upon their return, students must submit a notification of intent to reenroll in the institution.[9] As with USERRA, the implementing regulations for the readmission section of the HEOA contain important provisions that clarify and expand the language of the original statue.[10]

Pursuant to 34 C.F.R. § 668.18(a)(2), an institution must promptly readmit a servicemember whose absence was necessitated by military service with the same academic status as the student had when the student last attended the institution.[11] This means student-Soldiers receive the same enrollment status, the same number of credit hours, and the same academic standing on their readmission to the institution.[12] Most importantly, if the student-Soldier is readmitted into the same academic program, for the first academic year after returning, the tuition and fees will be the same as the academic year during which the student-Soldier left the institution.[13]

Another significant right provided to returning student-Soldiers is the right to receive refresher training to prepare for their academic programs.[14] Under 34 U.S.C. § 668.18(a)(2)(iv), if an institution determines student-Soldiers are not prepared to resume their program at the same academic status, the institution must make reasonable efforts at no extra cost to the student to assist them to become prepared.[15] These reasonable efforts may include providing free refresher courses and allowing the students to retake pretests at no extra cost.[16]

There are two important distinctions between the readmission provisions of the HEOA and USERRA.[17] First, the HEOA only applies to active-duty service "under Federal authority" for thirty or more consecutive days.[18] This means that inactive duty training (IDT), training pursuant to Title 32 for National Guard Soldiers, and active duty for fewer than thirty consecutive days are excluded from its protections.[19] Conversely, USERRA applies to IDT, Title 32 training periods, and active duty of any duration.[20] In addition, the HEOA allows returning Soldiers up to three years to provide notice of intent to return to their institution upon completion of their military service.[21] In contrast,

---

[*] Judge Advocate, U.S. Army Reserve (AGR). Presently assigned as Associate Professor, Administrative and Civil Law Department, The Judge Advocate General's Legal Center & School, Charlottesville, Virginia.

[1] *See* 20 U.S.C. §§ 1001–1161aa-1 (2012).

[2] *Id.* § 1091c (2012).

[3] *Id.*

[4] *Id.* § 1091c(b).

[5] *See id.* § 1091c (2012); 38 U.S.C. §§ 4301–4335 (2012).

[6] *See* 20 U.S.C. § 1091c(c).

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *See* 34 C.F.R. § 668.18 (2013).

[11] *Id.* § 668.18(a)(2).

[12] *Id.* § 668.18(a)(2)(iii).

[13] *Id.*. § 668.18(a)(2)(iii). If the students are admitted into different programs, they will be assessed no more than the tuition and fees that other students in the same program are assessed for that academic year. *Id.*

[14] *Id.* § 668.18(a)(2)(iv).

[15] *Id.*

[16] *Id.*

[17] *Id.* § 668.18(b), (c)(1)(iii); 20 C.F.R. §§ 1002.6; 1002.57; 1002.15 (2013).

[18] 34 C.F.R. § 668.18(b).

[19] *Id.* State active duty for the National Guard is excluded from both the HEOA and USERRA. *Id.*; 20 C.F.R. § 1002.57.

[20] *See* 20 C.F.R. §§ 1002.6, 1002.57.

[21] *See* 34 C.F.R. § 668.18(c)(1)(iii)(A). If student-Soldiers are injured during service, they are allowed up to two years from recovery to give notice of intent to return to their institution. *Id.* § 668.18(c)(1)(iii)(B).

USERRA only allows a maximum of ninety days for returning Soldiers to provide notice of their intent to return to their employers.[22]

In conclusion, the HEOA contains a little known but very important provision protecting servicemembers attending institutions of higher learning.[23] This provision and its implementing regulations create a regime of readmission rights applicable to all servicemembers serving on active duty for thirty or more consecutive days.[24] To the maximum extent possible, these readmission rights seek to place the absent servicemember in the same position as those students who did not leave their studies to answer their nation's call to duty.[25] This is a laudable goal that Judge Advocates should foster through education and training with respect to this important legislation.

—MAJ T. Scott Randall

[22] *See* 20 C.F.R. § 1002.15.

[23] *Id.* § 1091c.

[24] *Id.*; *see also* 34 C.F.R. § 668.18.

[25] *See generally* 20 U.S.C. § 1091c.

Iconoclast: A Neuroscientist Reveals How to Think Differently[1]

Reviewed by *Major Glen E. Woodstuff*[*]

Perception, courage, and social skills. The successful iconoclast learns to see things clearly for what they are and is not influenced by other people's opinions. He keeps his amygdale in check and doesn't let fear rule his decisions. And he expertly navigates the complicated waters of social networking so that other people eventually come to see things the way he does.[2]

I. Introduction

As the role of the judge advocate in the last ten years has morphed from pure staff officer to more of an active participant in military operations, the mindset of military members has had to change as well in terms of understanding that judge advocates assigned to their units can be value-added in real-world missions. In *Iconoclast: a Neuroscientist Reveals How to Think Differently*, author Gregory Berns[3] puts forth the definition of an iconoclast as "as a person who does something that others say can't be done."[4] In this sense, judge advocates, as a corps, have proven to be iconoclasts. According to Berns, the modern iconoclast overcomes conventional ways of thinking. The brain of an iconoclast operates very differently from that of an ordinary person. Iconoclastic brains differ in the functions of perception, fear response, social intelligence, and the circuits that implement them.[5]

In his exploration of iconoclasts, Berns explains complex biological actions of the brain and body, ties them to experiments to reinforce the scientific principle at hand and then offers up a personal sketch of a real person who exemplifies particular iconoclastic traits. Berns is not completely successful in tying together his science and his definition of an iconoclast. More precisely, his approach bogs down in the area of social intelligence and his chosen real life examples. In fact, his profile of the iconoclast is almost a distraction, as it is not clear whether thinking differently or the impact of the mighty iconoclast is the book's focus.

While his study of iconoclasm vacillates, he also promises an opportunity for the reader to "learn to think a bit more iconoclastically by understanding how the three key brain circuits work."[6] Here he succeeds. Berns is clearly a scientist with solid understanding of how the brain works and how it can work differently. For an audience of service members and military legal advisors, his examination of these three areas of brain function may allow consideration of the genesis of one's own thoughts and perhaps provide some insight into the behavior of fellow Soldiers.

II. Examining Perception, Fear Response, and Social Intelligence

Berns describes iconoclasts with some inconsistency by defining them in terms of perception, fear response, and social intelligence. However, his steadfast principle that iconoclasts "see things differently because their brains do not fall into efficiency traps as much as the average person's brain" rings true.[7] Readers will gain more benefit from the book if they remain open to the actual analysis of perception, fear response, and social intelligence, even if these areas are awkwardly applied to a definition of an iconoclast.

A. Perception

> [P]erception is not something that is immutably hardwired into the brain. It is a process that is learned through experience, which is both a curse and an opportunity for change.[8]

Berns notes that visual information begins in the eyes and then travels along two separate paths in the brain to the

---

[*] Judge Advocate, U.S. Army. Presently assigned as Command Judge Advocate, 418th Contract Support Brigade, Fort Hood, Texas.

[1] GREGORY BERNS, ICONOCLAST: A NEUROSCIENTIST REVEALS HOW TO THINK DIFFERENTLY (2010).

[2] *Id.* at app.

[3] Gregory S. Berns is the Distinguished Professor of Neuroeconomics and Director of the Center for Neuropolicy. His primary field of research is neuroecomonics, "the study of the neurobiological basis for individual preferences and how neurobiology places constraints on the decisions people make." *See Dr. Gregory S. Berns*, EMORY UNIV., http://www.ccnl.emory.edu/greg/ (last visited Aug. 19, 2013).

[4] *Id.* at 6.

[5] *Id.* at 5.

[6] *Id.* at 10.

[7] *Id.* at 7.

[8] *Id.* at 8. Berns goes on to explain,

> The brain faces the fundamental problem of interpreting physical stimuli that originate from the senses. Everything that the brain sees or hears or touches has multiple interpretations. The one that is ultimately chosen—the thing that is perceived—is simply the brain's best guess at interpreting what flows into it.

Id.

frontal cortex where visual processing occurs. One path carries information about the location of objects with respect to the viewer, while the other carries information about the type of object.[9] In order to process this information quickly, the brain takes shortcuts and makes assumptions.[10] Because Berns explains this scientific process so well for the layperson, the reader understands that the brain "pigeonholes" objects into categories resulting in a conventional view of things.[11] Focusing on how the brain categorizes visual information, Berns postulates that unfamiliarity forces the brain to discard usual categories of perception and create new ones. He suggests actually looking at something differently may break the brain out of normal low effort categorization that it is already accustomed to doing. A change of environment or considering an outside opinion may also do the trick.[12] Similarly, Berns theorizes that status quo visualizing hobbles imagination. Depicting a mental scene with more detail may break loose new ways of thinking.[13]

Knowing this effect exists is useful for any service member. Imagine when faced with a castle wall how viewing the earth under it as a place to stand or a place to tunnel may change the day. Changing perception of the physical world could make all the difference in combat, but just knowing that the brain grabs categories so "efficiently" is also useful. For instance, Soldiers in uniform might experience a momentary sense of surety when they see another Soldier practicing military tradition with pride and dedication. Military leaders can use this in understanding the underlying brain operations at work to preserve and reinforce esprit de corps.

B. Fear Response

> The stress system is not rational. It reacts when provoked, and this reaction is powerful enough to derail many of the most innovative people out there. The ability to tame the stress response represents the second great hurdle to becoming an iconoclast.[14]

Berns notes that fear causes people to avoid thinking and acting like iconoclasts. The brain will become sensitive to certain stressful scenarios and situations at the neuron level and avoid them.[15] The primary fears that inhibit iconoclasm are fear of the unknown, fear of failure, and fear of "looking stupid."[16] Fear arises from two separate biological systems. Both the neural and hormonal systems play a part, with the hormonal system often having long-lasting effects. Unfortunately, while these stress reactions can be quite beneficial in life and death situations, they are more likely activated in social situations in today's world where they are less helpful.[17]

In combat, a fuller understanding of fear's effects on the mind and body is always helpful. Understanding why the fear is unreasonable and repeated exposure to the source of that fear are tips on overcoming fear that are quite helpful.[18] However, Berns also recounts the experiments of Dr. Solomon E. Asch dealing with social pressure, explaining that "even when you strip away all the ambiguity of what an individual sees, and there is no possibility of personal gain or reprisal, people will still go along with the group." Berns explains that, disturbingly, this may happen at the perceptual level. Not only are people going with the group, but they might not even know they are doing so.[19]

Knowing that people might actually not only fail to speak out, but also adjust their thoughts to agree with the group is a disturbing phenomenon.[20] This should give every military leader pause. Not only is this apparently a routine mechanism of the brain, but military culture reinforces this by institutionally discouraging dissent. While there are good reasons for not quibbling in life and death situations, shutting off one's full analytical abilities in combat or even in general staff work can also have dire consequences. Helpfully, Berns notes that Asch's study shows that one additional dissenter is normally enough to break this "groupthink" effect. As a work around, Berns suggests that committees should not be required to arrive at a unanimous decision.[21] When just one other person shares a dissenting

[9] *Id.* at 20 (recounting the vision process, as detailed in *Brian A. Wandell, Foundations of Vision (1995)*).

[10] *Id.* at 28.

[11] *Id.* at 29.

[12] *Id.* at 33–35.

[13] *Id.* at 58.

[14] *Id.* at 62 ("In fact, the stress system is so important, and so active, that it can override every other system in the brain.").

[15] *Id*. at 68.

[16] *Id*. at 107.

[17] *Id.* at 62–63 (For an explanation of the human stress system, this author recommends *Robert M. Sapolsky, Why Zebras Don't Get Ulcers (2004)*.).

[18] *Id*. at 104.

[19] *Id.* at 92 (Berns reconstructed and commented on Asch's published observations of the experiment and his subjects' reactions.).

[20] *See generally* David Crump, *The Social Psychology of Evil: Can the Law Prevent Groups from Making Good People Go Bad?*, B.Y.U. L. REV. 1441 (2008) (exploring several negative incidents resulting in part from social pressure).

[21] The majority of sentences require two-thirds concurrence by the military panel. *See* 10 U.S.C. § 852(c) (2006). However, a sentence of death requires concurrence by all the members of the military panel. *See id.* §

opinion, the brain is far more likely to allow preservation of one's own judgment.[22]

Perhaps legal advisors should give in to temptation to play devil's advocate on occasion to encourage someone to speak up. If just one Soldier dons the beret of dissenting opinion, it is entirely possible that it may break open a floodgate of well-reasoned alternatives. Knowing this effect exists, military leaders may want to consider when it is appropriate to have committees meet in smaller groups before joining into a larger one. They may want to poll for opinions in writing before opening a topic for discussion. The workarounds are endless, but knowing that the effect exists is crucial. Remember: it is not that people will not speak up later, they may actually forget that they once had a differing opinion.

C. Social Intelligence

Berns notes the two key aspects of social intelligence as familiarity and reputation. He explains the phenomenon logically and clearly. It is not surprising that being familiar to others and having a good reputation is key to successful networking, yet Berns goes further and drills down into the neuroeconomics of familiarity. Berns explains that the brain clearly has a preference for familiarity at a subconscious level. He cites the work of psychologist Robert Zajonc and his "mere exposure effect,"[23] where people demonstrated a clear preference for images they had been exposed to previously. The exposure can be so brief that the images shown may not even be processed by the subject's minds. The subjects were not even aware they had seen them.[24]

The discussion of familiarity and reputation reinforces what every good military leader already knows. Similarly, networking is the bread and butter of any competent legal advisor. Nevertheless, understanding this familiarity phenomenon may be useful in implementing training and its effects can be seen every time changes occur in a more rigid institution like the military. The key is to get people comfortable with an idea before trying to implement it.

The book further explores some interesting networking phenomena by another renowned social scientist, Stanley Milgrim, who cleverly demonstrated that two randomly selected people are normally only separated by six degrees. This connection usually is done through a few connectors who form the glue of local society.[25] This study really demonstrates the exponential impact of successful networking and the effect should be considered by every military legal advisor. In the JAG Corps, when meeting a new colleague, it usually only takes a few minutes of conversation to figure out which JAs both co-workers know.

III. Where Things Fall Apart

While the topic of social intelligence is thoughtfully explored, this is where the book really starts to lose cohesion. Berns originally contends that social intelligence is a key aspect of being an iconoclast, but then toward the conclusion clarifies that social intelligence is required to be a "successful" iconoclast.[26] In terms of social intelligence, the author's theory just does not mesh as elegantly as it did in terms of perception, brain efficiency, and fear response. He is quite correct that networking is effective and an interesting topic to boot. However, this is where the book deteriorates from an interesting study of the brain to a rather meager and arguably impossible "how to" guide. Berns quibbles over his own proposed definition, going back and forth between a "true iconoclast," a "successful iconoclast," drawing the reader away from the sound principles he just spent over one hundred pages detailing and into strange semantic arguments.[27] This is just difficult to follow. Perhaps this inconsistency is best exemplified by his attempt to tie Milgrim's experiment on random people falling within six degrees of separation back to the iconoclast:

> Who were these common channels? . . . It makes sense that as the packets reached the vicinity of Boston, they should funnel to people who are viewed by the local community as well connected. These people are not iconoclasts. They couldn't be. As well-respected, upstanding citizens, connectors form the glue of local society. Iconoclasts, by their very nature, upset this delicate web of connectedness. But iconoclasts need connectors. Without them, the iconoclast stands no chance of achieving success. Sometimes iconoclasts have to create the connectors themselves.[28]

Thus, the reader will likely recall the original premise that iconoclasts are by definition socially intelligent. Then, the reader is told, successful iconoclasts are socially intelligent. On the other hand, socially intelligent people are well-

852(b)(1). Following the logic of Asch's study, does this requirement of unanimity make the sentence of death less likely or more?

[22] BARNES, *supra* not 1, at 103.

[23] *Id.* at 142 (describing the work of Robert Zajonc and the "mere exposure effect" he developed).

[24] *Id.* at 142.

[25] *Id.* at 134.

[26] *Id.* at 129.

[27] *Id.* at 6, 7, 129, 152.

[28] *Id.* at 135.

connected and that clearly iconoclasts upset connectedness. But then, the reader must understand that without connectedness an iconoclast will not be successful. Finally, the readers should be aware that sometimes iconoclasts create connectors themselves. Hopefully everyone is still tracking.

Intuitively, the reader will grasp that all the science offered so far seems to point toward the idea that iconoclasts think differently because their brains are different. Their brains categorize differently. Their brains do not shy away when others fear to think and act. Now Berns really tries to oversell iconoclasts as engaging paragons of social intelligence. It is almost as if the author wrote his study of the brain, decided to sell his idea, and then quickly wrote the book to make iconoclasm sound like a fun thing that you too can do.[29] No doubt glamourizing iconoclasm—appealing to the reader's secret hope that he is an iconoclast who is ready to shake worlds—will sell more books. It just does not ring true. Did the author not say that their brains were different? Is there no link between overcoming innate social awkwardness at an early age and having a more controlled fear response? Is there no intuitively obvious inverse proportion between inability to see the world as others do combined with willingness to stand outside a group and social intelligence? Berns may have left some interesting observations on the table. In doing so, he definitely detracts from the quality observations already made.

Berns also gives a few distracting examples of real life iconoclasts, no doubt because they are familiar or admirable figures. Some fail as instances of the trait of iconoclasm he is referencing and on a few occasions these cases fail his own definition of iconoclasm, which of course includes social intelligence. Oddly, Berns uses as his very first example an iconoclast who kills himself after a miserable failure in business.[30] Later in the book, to demonstrate overcoming fear response, he tells the story of a Dixie Chick. Natalie Maines overcame fear brought on by a change in public opinion after she criticized the President. According to Berns, this made her an iconoclast.[31] It is never made clear how a singer, being paid good money to sing, who continues to sing without really changing anything or going against any traditional norm or cultural edifice, might be an iconoclast.

IV. Conclusion

Iconoclast is an often interesting read that offers much in the way of scientific factoids and entertaining sketches. Berns has a knack for explaining the complex. It is unfortunate that *Iconoclast* fails to deliver on a unifying theme or consistent definition of an iconoclast. It forces the reader to hunt through the book searching for usable ideas instead of providing a cohesive read. If the author had explained the brain of an iconoclast and then divided out the benefit of social intelligence, the book would have been easier to digest. Similarly, many of the anecdotal stories meant to exemplify a particular iconoclastic trait fail to fit the mold he cast. Regardless, the strength of this book is not in how iconoclasts are exceptional and how you may secretly be one, notwithstanding the emerging role of the judge advocate being compared to an iconoclast; it is in the repeatedly referenced and thoroughly explained observation that the brain is a lazy piece of meat.[32] If judge advocate readers commit many of the scientific phenomena to practice and endeavor to spot their own lazy thinking, they may not wake in themselves a fully formed iconoclast, but another tool might be added to their problem-solving kits.

[29] *Id.* at 200.

[30] *Id.* at 2.

[31] *Id.* at 65–67.

[32] *Id.* at 36.

CLE News

1. Resident Course Quotas

a. Attendance at resident continuing legal education (CLE) courses at The Judge Advocate General's Legal Center and School, U.S. Army (TJAGLCS), is restricted to students who have confirmed reservations. Reservations for TJAGSA CLE courses are managed by the Army Training Requirements and Resources System (ATRRS), the Army-wide automated training system. If you do not have a confirmed reservation in ATRRS, attendance is prohibited.

b. Active duty servicemembers and civilian employees must obtain reservations through their directorates training office. Reservists or ARNG must obtain reservations through their unit training offices.

c. Questions regarding courses should be directed first through the local ATRRS Quota Manager or the ATRRS School Manager, Academic Department at (800) 552-3978, extension 3172.

d. The ATTRS Individual Student Record is available on-line. To verify a confirmed reservation, log into your individual AKO account and follow these instructions:

Go to Self Service, My Education. Scroll to ATRRS Self-Development Center and click on "Update" your ATRRS Profile (not the AARTS Transcript Services).

Go to ATTRS On-line, Student Menu, Individual Training Record. The training record with reservations and completions will be visible.

If you do not see a particular entry for a course that you are registered for or have completed, see your local ATTRS Quota Manager or Training Coordinator for an update or correction.

e. The Judge Advocate General's School, U.S. Army, is an approved sponsor of CLE courses in all states that require mandatory continuing legal education. These states include: AL, AR, AZ, CA, CO, CT, DE, FL, GA, ID, IN, IA, KS, KY, LA, ME, MN, MS, MO, MT, NV, NH, NM, NY, NC, ND, OH, OK, OR, PA, RI, SC, TN, TX, UT, VT, VA, WA, WV, WI, and WY.

2. Continuing Legal Education (CLE)

The armed services' legal schools provide courses that grant continuing legal education credit in most states. Please check the following web addresses for the most recent course offerings and dates:

a. The Judge Advocate General's Legal Center and School, U.S. Army (TJAGLCS).

Go to: https://www.jagcnet.army.mil. Click on the "Legal Center and School" button in the menu across the top. In the ribbon menu that expands, click "course listing" under the "JAG School" column.

b. The Naval Justice School (NJS).

Go to: http://www.jag.navy.mil/njs_curriculum.htm. Click on the link under the "COURSE SCHEDULE" located in the main column.

c. The Air Force Judge Advocate General's School (AFJAGS).

Go to: http://www.afjag.af.mil/library/index.asp. Click on the AFJAGS Annual Bulletin link in the middle of the column. That booklet contains the course schedule.

3. Civilian-Sponsored CLE Institutions

For additional information on civilian courses in your area, please contact one of the institutions listed below:

AAJE:	American Academy of Judicial Education P.O. Box 728 University, MS 38677-0728 (662) 915-1225
ABA:	American Bar Association 750 North Lake Shore Drive Chicago, IL 60611 (312) 988-6200
AGACL:	Association of Government Attorneys in Capital Litigation Arizona Attorney General's Office ATTN: Jan Dyer 1275 West Washington Phoenix, AZ 85007 (602) 542-8552
ALIABA:	American Law Institute-American Bar Association Committee on Continuing Professional Education 4025 Chestnut Street Philadelphia, PA 19104-3099 (800) CLE-NEWS or (215) 243-1600
ASLM:	American Society of Law and Medicine Boston University School of Law 765 Commonwealth Avenue Boston, MA 02215 (617) 262-4990
CCEB:	Continuing Education of the Bar University of California Extension 2300 Shattuck Avenue Berkeley, CA 94704 (510) 642-3973
CLA:	Computer Law Association, Inc. 3028 Javier Road, Suite 500E Fairfax, VA 22031 (703) 560-7747
CLESN:	CLE Satellite Network 920 Spring Street Springfield, IL 62704 (217) 525-0744 (800) 521-8662
ESI:	Educational Services Institute 5201 Leesburg Pike, Suite 600 Falls Church, VA 22041-3202 (703) 379-2900

FBA:	Federal Bar Association 1815 H Street, NW, Suite 408 Washington, DC 20006-3697 (202) 638-0252
FB:	Florida Bar 650 Apalachee Parkway Tallahassee, FL 32399-2300 (850) 561-5600
GICLE:	The Institute of Continuing Legal Education P.O. Box 1885 Athens, GA 30603 (706) 369-5664
GII:	Government Institutes, Inc. 966 Hungerford Drive, Suite 24 Rockville, MD 20850 (301) 251-9250
GWU:	Government Contracts Program The George Washington University Law School 2020 K Street, NW, Room 2107 Washington, DC 20052 (202) 994-5272
IICLE:	Illinois Institute for CLE 2395 W. Jefferson Street Springfield, IL 62702 (217) 787-2080
LRP:	LRP Publications 1555 King Street, Suite 200 Alexandria, VA 22314 (703) 684-0510 (800) 727-1227
LSU:	Louisiana State University Center on Continuing Professional Development Paul M. Herbert Law Center Baton Rouge, LA 70803-1000 (504) 388-5837
MLI:	Medi-Legal Institute 15301 Ventura Boulevard, Suite 300 Sherman Oaks, CA 91403 (800) 443-0100
MC Law:	Mississippi College School of Law 151 East Griffith Street Jackson, MS 39201 (601) 925-7107, fax (601) 925-7115
NAC	National Advocacy Center 1620 Pendleton Street Columbia, SC 29201 (803) 705-5000

NDAA:	National District Attorneys Association 44 Canal Center Plaza, Suite 110 Alexandria, VA 22314 (703) 549-9222
NDAED:	National District Attorneys Education Division 1600 Hampton Street Columbia, SC 29208 (803) 705-5095
NITA:	National Institute for Trial Advocacy 1507 Energy Park Drive St. Paul, MN 55108 (612) 644-0323 (in MN and AK) (800) 225-6482
NJC:	National Judicial College Judicial College Building University of Nevada Reno, NV 89557
NMTLA:	New Mexico Trial Lawyers' Association P.O. Box 301 Albuquerque, NM 87103 (505) 243-6003
PBI:	Pennsylvania Bar Institute 104 South Street P.O. Box 1027 Harrisburg, PA 17108-1027 (717) 233-5774 (800) 932-4637
PLI:	Practicing Law Institute 810 Seventh Avenue New York, NY 10019 (212) 765-5700
TBA:	Tennessee Bar Association 3622 West End Avenue Nashville, TN 37205 (615) 383-7421
TLS:	Tulane Law School Tulane University CLE 8200 Hampson Avenue, Suite 300 New Orleans, LA 70118 (504) 865-5900
UMLC:	University of Miami Law Center P.O. Box 248087 Coral Gables, FL 33124 (305) 284-4762
UT:	The University of Texas School of Law Office of Continuing Legal Education 727 East 26th Street Austin, TX 78705-9968

VCLE: University of Virginia School of Law
Trial Advocacy Institute
P.O. Box 4468
Charlottesville, VA 22905

4. Information Regarding the Judge Advocate Officer Advanced Course (JAOAC)

a. The JAOAC is mandatory for an RC company grade JA's career progression and promotion eligibility. It is a blended course divided into two phases. Phase I is an online nonresident course administered by the Distributed Learning Division (DLD) of the Training Developments Directorate (TDD), at TJAGLCS. Phase II is a two-week resident course at TJAGLCS each January.

b. Phase I (nonresident online): Phase I is limited to USAR and Army NG JAs who have successfully completed the Judge Advocate Officer's Basic Course (JAOBC) and the Judge Advocate Tactical Staff Officer Course (JATSOC) prior to enrollment in Phase I. Prior to enrollment in Phase I, students must have obtained at least the rank of CPT and must have completed two years of service since completion of JAOBC, unless, at the time of their accession into the JAGC they were transferred into the JAGC from prior commissioned service. Other cases are reviewed on a case-by-case basis. Phase I is a prerequisite for Phase II. For further information regarding enrolling in Phase I, please contact the Judge Advocate General's University Helpdesk accessible at https://jag.learn.army.mil.

c. Phase II (resident): Phase II is offered each January at TJAGLCS. Students must have submitted all Phase I subcourses for grading, to include all writing exercises, by 1 November in order to be eligible to attend the two-week resident Phase II in January of the following year.

d. Regarding the January 2014 Phase II resident JAOAC, students who fail to submit all Phase I non-resident subcourses by 2400 hours, 1 November 2013 will not be allowed to attend the resident course.

e. If you have additional questions regarding JAOAC, contact MAJ T. Scott Randall, commercial telephone (434) 971-3368, or e-mail Thomas.s.randall2.mil@mail.mil.

5. Mandatory Continuing Legal Education

a. Judge Advocates must remain in good standing with the state attorney licensing authority (i.e., bar or court) in at least one state in order to remain certified to perform the duties of an Army Judge Advocate. This individual responsibility may include requirements the licensing state has regarding continuing legal education (CLE).

b. To assist attorneys in understanding and meeting individual state requirements regarding CLE, the Continuing Legal Education Regulators Association (formerly the Organization of Regulatory Administrators) provides an exceptional website at www.clereg.org (formerly www.cleusa.org) that links to all state rules, regulations and requirements for Mandatory Continuing Legal Education.

c. The Judge Advocate General's Legal Center and School (TJAGLCS) seeks approval of all courses taught in Charlottesville, VA, from states that require prior approval as a condition of granting CLE. For states that require attendance to be reported directly by providers/sponsors, TJAGLCS will report student attendance at those courses. For states that require attorneys to self-report, TJAGLCS provides the appropriate documentation of course attendance directly to students. Attendance at courses taught by TJAGLCS faculty at locations other than Charlottesville, VA, must be self-reported by attendees to the extent and manner provided by their individual state CLE program offices.

d. Regardless of how course attendance is documented, it is the personal responsibility of Judge Advocates to ensure that their attendance at TJAGLCS courses is accounted for and credited to them and that state CLE attendance and reporting requirements are being met. While TJAGLCS endeavors to assist Judge Advocates in meeting their CLE requirements, the ultimate responsibility remains with individual attorneys. This policy is consistent with state licensing authorities and CLE administrators who hold individual attorneys licensed in their jurisdiction responsible for meeting licensing requirements, including attendance at and reporting of any CLE obligation.

e. Please contact the TJAGLCS CLE Administrator at (434) 971-3309 if you have questions or require additional information.

Current Materials of Interest

1. The Legal Automation Army-Wide Systems XXI—JAGCNet

a. The Legal Automation Army-Wide Systems XXI (LAAWS XXI) operates a knowledge management and information service called JAGCNet primarily dedicated to servicing the Army legal community, but also provides for Department of Defense (DoD) access in some cases. Whether you have Army access or DoD-wide access, all users will be able to download TJAGSA publications that are available through the JAGCNet.

b. Access to the JAGCNet:

(1) Access to JAGCNet is restricted to registered users who have been approved by the LAAWS XXI Office and senior OTJAG staff:

(a) Active U.S. Army JAG Corps personnel;

(b) Reserve and National Guard U.S. Army JAG Corps personnel;

(c) Civilian employees (U.S. Army) JAG Corps personnel;

(d) FLEP students;

(e) Affiliated (U.S. Navy, U.S. Marine Corps, U.S. Air Force, U.S. Coast Guard) DoD personnel assigned to a branch of the JAG Corps; and, other personnel within the DoD legal community.

(2) Requests for exceptions to the access policy should be e-mailed to: LAAWSXXI@jagc-smtp.army.mil.

c. How to log on to JAGCNet:

(1) Using a Web browser (Internet Explorer 6 or higher recommended) go to the following site: http://jagcnet.army.mil.

(2) Follow the link that reads “Enter JAGCNet.”

(3) If you already have a JAGCNet account, and know your user name and password, select “Enter” from the next menu, then enter your “User Name” and “Password” in the appropriate fields.

(4) If you have a JAGCNet account, *but do not know your user name and/or Internet password*, contact the LAAWS XXI HelpDesk at LAAWSXXI@jagc-smtp.army.mil.

(5) If you do not have a JAGCNet account, select “Register” from the JAGCNet Intranet menu.

(6) Follow the link “Request a New Account” at the bottom of the page, and fill out the registration form completely. Allow seventy-two hours for your request to process. Once your request is processed, you will receive an e-mail telling you that your request has been approved or denied.

(7) Once granted access to JAGCNet, follow step (c), above.

2. TJAGSA Publications Available Through the LAAWS XXI JAGCNet

a. The Judge Advocate General’s School, U.S. Army (TJAGSA), Charlottesville, Virginia continues to improve capabilities for faculty and staff. We have installed new computers throughout TJAGSA, all of which are compatible with Microsoft Windows Vista™ Enterprise and Microsoft Office 2007 Professional.

b. The faculty and staff of TJAGSA are available through the Internet. Addresses for TJAGSA personnel are available by e-mail at jagsch@hqda.army.mil or by accessing the JAGC directory via JAGCNET. If you have any problems, please

contact Legal Technology Management Office at (434) 971-3257. Phone numbers and e-mail addresses for TJAGSA personnel are available on TJAGSA Web page at http://www.jagcnet.army.mil/tjagsa. Click on "directory" for the listings.

c. For students who wish to access their office e-mail while attending TJAGSA classes, please ensure that your office e-mail is available via the web. Please bring the address with you when attending classes at TJAGSA. If your office does not have web accessible e-mail, forward your office e-mail to your AKO account. It is mandatory that you have an AKO account. You can sign up for an account at the Army Portal, http://www.jagcnet.army.mil/tjagsa. Click on "directory" for the listings.

d. Personnel desiring to call TJAGSA can dial via DSN 521-7115 or, provided the telephone call is for official business only, use the toll free number, (800) 552-3978; the receptionist will connect you with the appropriate department or directorate. For additional information, please contact the LTMO at (434) 971-3264 or DSN 521-3264.

3. The Army Law Library Service

a. Per *Army Regulation 27-1*, paragraph 12-11, the Army Law Library Service (ALLS) must be notified before any redistribution of ALLS-purchased law library materials. Posting such a notification in the ALLS FORUM of JAGCNet satisfies this regulatory requirement as well as alerting other librarians that excess materials are available.

b. Point of contact is Mr. Daniel C. Lavering, The Judge Advocate General's Legal Center and School, U.S. Army, ATTN: ALCS-ADD-LB, 600 Massie Road, Charlottesville, Virginia 22903-1781. Telephone DSN: 521-3306, commercial: (434) 971-3306, or e-mail at Daniel.C.Lavering.mil@mail.mil.

Individual Paid Subscriptions to *The Army Lawyer*

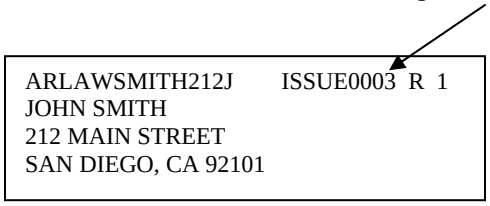
Attention Individual Subscribers!

The Government Printing Office offers a paid subscription service to *The Army Lawyer*. To receive an annual individual paid subscription (12 issues) to *The Army Lawyer*, complete and return the order form below (photocopies of the order form are acceptable).

Renewals of Paid Subscriptions

When your subscription is about to expire, the Government Printing Office will mail each individual paid subscriber only one renewal notice. You can determine when your subscription will expire by looking at your mailing label. Check the number that follows "ISSUE" on the top line of the mailing label as shown in this example:

A renewal notice will be sent when this digit is 3.



The numbers following ISSUE indicate how many issues remain in the subscription. For example, ISSUE001 indicates a subscriber will receive one more issue. When the number reads ISSUE000, you have received your last issue unless you renew.

You should receive your renewal notice around the same time that you receive the issue with ISSUE003.

To avoid a lapse in your subscription, promptly return the renewal notice with payment to the Superintendent of Documents. If your subscription service is discontinued, simply send your mailing label from any issue to the Superintendent of Documents with the proper remittance and your subscription will be reinstated.

Inquiries and Change of Address Information

The individual paid subscription service for *The Army Lawyer* is handled solely by the Superintendent of Documents, not the Editor of *The Army Lawyer* in Charlottesville, Virginia. Active Duty, Reserve, and National Guard members receive bulk quantities of *The Army Lawyer* through official channels and must contact the Editor of *The Army Lawyer* concerning this service (see inside front cover of the latest issue of *The Army Lawyer*).

For inquiries and change of address for individual paid subscriptions, fax your mailing label and new address to the following address:

United States Government Printing Office
Superintendent of Documents
ATTN: Chief, Mail List Branch
Mail Stop: SSOM
Washington, D.C. 20402

United States Government INFORMATION
PUBLICATIONS ★ PERIODICALS ★ ELECTRONIC PRODUCTS

Army Lawyer and Military Review
SUBSCRIPTION ORDER FORM

Order Processing Code: **5937**

Easy Secure Internet: **bookstore.gpo.gov**

Toll Free: 866 512-1800
Phone: 202 512-1800
Fax: 202 512-2104

Mail: Superintendent of Documents
PO Box 371954
Pittsburgh, PA 15250-7954

☐ **YES,** enter my subscription(s) as follows:

_____subscription(s) of the *Army Lawyer* (ARLAW) for $50 each ($70 foreign) per year.

_____subscription(s) of the *Military Law Review* (MILR) for $20 each ($28 foreign) per year. The total cost of my order is $_____.

Prices include first class shipping and handling and is subject to change.

Check method of payment:

Personal name (Please type or print)

Company name

Street address City, State, Zip code

Daytime phone including area code

Purchase Order Number

☐ Check payable to Superintendent of Documents

☐ SOD Deposit Account ☐☐☐☐☐☐ – ☐

☐ VISA ☐ MasterCard ☐ Discover/NOVUS ☐ American Express

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

☐☐☐☐ (expiration date)

Thank you for your order!

Authorizing signature

11/02