CYBER PRIVATEERS: A BRIEF INTRODUCTION TO THE MODERN USE OF LETTERS OF MARQUE AND REPRISAL

By Ben Laney

I. Introduction....1
II. Factual Background and Understanding the Problem....3
A. What is cyber warfare?....3
B. Examples of Cyber Conflicts....5
C. Cyber and the Law of Armed Conflict....7
D. The Big Issues of Cyber Warfare....10
1. What is and what is not an attack?....10
2. When does a Cyber Event Translate into a Real-World Action?....11
3. What can the military do to combat cyberattacks?....13
III. Creative Solution: Cyber Letters of Marque....16
A. Historical Background....16
B. Use of Privateers in a Modern Context....18
IV. Conclusion....24

I. Introduction

When faced with cybercrime and cyber terrorism from enemies, the United States must find unique and modern ways to tailor a response. In addressing the future of cyberwarfare, the government may find guidance in looking to the past. Given the transient and guerilla-like nature of cyberwarfare, the lessons of history learned in the Golden Age of Piracy may find relevance yet again in today's modern world.

Cyberwarfare is a new and constantly changing field of war and may include attacks on computer networks and information systems, as well as espionage on foreign entities. Both

individuals and state actors may be responsible for these actions, and many governments have established dedicated units of their militaries to cyber conflicts.

Among these are the nations of China, Russia, and North Korea, who have risen to challenge the United States in a new "Cyber Cold War." Since the overwhelming military dominance of the United States cannot be challenged, these nations seek the asymmetrical realm of the cyber world to close the gap. China has invested heavily into this strategy, believing that conducting cyber operations on American support networks and infrastructure can destroy the American "will to fight without having to actually enter into military combat."[1] China has emerged as the United States' most serious adversary in the realm of cyberwarfare, with previous successful attacks like hacking Google and stealing designs for the F-35 fighter jet.[2]

The application of Just War Theory to cyber conflicts is challenging. One theory suggested as a practical solution to the issue is the concept of a "cyber letter of marque." This concept is based on the practice of multiple nations during the Age of Sail and the Golden Age of Piracy, the period spanning from the mid-18th century to the early 19th century. Just as nations bestowed privateers with letters of marque as a way to attack opposing navies, the United States may find a successful deterrent in granting a cyber equivalent. This paper will analyze the principles of *jus ad bellum* and *jus in bello* as they apply to cyberwarfare and the real world, with special consideration given to the concepts of proportionality and attribution. This paper will then explore the creative solution of cyber letters of marque. This includes the historical context, the logistics of a modern letter of marque, and the potential issues and shortcomings of such a strategy.

---

[1] Richard J. Kilroy, Cyber Warfare and Cyber Terrorism 443-44 (2008).
[2] Christopher J. Eberle, *Just War and Cyberwar*, 12 J. Mil. Ethics 56 (2013).

II. Factual Background and Understanding the Problem

To understand what a cyber letter of marque is and how it may be employed, it is useful to have a basic overview of cyber warfare as it relates to the law of war. To do so, this paper will define commonly used terms as well as analyze the similarities and differences between traditional and cyber war.

A. What is cyber warfare?

Cyber warfare is a broad term encompassing any action taken for offense or defense in relation to computer networks.[3] Cyber operations include attempts to expose, alter, destroy, disable, or otherwise interfere with information networks.[4] These actions may include "defending information and computer networks, deterring information attacks, as well as denying an adversary's ability to do the same. It can include offensive information operations mounted against an adversary . . . ."[5] These actions may originate by a state actor, an agent of a state, or a non-state actor or group.[6]

Cyber warfare is a new field of combat with its own terminology. Before descending into the analysis, an overview of helpful terms follows.

- Cyberattack – any unauthorized attempt to access, alter, destroy, steal, or disable computer systems or networks.[7]
- Penetration testing – hacking into another's systems with no immediate intent of destruction in order to test both one's own offensive abilities and the defensive integrity

[3] Gary D. Solis, *Cyber Warfare*, 219 Mil. L. Rev. 1, 3 (2014).
[4] *Id*.
[5] *Id.*
[6] *Id*.
[7] Megan Costello, *Overview of Cyberattacks*, 1 Data Sec. & Privacy Law § 2:3 (2020-2021).

of the target. This is an ethical grey area that is closer to espionage until any destruction occurs.[8]

- Distributed Denial of Service (DDoS) Attack – a common offensive cyber-attack that involves multiple computers targeting a system or service at once to overload or restrict access to the system or service. DDoS attacks are temporary and do not typically lead to long-term disruption.[9]
- White hat hackers – an ethical computer hacker. Generally, a hacker employed by the government to penetration test systems with the intent of finding weaknesses to fix them.[10]
- Black hat hackers – a malicious computer hacker. Generally, a hacker with the goal of breaking a system to cause damage, either independently or for a government. These white hat/black hat designations are based off of old cowboy movies. Bad guys wore black cowboy hats, good guys wore white cowboy hats.[11]
- Stuxnet – a famous piece of weaponized malware. In 2010, it infected a vast number of computers, including Iran's uranium refinement systems. Using malicious code, Stuxnet was employed to physically destroy refinement controllers, disrupting the Iranian nuclear program.[12]

---

[8] 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, 85 n. 146 (2009).
[9] *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Nov. 20, 2019) https://us-cert.cisa.gov/ncas/tips/ST04-015.
[10] *What is the Difference Between Black, White and Grey Hat Hackers?*, NORTON, (Jul. 24, 2017) https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html.
[11] *Id*.
[12] Lieutenant Andrew Moore*, Stuxnet and Article 2(4)'s Prohibition Against the Use of Force*: *Customary Law and Potential Models*, 64 NAVAL L. REV. 1, 6 (2015).

While cyber warfare shares many similarities with traditional warfare, there are differences as well. In both traditional and cyber, there is no such thing as a "perfect defense." Throughout history, establishing a strong military defense meant building up forces to a level that discouraged attack, whether that be by constructing walls around a city or a fleet of naval vessels. In the cyber realm, defense means constantly employing your troops to break the current informational systems through penetration testing.[13] This is a necessary piece of maintaining a nation's cyber infrastructure, as only by trying to poke holes in the wall can the weaknesses be found. In a sense, the old adage of "the best defense is a good offense" still rings true, except the nation's offensive measures are directed at itself.

B. Examples of Cyber Conflicts

Military operations in the digital space are relatively new, but they are not rare. The United States has conducted several successful cyber operations towards foreign adversaries, and is widely attributed with creating Stuxnet.[14]

Cyberattacks do not always target such high value objectives. Cyber operations may play a support role in traditional military operations. For example, in the spring of 2014, Russia invaded and annexed the Crimean Peninsula.[15] As the Russian troops marched into the city of Sevastopol, Russian cyber forces began shutting down the city's cell phone networks and hindering the

[13] Cyber Security Services, *Penetration Testing*, https://www.cybersecurityservices.com/penetration-testing/ (last visited Dec. 8, 2020).
[14] Josh Fruhlinger, *What is Stuxnet, who created it and how does it work?*, CSO Online (Aug. 22, 2017), https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
[15] Steven Lee Myers & Ellen Barry, *Putin Reclaims Crimea for Russia and Bitterly Denouces the West*, N.Y. Times (Mar. 18, 2014) https://www.nytimes.com/2014/03/19/world/europe/ukraine.html.

Ukrainian ability to counterattack.[16] By attacking the enemy's ability to communicate and coordinate a response, Russia faced little local resistance in its actions.

The United States faces cyberattacks from foreign enemies on a regular basis. For example, Chinese hackers are especially troublesome in their intrusions and theft of intellectual property.[17] A Chinese operation known as "Night Dragon" involved the theft of hundreds of terabytes of plans and design documents for the Lockheed Martin F-35 fighter jet.[18] China has successfully conducted attacks on "citizens, private corporations, defense contractors, [and] government agencies" in its mission to infiltrate U.S. information systems.[19]

The persistent nature of these attacks has led to a new Cold War-esque conflict, one where both nations run interference on the other in the secret world of cyberspace. Like the conflict between the U.S. and the U.S.S.R. in the second half of the 20th Century, this new Cyber Cold War involves the "probing of military and industrial secrets… [and of] each other's territorial defenses."[20] The stark difference from the previous Cold War is that now there is no guarantee of mutually assured destruction in cyber warfare. Instead, the main threat lies in undermining citizens' confidence in government to protect them.

---

[16] Pierluigi Paganini, *Crimea – The Russian Cyber Strategy to Hit Ukraine*, InfoSec (Mar. 11, 2014), https://resources.infosecinstitute.com/topic/crimea-russian-cyber-strategy-hit-ukraine/.
[17] *See* David E. Sanger & Nicole Perlroth, *Chinese Hackers Resume Attacks on U.S. Targets*," N.Y. Times, May 20, 2013, at A1; Edward Wong, *Hackers Find China is Land of Opportunity*," N.Y. Times, May 23, 2013, at A1; David E. Sanger, *In Cyberspace, New Cold War*, N.Y. Times, Feb. 24, 2013, at A1.
[18] Jason Healey, *A Brief History of US Cyber Conflict*, in Jason Healey, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012, at 14, 68 (Cyber Conflict Stud. Ass'n 2013).
[19] Christopher J. Eberle, *Just War and Cyberwarfare*, 12 J. Mil. Ethics 1, 56 (2013).
[20] Randall R. Dipert, *The Ethics of Cyberwarfare*, 9 J. Mil. Ethics 1, 384-410 (2010).

C. Cyber and the Law of Armed Conflict

Cyber warfare is a difficult subject to define. The technology, policies, techniques, and strategies of cyber warfare constantly change in a way that makes it difficult to stay current. Despite this permeable nature, the Law of Armed Conflict applies to the cyber domain.[21]

The International Court of Justice notes that the law of war applies to "any use of force, regardless of the weapons employed."[22] The United States also treats cyber under the LOAC, officially stating that "the development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior–in times of peace and conflict–also apply in cyberspace."[23] Although cyber conflict law continues to develop with time, the Department of Defense "conducts [cyber operations] consistent with US domestic law, applicable international law, and relevant [United States Government] and DOD policies. The laws that restrict military actions in US territory also apply to cyberspace."[24] There are no multi-national treaties specifically dealing with the issue of cyber warfare.[25]

The traditional Just War Theory has two categories: *jus ad bellum* and *jus in bello*. *Jus ad bellum* is the law governing the right of going to war; *jus in bello* is the law governing permissible conduct once the conflict has begun.[26] A difficult question of cyber law depends on

---

[21] Gary D. Solis, *Cyber Warfare*, 219 MIL. L. REV. 1 (2014); *see also* U.S. DEP'T OF DEFENSE, LAW OF WAR MANUAL § 16.2.2 (June 2015) (Updated Dec. 2016) (stating that when no specific rule applies, use general principles of the law of war).

[22] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1995, I.C.J. 226-67, ¶ 39 (July 8).

[23] WHITE HOUSE, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World 9 (May 2011), http://www.slideshare.net/DepartmentofDefense/department-of-defense-strategy-for-operating-in-cyberspace.

[24] JOINT CHIEFS OF STAFF, JOINT PUB. 3-12, CYBERSPACE OPERATIONS I-1 (June 8, 2018).

[25] Gary D. Solis, *Cyber Warfare*, 219 MIL. L. REV. 1, 2 (2014).

[26] *Jus ad Bellum*, BLACK'S LAW DICTIONARY (11th ed. 2019); *Jus in Bello*, BLACK'S LAW DICTIONARY (11th ed. 2019).

whether the actions taken by foreign adversaries fit into the former or latter category. There are two ways of thinking: either (1) the United States is already engaged in a cyber war and thus must adhere to *jus in bello*; or (2) the United States is currently monitoring and on guard for a cyberattack, thus it must adhere to *jus ad bellum*.

Of course, cyberattacks will not occur only when Just War criteria have been met. In the cyber world, there are constant attempted hackings of systems.[27] While an adversary may violate the Just War Theory, it does not mean the United States can. Additionally, cyber is now arguably the most important tool in a modern military's arsenal, with cyber operations now taking place in tandem with military operations.[28] There is now a real possibility the decisive parts of a future conflict will focus on cyber, with space, submarines, and special forces following before the deployment of the surface navy or ground forces.[29] In this scenario, troops will not show up to the conflict until the end, with everything else taking place either in cyberspace or by small tactical teams carrying out pinpoint operations.

---

[27] Dominic Nicholls, *Britain is 'at war every day' due to the constant cyber attacks, Chief of the Defence Staff says*, THE TELEGRAPH (Sept. 29, 2020), https://www.telegraph.co.uk/news/2019/09/29/britain-war-every-day-due-constant-cyber-attacks-chief-defence/.

[28] INT'L COMM. OF THE RED CROSS, *Cyber attacks are a known threat: Now is the time for preventative action* (Aug. 26, 2020), https://www.icrc.org/en/document/cyber-attacks-are-known-threat-now-time-preventive-action ("The use of cyber operations during conflict is no longer a hypothetical scenario.
Over the past years, several States have stated publicly that they used cyber operations in military operations. As an increasing number of States are developing military cyber capabilities, the ICRC expects that their use is likely to also increase in future conflicts.");

[29] *See* Christopher Wooding, *The Rise of Cyber and the Changing Nature of War*, GROUNDED CURIOSITY (Sept. 1, 2019), https://groundedcuriosity.com/the-rise-of-cyber-and-the-changing-nature-of-war/ (asserting that cyber warfare is becoming the primary way for a nation to assert influence instead of through traditional war); *see also* Anna Johansson, *The future of war is cyber*, THE NEXT WEB (Jan. 20, 2019), https://thenextweb.com/contributors/2019/01/21/the-future-of-war-is-cyber/ ("Battles of the future won't be fought on the ground or sea – or even in the air. They'll be waged behind computers and servers.").

Cyber defense is a necessity. Since the nature of cyber defense is offensive action through penetration testing, the United States must hack foreign targets in order to avoid being outpaced in the Cyber Cold War. United States Cyber Command calls this policy "persistent engagement."[30] This strategy is the cyber equivalent of "defend forward," and involves the United States taking a proactive stance in advancing the initiatives of the armed forces in cyberspace, rather than a reactive approach.[31]

This requires a concerted effort from the military. The Constitution charges the Congress with "maintain[ing] a navy"–the United States cannot suddenly acquire a fleet of ships as soon as a conflict starts.[32] Likewise, cyber defense capabilities cannot be raised overnight, but instead must be cultivated and maintained.[33] Therefore, as a general matter, it is reasonable and just under the law of armed conflict for the United States to conduct offensive operations in a manner to develop its cyber defense capabilities.

While cyber operations as a whole are necessary for the health and defense of the nation, there remains the question of individual cyber actions. Unfortunately, there is no easy analytical framework to follow for assessing the legality of a single cyber operation. However, the National Security Law Department Operational Law Handbook provides a set of factors and questions to

[30] Nicole Lindsey, *US Cyber Command Signals More Aggressive Approach Involving Persistent Engagement Ahead of 2020 Election*, CPO Magazine (Sept. 16, 2020), https://www.cpomagazine.com/cyber-security/us-cyber-command-signals-more-aggressive-approach-involving-persistent-engagement-ahead-of-2020-election/.
[31] *Id*.
[32] U.S. Const. Art. I, § 8, cl. 12.
[33] *See generally* David E. Sanger, John Markoff, & Thom Shanker, *U.S. Steps Up Effort on Digital Defenses*, NY Times (Apr. 27, 2009), https://www.nytimes.com/2009/04/28/us/28cyber.html (supporting the assertion that military cyber capabilities cannot be raised quickly, but rather are a long-term investment); *see also* U.S. Dep't of Energy, *Cyber Security is National Security*, (Oct. 5, 2020), https://www.energy.gov/articles/cyber-security-national-security (recognizing the constant and expansive need for cyber defense capabilities).

consider. This includes asking the purpose of the activity, the military objective sought, how the task will be completed, and other relevant questions.[34]

D. The Big Issues of Cyber Warfare

There are three main questions that arise when applying the LOAC to cyber: (1) What is and what is not a cyberattack? (2) What can the military do to combat the cyberattack? (3) When does a cyber event translate into a real-world action?

1. What is and what is not an attack?

There is no strict definition as to what a cyberattack may entail. The TALLINN Manual defines a cyberattack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[35] The DoD Law of War Manual provides boundaries by defining what is not an attack. As stated previously, actions such as "defacing government webpages, minor, brief disruption of internet service, briefly disrupting communications, [and] disseminating propaganda" do not amount to an "attack" under the law of war.[36] Additionally, the cyber operation must not "be conducted in a way that unnecessarily causes inconvenience to civilians or neutral persons."[37]

The Operational Law Handbook provides factors for what might be an attack. Those factors frame the analysis in terms of severity, immediacy, directness, invasiveness, measurability, military character, state involvement, presumptive legitimacy.[38] While these

---

[34] The Judge Advocate General's Legal Center & School, U.S. Army, National Security Law Department, Operational Law Handbook [219-20] (2020) ("Operational Law Handbook").
[35] NATO Cyber Center of Excellence, TALLINN Manual on the International Law Applicable to Cyber Warfare, 415 (Michael N. Schmitt gen. ed. 2017) ["TALLINN 2.0"]
[36] Law of War Manual, *supra* note 21, § 16.5.2.
[37] *Id*.
[38] Operational Law Handbook, *supra* note 34, at 220.

factors are not the official policy of the Department of Defense, they are useful in applying the LOAC to assess whether a cyber operation has risen to the level of an attack.

2. When does a Cyber Event Translate into a Real-World Action?

This is a question that authors have sought to answer for years. If the United States is attacked in the cyber realm, it does not have to respond by cyber-based means. The Department of Defense Law of War Manual states that "any cyber operation that constitutes an illegal use of force against a State potentially gives rise to a right to take necessary and proportionate action in self-defense."[39] Additionally, "[t]here is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality."[40]

It is important to note that a cyberattack has never led to a real-world kinetic retaliation, with every state so far choosing to answer an attack in a digital manner. For example, in response to the Sony Pictures hack of 2014 by North Korea, President Obama declared that the United States would take a "proportional response" to the "cyber-vandalism."[41] In the weeks following the hack, North Korea's access to the internet was mysteriously severed. Publicly, it is unknown if this is the result of an American counterattack, or even a "mostly symbolic… warning shot that two can play the game of disruption."[42]

Under the LOAC, there are concerns about proportionality when it comes to a cyber response. "Enforcement measures must be reasonably related to the laws or regulations to which they are directed; punishment for noncompliance must be preceded by an appropriate

[39] U.S. DEP'T OF DEFENSE, LAW OF WAR MANUAL, § 16.3.3.1 (Dec. 2016) ("LAW OF WAR MANUAL").
[40] *Id*. § 16.3.3.2.
[41] Nicole Perlroth & David E. Sanger, *North Korea Loses Its Link to the Internet*, N.Y. TIMES, May 20, 2013, at A1.
[42] *Id.*

determination of violation and must be proportional to the gravity of the violation."[43] Under this rule of proportionality, any in-person or cyber-based counterattack must be proportional in scale to the original cyberattack.

Trying to come up with a real-world response for a cyber attack is difficult, as analogies between the physical world and digital world do not translate cleanly.[44] For example, when does a DDoS attack reach the level of severity that permits a nation to physically invade the cyber attacker? Does the hacking of a government server meet the requirements of *jus ad bellum* to allow the bombing of an enemy base? If the Chinese take the American power grid offline, does that justify the deployment of tanks?

Professor Michael Schmitt has offered eight factors to help determine when a cyber operation equals a use of force.[45] These factors are not exclusive or required, but helpful signposts. The factors include severity of the attack, whether a state or a rogue individual was involved, and the presumptive legitimacy of the attack.[46] While these may provide guidance when faced with the difficult task of assessing proportionality, it is ultimately up to a command's judge advocate and to make a decision.[47]

3. What can the military do to combat cyberattacks?

---

[43] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 431 (AM. L. INST. 1987).
[44] *See generally* George Perkovich & Alriel Levite, *Introduction to Understanding Cyber Conflict*, CARNEGIE ENDOWNMENT FOR INT'L PEACE (Oct. 16, 2017), https://carnegieendowment.org/2017/10/16/introduction-to-understanding-cyber-conflict-14-analogies-pub-73392 (providing analogies between cyber and kinetic combat, as well as recognizing the limitations of comparison).
[45] OPERATIONAL LAW HANDBOOK, *supra* note 34, at 219-20 (The eight factors are severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legitimacy).
[46] *Id*.
[47] *Id*. at 215-16.

A challenge uniquely difficult to cyber is determining where an attack came from. The underlying question here is "what is a valid target?" This calls upon the LOAC principle of distinction.[48] Under this principle, a military operation must only target opposing military forces, not innocent civilians.[49] The parties of a conflict must: (1) take measures to ensure military forces are visually distinct from civilians; (2) physically separate military objectives from the civilian population; and (3) refrain from using civilians as a shield to military objectives.[50]

In cyber warfare, any cyber operation can be made to look like it is coming from someone else, like a state spoofing its IP address to look like a civilian.[51] By spoofing the IP address of an innocent or by covering one's tracks with a virtual private network, it is extremely difficult to distinguish which actions are from state actors and which originate from a nonstate or private actor.[52] "Civilians are not prohibited from directly participating in cyber operations amounting to hostitilites, but forfeit their protection from attacks for such a time as they so participate."[53] Regardless, the United States has the right to "take necessary and proportionate action in self-defense in response to an armed attack originating through cyberspace applies whether the attack is attributed to another State or to a non-State actor."[54]

A cyber counterattack does not have to occur openly, the United States may hide its presence by masking its traffic. While normally there is a bar on using an enemy's uniform or

---

[48] LAW OF WAR MANUAL, *supra* note 21, § 2.5.1; *see also* TALLINN 2.0, *supra* note 35, at 420.
[49] *Id*.
[50] *Id*. § 2.5.1.
[51] Matthew Tanase, *IP Spoofing: An Introduction*, (Mar. 11, 2003), https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=9d18fc06-b229-4c4a-8ca5-7386d0870c01&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.
[52] Margaret Rouse, *VPN (Virtual Private Network)*, SEARCHNETWORKING, https://searchnetworking.techtarget.com/definition/virtual-private-network (last visited Dec. 4, 2020).
[53] TALLINN 2.0, *supra* note 35, at 413.
[54] LAW OF WAR MANUAL, *supra* note 21, § 16.3.3.4.

flag to conceal a military operation, a cyber operation is not bound to the rules.[55] Since cyber does not involve a tangible visual object, "it would not be prohibited to disguise network traffic as though it came from enemy computers or to use enemy codes during cyber operations."[56]

Determining where the attack comes from is easy when the power and information technology network is concentrated or carefully controlled by the government, like in North Korea.[57] When the identity of the attacker is known, the question of attribution becomes less of a concern.[58]

When the attack comes from a nonstate actor, or a state actor masquerading as one, the analysis is markedly more difficult. Any cyber operation must take precautions to not affect or to minimize the effect on civilian infrastructure and users.[59] Certain activities against civilians are not necessarily an act of war. Temporary detainment, restricting movement, or seeking to influence with propaganda are all acceptable non-violent measures of military necessity that may be carried out on enemy civilians.[60] Additionally, not every cyber operation is an attack. Actions such as briefly disrupting the internet, defacing a government webpage, or other acts of cyber-vandalism do not rise to the definition of an "attack."[61] "Only when a cyber operation

[55] *Id*. § 16.5.4.
[56] *Id*.
[57] Michael Raska, *North Korea's Cyber Warfare Capabilities Are Just Getting Started*, THE NATIONAL INTEREST (Oct. 4, 2020), https://nationalinterest.org/blog/reboot/north-koreas-cyber-warfare-capabilities-are-just-getting-started-169991 ("North Korea's internet infrastructure is isolated from global networks, with the country's entire internet traffic channelled through only two providers — China's Unicom and Russia's TransTeleCom. The country is largely unplugged from the global internet and is ringfenced by China's 'Great Firewall'.").
[58] *See* OFF. OF THE DIR. OF NAT'L INTEL., *A Guide to Cyber Attribution*, (Sept. 14, 2018) at 4.
[59] LAW OF WAR MANUAL, *supra* note 21, § 16.5.3.
[60] *Id*. § 5.2.2.1.
[61] *Id*. § 16.5.2.

against civilians . . . rises to the level of an attack is it prohibited by the priniciple of distinction . . . ."[62]

Attribution is especially difficult, as it is hard to say with 100% certainty when a cyberattack occurs. In the real world, an attack on an enemy base or a ship has a tangible effect. In the cyber world, operations are happening constantly, every day and at every hour. Whether the attacking force is military, a random civilian, or even a member of a "cyber gang" is difficult to ascertain.[63] If a power grid goes down, it may be a black hat hacker in Russia or it may just be a particularly nefarious squirrel.[64] When it is unclear whether an actor is an enemy combatant or a civilian, the default is to treat them as a civilian.[65]

When the perpetrator is a nonstate actor, or even a U.S. citizen, the proper response is to hand the case over to the FBI. The military does not typically act against lone-wolf cyber criminals. Generally speaking, unless an enemy cyber operation is so prolific as to being on par with Stuxnet, something that would open the door to a preeminent strike, or a "Cyber Pearl Harbor," the U.S. military will choose not to counterattack.[66] The military would most likely not get involved in an investigation of a DDoS attack of a private company.

---

[62] TALLINN 2.0, *supra* note 35, at 422.
[63] Misha Glenny, *Cyber Subterfuge*, N.Y. Times (Nov. 27, 2013), https://www.nytimes.com/2013/11/28/opinion/cyber-subterfuge.html? ("the virtual world is awash with subterfuge, malware and deception").
[64] David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid*, N.Y. Times (June 15, 2019), https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html; Washington Post, *Squirrel attacks on the US power grid shown in one hilarious map*, The Independent (13 Jan. 2016), https://www.independent.co.uk/news/world/americas/squirrel-attacks-us-power-grid-shown-one-hilarious-map-a6809171.html.
[65] TALLINN 2.0, *supra* note 35, at 424.
[66] Sharon Weinberger, *Cyber Pearl Harbor: What hasn't a mega attack happened?*, BBC Future (Aug. 19, 2013), https://www.bbc.com/future/article/20130820-cyber-pearl-harbor-a-real-fear.

Each cyber operation requires its own unique analysis. For example, it is likely unlawful for the United States take out a Domain Name System (DNS) server in China to respond the theft of government files. Doing so would disrupt the internet service not only for the government, but for ordinary citizens as well, a lack of distinction and precision that violates the LOAC. Even if the military was able to find the single individual who started the hack, it would be bound to the rules of proportionality when delivering a response. Since cyber warfare is conducted through proxies and by spoofing locations, the burden of establishing that the civilian was indeed the perpetrator with enough certainty to overcome the presumption of innocence is quite high.[67]

III. Creative Solution: Cyber Letters of Marque

Cyber warfare is a constantly evolving field, with technology improving at a blistering pace. In search of solutions to the issues of waging a cyber war, some have suggested looking to the past and modernizing a forgotten tool of war: the letter of marque and reprisal.[68]

A. Historical Background

During the Golden Age of Sail (roughly the late Middle Ages to the 18th century), naval power was the dominant tool of militaries and empires. A letter of marque and reprisal was a government license that authorized private individuals, such as privateers or corsairs, to attack and capture vessels of an enemy nation legally.[69] Originally, privateers were essentially independent contractors for the Crown; rather than the British Empire spend military assets on

[67] Christopher S. Chivvis and Cynthia Dion-Schwarz, *Why It's So Hard to Stop a Cyberattack – and Even Harder to Fight Back*, The RAND Blog (Mar. 30, 2019), https://www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html.
[68] *See* Ensign Lucian Rombado, *Grant Cyber Letters of Marque to Manage "Hack Backs,"* U.S. Naval Institute, Vol. 145/10/1,400, https://www.usni.org/magazines/proceedings/2019/october/grant-cyber-letters-marque-manage-hack-backs; *see also* Adam J. Macleod, *Making Cyber Criminals Walk the Constitutional Plank*, Law & Liberty (Nov. 23, 2020) https://lawliberty.org/making-cyber-criminals-walk-the-constitutional-plank/.
[69] *Id*. at 6.

combating the Spanish Armada, it could grant letters of marque to a dozen corsairs to go harass the Spanish on the King's behalf.[70]

With a letter of marque, a civilian is deputized by the granting entity, giving the recipient policing powers. This includes permission to cross international borders to conduct reprisal attacks, while also requiring privateers to follow the laws of war, avoid attacking neutral parties, and treat captives properly.[71]

A letter of marque required privateers to bring the ships, crews, and cargo they captured before an admiralty court for condemnation.[72] The admiralty law concept of prize would apply, and following an *in rem* proceeding in an admiralty court, the property would be sold and the proceeds would be split amongst the crew of the privateer.[73] This process is called condemnation, and transfers title from the enemy to the to the privateer and the crew.[74]

In its early history, the United States was a proponent of letters of marque.[75] Due to the small amount of ships in its fleet, privateers were seen as a valuable military resource, with Thomas Jefferson once saying: "every possible encouragement should be given to privateering in time of war .... Our national ships are too few ... to ... retaliate the 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."[76] Privateers played a key role in the War of 1812, supplementing the United States' fleet of sixteen ships against Britain's 1,060.[77]

---

[70] Francis R. Stark, *The Abolition of Privateering and the Declaration of Paris*, in 8 Studies in History, Economics and Public Law 221, 270–71 (Colum. Univ. 1897).
[71] *Id*. at 273.
[72] Robert Force & Martin J. Norris, The Law of Seamen § 18:17 (2020).
[73] Sonja Larsen, CSJ WAR § 24 (2020).
[74] *Condemnation*, Black's Law Dictionary (11th ed. 2019).
[75] See Robert P. DeWitte, *Let Privateers Marque Terrorism: A Proposal for a Reawakening*, 82 Ind. L.J. 131, 140 (2007).
[76] *Id*. at 134.
[77] Jerome R. Garitee, The Republic's Private Navy: The American Privateering Business as Practiced by Baltimore During the War of 1812, 244 (1977).

Letters of marque began to fall out of favor with the Paris Declaration Respecting Maritime Law, signed in 1856. This treaty contained three major provisions: (1) an abolition of privateering; (2) a prevention of the seizing of enemy goods on neutral ships; and (3) a prevention on the seizing of neutral goods on enemy ships.[78] The United States refused to sign the treaty, as it still did not yet possess a Navy capable of challenging the major powers. The United States did not officially end the practice of privateering until the 1907 Hague Peace Conference following the Spanish-American War.[79] While the United States no longer recruits privateers, there have been a few proposals to reinstate the practice in the context of aviation.[80] None of these have ever seriously been considered.

B. Use of Privateers in a Modern Context

The United States could grant a "Cyber Letter of Marque" to private companies as part of Cyber Command's "persistent engagement" strategy.[81] This is a self-help remedy in which:

> 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.[82]

---

[78] *Id*.
[79] *Id*.
[80] The Office of U.S. Representative Ron Paul, *Paul Offers President New Tool in the War on Terrorism*, U.S. House of Representatives (Oct. 11, 2001), https://web.archive.org/web/20070502184326/http://www.house.gov/paul/press/press2001/pr101101.htm.
[81] *See supra* Lindsey, note 30.
[82] 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).

Under this method, Cyber Command would deputize data companies and give them the ability to retaliate against attempted hacks independent of official United States intervention, similar to the original privateers of centuries past.[83]

For example, if Google was given a cyber letter of marque, it would have the legitimacy to counterattack against any individual or government that tries to hack it. This would be an express authorization to "hack back," an active defense inline with Cyber Command's persistent engagement strategy.[84] Normally, if Google discovered an attempted hack on its network, it would go to the FBI with all of the evidence it collected, leaving the case in the hands of the government. Once granted a cyber letter of marque and reprisal, if Google were to "see" an enemy hacker "in the wild" or on its network, it could attack the hacker unprovoked if it chose to. This is in line with the classic function of a letter of marque, in which a privateer could attack and capture an enemy vessel with the authority granted to the them by the state.[85]

As an agent and deputy of the United States, Google would still be required to follow the Law of War, just as was required in the Golden Age of Sail.[86] The United States would theoretically take responsibility if one of its cyber privateers did something it should not have done.[87] However, this cyber respondeat superior issue is not the problem it appears to be. Realistically, Google is not going to do something so egregious or escalatory as to hack the Chinese power grid. Cyber privateer behavior can be controlled through the threat of revocation

---

[83] *See supra* Section III.A.
[84] Matt Egan, *Hack the Hackers? Companies Itching to Go on Cyber Offense*, FOX BUS. (Dec. 7, 2012), https://www.foxbusiness.com/features/hack-the-hackers-companies-itching-to-go-on-cyber-offense; *see supra* Lindsey, note 30.
[85] *See supra* Larsen, note 73.
[86] *See supra* Stark, note 70.
[87] *See* Jill. M. Fraley, *The Government Contractor Defense and Superior Orders in International Human Rights Law*, 4 FLAMULR 43, 58 (2009) (for a discussion on the Superior Orders Defense and the Government Contractor's Defense in context to international humanitarian law); *see also infra* note 88.

of letters of marque or through potential tort liability.[88] Google will instead use the cyber letter of marque to maintain an active defense of its own network by allowing its own hackers to hack back, freeing Cyber Command to shift its focus elsewhere.

Were a cyber privateer to "go rogue" and trade their white hat for a black hat, the government would revoke his letter of marque and hold the individual or company responsible.[89] This is what historically occurred to those who exceeded the commission granted to them, such as Captain Kidd, who exceeded his authority and became a pirate.[90]

Cyber letters of marque would simplify the task of establishing a comprehensive defense, as the government and military would essentially outsource the task to privateers to support official operations. The scope and scale of cyber defense is massive, with so much surface area to cover in order to maintain efficiency.[91] The added resources and people to be gained from issuing these commissions may work towards covering all weak points, even as the boundary of competent defense changes constantly.

1. Pre-Existing Legal Framework

A cyber letter of marque could apply the existing federal law on privateers to work in the modern era. Much of the common law and federal law created pre-Civil War could easily apply to the cyber domain.[92] The federal judiciary holds jurisdiction over admiralty proceedings, with

---

[88] Theodore T. Richard, *Reconsidering The Letter of Marque: Utilizing Private Security Providers Against Piracy*, 39 PUBCONLJ 452, 455 (2010); *see also The Santissima Trinidad*, 20 U.S. 283 (1822) (holding that illegal privateers "are tortuous – and the original owner is entitled to restitution when brought within our jurisdiction").
[89] *Id*. at Section VII.A.
[90] *Id*.
[91] *See generally* U.S. Gov't Accountability Office, *Cybersecurity Challenges Facing the Nation – High Risk Issue* (2020), https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary (highlighting the vast number of cybersecurity risks).
[92] *See* Richard, *supra* note 88 at 438 ("In other words, Congress has already authorized the president to deputize private entities to act within the law to disable and capture pirates.").

the ability to determine prizes and administer a letter of marque.[93] The Supreme Court has heard multiple cases of privateering incidents, establishing a legal history of judicial oversight.[94]

Similar to traditional maritime prize law and the capture of ships and cargo, a cyber privateer could bring the data and assets it recovers from the attacker to a "cyber admiralty court" to have the government condemn it.[95] With a successful counterattack, the privateer could discover a vast amount of information about the hacker, a database of contacts, assets, or other digital loot.[96]

The decentralized nature of historical letters of marque meant there was a lack of organization or unified command.[97] To fix this issue, it reasonable to think Cyber Command or another issuing authority would mandate reporting requirements for authorized cyber privateers.[98] With Cyber Command acting as a central authority, the government would have the ability to monitor its agents to ensure compliance with the Law of War.

C. Issues and Shortcomings

Issuing a cyber letter of marque to private data companies is not a perfect solution to enhance the United States' cyber defense strategy, and presents more problems than it solves. As

---

[93] 10 U.S.C.A. § 8852 ("the United States district courts have original jurisdiction, exclusive of the courts of the States, of each prize and each proceeding for the confemnation of property taken as prize"); 33 U.S.C.A. § 386 ("The President is authorized to instruct the commanders of the public-armed vessels of the United States . . . to subdue, seize, take . . . any vessel").
[94] *See, e.g.*, *The Resolution*, 2 U.S. 19 (1781); *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).
[95] *See* Force & Norris, *supra* note 72.
[96] NERC, *Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities*, (Sept. 4, 2019), https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf (an example of a postmortem on a cyberattack and lessons learned); *see also supra* OFF. OF THE DIR. OF NAT'L INTEL., note 58 (examples of what can be learned from a cyberattack).
[97] *See* Edgar Stanton Maclay, *History of Privateers*, xxiv (1900) (privateers were often unaware of whether a ship was friendly due to a lack of coordination and communication).
[98] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) (example of precedence for establishing similar cyber defense authority).

discussed above, attributing a cyber operation to a specific nation or individual is uniquely difficult.[99]

For example, imagine Microsoft's main campus in Redmond, Washington suffered an attack to its data center and had files stolen.[100] At a glance, it appears the attack originated from a server located in Russia. However, this does not necessarily mean Russia conducted the operation; the attacker could have used a proxy to remotely connect to the Russian server while physically working in China. With a cyber letter of marque, Microsoft could counterattack immediately without coordinating with Cyber Command. Microsoft could choose to "shoot from the hip" and retaliate against Russia before conducting an investigation to determine whether Russia was actually responsible. In a worst case scenario, Microsoft would conduct an attack on an innocent and unsuspecting Russia for the actions of another party. As a deputized agent of the government, Microsoft would incur liability for the United States.

Of course, Microsoft or any other private company is not going to take down the Russian powergrid or pull off the next Stuxnet. Realistically, no operation that big would be carried out independent from the United States military. However, this hypothetical does highlight the issue of control. The holders of historical letters of marque and reprisal operated on their own, hundreds of miles from the nearest port and with no way to contact the issuing government.[101] Receiving a modern letter of marque could require the privateer to coordinate with the United States in conducting cyber operations, or require notice before hacking back. Such a requirement does negate the independence of a letter of marque, making the holder less of a cyber privateer and more of a government contractor.[102]

---

[99] *See supra* Section II.D.3.
[100] Author's original hypothetical.
[101] Maclay, *supra* note 97.
[102] *See* Richard, *supra* note 88.

The proportionality issue is still a concern.[103] In another example, Target is hacked and four million customers' credit card data is leaked to the world.[104] After an investigation, it is revealed three black hat hackers operating out of Turkey are responsible for the hack. How does Target retaliate in a way that is proportional under the law of war? How do you quantify the data of four million customers, and then how do you decide if it is proportional to inflict that much punishment on three individuals? Now assume the hypothetical is changed so the attack just penetration testing, an act significantly less egregious. Is Target limited to only engaging in penetration testing back at the three hackers, or can it do something like remotely destroying the attacking computer so the hackers cannot continue to harass the corporation?[105]

Additionally, granting cyber letters of marque may have the effect of making the United States look weak. Traditionally, the state owns a monopoly on policing power and the legitimate use of force.[106] Outsourcing cyber defense to private companies potentially undermines the sovereignty and authority of the United States, as it chooses to rely not on its own might, but on the strength of corporations.[107]

Overall, letters of marque do not do enough to solve the problems of adapting the Law of Armed Conflict to cyber. Instead, it merely shifts the immediate decision-making burden of what to do when encountering a cyberattack from the government to a private entity. The aforementioned issues with proportionality and attribution are not solved with this method, and instead open the United States up to liability for the actions of its cyber privateers.

---

[103] *See supra* Section II.D.2.
[104] Author's original hypothetical; Nicole Perlroth, *Target Investigates Breach Involving Credit Card Data*, N.Y. TIMES (Dec. 18, 2013), https://bits.blogs.nytimes.com/2013/12/18/target-looking-into-security-breach/?searchResultPosition=1 .
[105] *See* Moore, *supra* note 12.
[106] *See* Richard, *supra* note 88 at 451.
[107] *Id*.

The idea is novel and has precedence in history.[108] However, cyber letters of marque are not the solution the United States needs to continue the growth of its cyber defense capabilities. Before the internet made near-instantaneous communication possible, the ability to authorize privateers to operate independently allowed the United States to bolster its burgeoning navy.[109] While there is a present need for the military to increase its cyber capabilities, the solution is not to give cyber privateers to carry out justice on behalf of the nation. To accomplish Cyber Command's persistent engagement policy, the smarter solution is to increase funding for expanding the military's cyber operations as well as increasing civilian contracting through the Department of Defense.[110]

IV. Conclusion

Cyber warfare is the newest and fastest developing battlefield. While cyber operations take place entirely in the virtual world, the traditional Law of Armed Conflict still applies.[111] The United States conducts cyber warfare consistent with applicable domestic and international law.[112]

Keeping pace in the Cyber Cold War means the United States must constantly attempt to hack foreign targets.[113] This is inline with Cyber Command's policy of persistent engagement, in which the military takes a proactive approach to engaging in cyber warfare, rather than a reactionary approach.[114]

---

[108] *See supra* Section III.A.
[109] *Id*.
[110] *See supra* Section III.B; White House, *24. Cybersecurity Funding*, (Mar. 2019), https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf.
[111] *See supra* Section II.C.
[112] *See supra* Section II.C.
[113] *See supra* Section II.B.
[114] *See supra* Section II.C.

There are three main questions that arise when applying the LOAC to cyber: (1) What is and what is not a cyberattack? (2) What can the military do to combat the cyberattack? (3) When does a cyber event translate into a real-world action? All three are fact-specific questions that depend on the circumstances surrounding an operation, but various publications provide guideposts for calculating a response.[115] When conducing an analysis on how to retaliate, the principles of proportionality, distinction, and attribution become uniquely difficult in the cyber context.[116]

A possible solution to these issues is to grant cyber letters of marque to white hat hackers and private companies to engage enemies in cyberspace on the United States' behalf.[117] This idea has historical background in the Age of Sail, when privateers would attack and capture enemy ships and cargo on behalf of the authority granting them letters of marque and reprisal.[118] Under this concept, a private entity could engage with an enemy it encounters in cyberspace or immediately retaliate independent of the government.[119] However, the United States would still ultimately be liable for the actions of those it grants this power too.[120]

Because of the challenge of properly attributing an attack and calculating an appropriate, proportional response, as well as the extra source of liability, the government is unlikely to seriously pursue this idea.[121] While a creative solution, the same result of fortifying the nation's cyber defense can be accomplished by easier, less risky means.

---

[115] *See supra* Section II.D.
[116] *See supra* Section II.D.
[117] *See supra* Part III.
[118] *See supra* Section III.A.
[119] *See supra* Section III.B.
[120] See supra Section III.C.
[121] *See supra* Section III.C.