Sea Dogs in Cyberspace: Exploring the Employment of Privateers in the Cyber Domain

A Monograph

by

MAJ Joshua R. Taft
US Army

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2020

REPORT DOCUMENTATION PAGE

Form Approved

OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
28-06-2019	Master's Thesis	JUN 2019-MAY 2020

4. TITLE AND SUBTITLE
Sea Dogs in Cyberspace: Exploring the Employment of Privateers in the Cyber Domain

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Joshua R. Taft

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATXL-SWD-GD
Fort Leavenworth, Kansas 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Military Studies Program, School of Advanced Military Studies.

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

During the age of sail, the employment of letters of marque and reprisal were a legitimate form of naval warfare, enhancing a state's maritime power while disrupting its enemy's economic capacity to wage war. Privateers were state-sponsored pirates—civilian auxiliaries commissioned by authorized government officials to attack an enemy nation's merchant fleet. Letters of marque and reprisal issued by their government legitimized their piratical activities. With the cover of such documents, privateers preyed upon on any vessel flying the flag of an enemy nation. Governments paid nothing to these mariners during war, but gained from their exploits against enemies, usually taking portions of prizes seized from enemy vessels. This monograph follows pragmatist methodology and uses a historical analogy to compare characteristics of privateering to a recent state-sponsored cyber operation. It also explores the possibility of privateers in cyberspace operating on behalf of American interests. This paper does not investigate analogy to claim that history repeats itself, but instead evaluates whether and how historical concepts can be useful when interpreting contemporary events.

15. SUBJECT TERMS
Privateering, Cyber Operations, Non-State Actors, Operational Contractor Support, Private Security Contractors

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					MAJ Joshua R. Taft
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	(U)	40	**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)			(914) 438-4628

Monograph Approval Page

Name of Candidate: MAJ Joshua R. Taft

Monograph Title: Sea Dogs in Cyberspace: Exploring the Employment of Privateers in the Cyber Domain

Approved by:

_____, Monograph Director
Adam D. Lowther, PhD

_____, Seminar Leader
Leroy B. Butler, LtCol

_____, Director, School of Advanced Military Studies
Brian A. Payne, COL

Accepted this 21st day of May 2020 by:

_____, Acting Director, Office of Degree Programs
Prisco R. Hernandez, PhD

Abstract

Sea Dogs in Cyberspace: Exploring the Employment of Privateers in the Cyber Domain, by MAJ Joshua R. Taft, 40 pages.

During the age of sail, the employment of letters of marque and reprisal were a legitimate form of naval warfare, enhancing a state's maritime power while disrupting its enemy's economic capacity to wage war. Privateers were state-sponsored pirates—civilian auxiliaries commissioned by authorized government officials to attack an enemy nation's merchant fleet. Letters of marque and reprisal issued by their government legitimized their piratical activities. With the cover of such documents, privateers preyed upon on any vessel flying the flag of an enemy nation. Governments paid nothing to these mariners during war, but gained from their exploits against enemies, usually taking portions of prizes seized from enemy vessels.

This monograph follows pragmatist methodology and uses a historical analogy to compare characteristics of privateering to a recent state-sponsored cyber operation. It also explores the possibility of privateers in cyberspace operating on behalf of American interests. This paper does not investigate analogy to claim that history repeats itself, but instead evaluates whether and how historical concepts can be useful when interpreting contemporary events.

Contents

Acknowledgements

I would like to thank my wife and love of my life, Macarena, for her unwavering support, understanding, and patience throughout my tenure at AMSP. You are my rock, and I would not have completed this project without you. Secondly, I would like to thank my parents, Cathey and Stephen Taft, whose unrelenting encouragement throughout my military career continues to push me to discover new goals and achieve new limits. To LtCol Bryant Butler and Dr. Adam Lowther, thank you for your professional conversations and feedback, both of which made this monograph possible. Finally, to my classmates in AMSP Seminar 4, thank you for continuing to push me to become a better student and officer throughout this academic year.

Abbreviations

AMT	Account Management Tool
AOR	Area of Responsibility
CAAF	Contractors Authorized to Accompany the Force
CFAA	Computer Fraud and Abuse Act
CFR	United States Code of Federal Regulations
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
DoD	Department of Defense
DODI	Department of Defense Instruction
FSB	Russian Federal Security Service
ICC	International Criminal Court
IHL	International Humanitarian Law
JP	Joint Publication
NCMF	National Cyber Mission Force
NGO	Nongovernmental Organizations
OCS	Operational Contract Support
PSC	Private Security Contractors
UDB	User Database
US	United States
USC	United States Code

Tables

Introduction

On September 26, 1580, Sir Francis Drake returned to Plymouth, England, after circumnavigating the world. With permission from Queen Elizabeth via her vice-chamberlain, Sir Christopher Hatton, Drake had originally embarked not to gain national prestige or flaunt England's maritime ability, but to intercept precious minerals and jewels from the Spanish Empire.[1] As his sailors rejoiced upon their arrival to England and unloaded their plunder, the value of their stolen riches was tallied. Drake amassed 160,000 Elizabethan pounds during his three-year voyage—almost half a billion pounds in today's currency, and Queen Elizabeth used part of the bounty to pay off England's debt.[2]

Sir Francis Drake was one of England's most famous "sea dogs:" privateers hired by the Crown to raid Spanish colonial holdings along the western coast of South America. Between the late sixteenth and mid-nineteenth centuries, a period also referred to as the age of sail, privateers were state-sponsored pirates: civilian auxiliaries commissioned by authorized government officials to attack an enemy nation's merchant ships. A letter of marque issued by their government legitimized their piratical activities.[3] With the cover of such documents, privateers were free to prey on any vessel flying the flag of an enemy nation, seizing cargo and vessels as prizes of war, and later dividing those prizes amongst themselves and their issuing state.

During the reign of Queen Elizabeth I, England's maritime position in the world depended on privateers, and privateers made up the nucleus of the Royal Navy. It was natural for the Queen to employ her ships in commerce while the realm was at peace as it was for ship

---

[1] David Hume, *The History of England* (Indianapolis, IN: Liberty Fund, Inc., 1983), 185.

[2] "The Circumnavigation, 1577-1580," 2019, The Golden Hind, accessed November 30, 2019, https://goldenhind.co.uk/the-circumnavigation.html.

[3] James A. Wombwell, *The Long War Against Piracy: Historical Trends*, Occasional Paper 32 (Fort Leavenworth, KS: Combat Studies Institute Press, 2010), 3.

owners to accept a charter-party from the admiralty at the outbreak of war.[4] The mercantile marine formed what now is called a naval reserve. Queen Elizabeth actively endorsed privateering during her reign since the crown paid nothing to these mariners during war but gained from their exploits against England's enemies.

When the founding fathers wrote the US Constitution in the eighteenth-century, they intended to have letters of marque and reprisal to supplement the US Navy. Letters of marque are expressly granted in Article 1, Section 8 of the Constitution: "The Congress shall have the power … to declare war, grant letters of marque and reprisal."[5] Even during the American Revolution, the Continental Congress issued 1,738 letters of marque to vessels bearing over 15,803 guns and crewed by over 60,245 seamen to attack the Royal Navy and British commerce vessels.[6] After the war, the authors of the Constitution knew that only by hiring a privateer force during a time of war would the fledgling United States stand a chance against stronger European powers along the Atlantic coast.

During the age of sail, letters of marque and reprisal were a legitimate form of naval warfare, enhancing a state's sea power and disrupting an enemy's economic capacity to wage war. Privateering remained a component of naval warfare until the nineteenth-century. The practice ceased with the enactment of the *Paris Declaration Respecting Maritime Law* during the Congress of Paris of 1856; however, a similar behavior may have recently appeared in the modern era within the cyber domain.[7] Elements of naval warfare during the age of sail may

---

[4] Julian Corbet, *Sir Francis Drake* (1890; repr., Coppell, TX: CreateSpace Independent Publishing Platform, 2016), 9.

[5] US Constitution, art. 1, sec. 8.

[6] Donald Grady Shomette, *Privateers of the Revolution: War on the New Jersey Coast, 1775-1783* (Atglen, PA: Schiffer Publishing, 2016), 11.

[7] Alexander Tabarrok and Alex Nowrasteh, "Privateers! Their History and Future," *Fletcher Security Review* 2, no. 1 (January 2015): 57.

illustrate similarities to contemporary operations in cyberspace, particularly the employment of cyber actors by states to pursue state objectives.

John Gaddis proposes that those who seek a better understanding of the world depend on metaphors, the recognition of patterns, and the realization that something is "like" something else.[8] This monograph compares characteristics of privateering during the age of sail to apply "like" concepts in the cyber domain. This monograph aims to explore how the conceptual understanding of privateers and their relationships to the state generates new understandings of contemporary cases of state-sponsored offensive cyber operations. It then explores the possibility of privateers in cyberspace operating on behalf of American interests.

The argumentative approach of this monograph is analogical. Following the work of Markus Kornprobst, this monograph follows pragmatist methodology to pursue the use of a historical analogy. An analogy can be defined as "a comparison of two otherwise unlike things based on the resemblance of a particular aspect."[9] This paper does not investigate analogy to claim that history repeats itself, but demonstrates how historical concepts can be useful when interpreting contemporary events. This monograph will then apply this methodological framework, created by Kornprobst, against two historical case studies with the first focused on identifying those characteristics of historical maritime privateering, and secondly, applying these characteristics to a recent state-sponsored cyber operation.

Four sections comprise this monograph. The first section of this work is the introduction, which seeks to provide context for this examination, while also introducing key concepts. The introduction also outlines the purpose of the study, definitions, and terminology, and describes the

---

[8] John Gaddis, *Landscape of History: How Historians Map the Past* (New York: Oxford University Press, 2004), 2. Gaddis refers to a literary devise of metaphor, which is a type of an analogy; however, the other analogous literary devise actually associated with the comparison of two "like" things is the simile.

[9] *Merriam-Webster Dictionary*, s.v. "Analogy," accessed January 20, 2020, https://www.merriam-webster.com/dictionary/analogy.

methodology used for this research. The second section consists of an analogical case study, which compares American privateering during the War of 1812 to a contemporary case of Russia-sponsored cyber operations. The third section expounds upon American privateering and analyzes the feasibility of executing cyber privateering operations today. The fourth section concludes the investigation and proposes recommendations for further research.

Definitions and Terminology

To avoid confusion and provide a common understanding, this research outlines definitions of several key concepts discussed throughout the paper. Joint Publication (JP) 3-32, *Joint Maritime Operations*, defines the maritime domain is the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals.[10] This monograph identifies privateers as civilian auxiliaries commissioned by authorized government officials to attack an enemy nation's merchant ships. Governments commissioned privateers through *letters of marque*, which allowed specified individuals to commit what would otherwise be considered criminal acts against targets of specified nationalities for particular offenses.[11] Pirates, on the other hand, preyed on ships from all states for personal gain.[12] The primary difference between privateers and pirates is their ultimate purpose. Since privateers were state-sanctioned, their goal was to protect or strengthen their nation by weakening its enemies' merchant fleets and commercial power.[13]

Joint doctrine defines cyberspace as a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident

---

[10] US Department of Defense, Joint Staff, Joint Publication (JP) 3-32, *Joint Maritime Operations* (Washington, DC: Government Printing Office, 2018), I-5.

[11] Wombwell, *The Long War Against Piracy*, 3.

[12] Wombwell, *The Long War Against Piracy*, 9.

[13] Wombwell, *The Long War Against Piracy*, 10.

data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.[14] Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.[15] Offensive cyber operations are cyberspace operations missions intended to project power in and through foreign cyberspace through actions taken in support of CCDR or national objectives.[16]

Cyberspace exploitation actions include military intelligence activities, maneuvers, information collection, and other enabling actions required to prepare for future military operations. Cyberspace exploitation includes activities to gain intelligence and support operational preparation of the environment for current and future operations through measures such as gaining and maintaining access to networks, systems, and nodes of military value; maneuvering to positions of advantage; and positioning cyberspace capabilities to facilitate follow-on actions.[17] Unlike cyberspace exploitation actions, which often remain clandestine to be effective, cyberspace attack actions will be apparent to system operators or users, either immediately or eventually, since they remove some user functionality.[18] Cyberspace attack actions create noticeable denial effects in cyberspace or manipulation that leads to denial effects in the physical domains.[19]

---

[14] US Department of Defense, Joint Staff, *DOD Dictionary of Military and Associated Terms* (Washington DC, Government Printing Office, 2020), 55.

[15] US Department of Defense, Joint Staff, Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: Government Printing Office, 2018), I-1.

[16] US Joint Staff, JP 3-12 (2018), xi.

[17] US Joint Staff, JP 3-12 (2018), II-6.

[18] US Joint Staff, JP 3-12 (2018), II-7.

[19] US Joint Staff, JP 3-12 (2018), II-7.

Nation-state threats are potentially the most dangerous because of nation-state access to resources, personnel, and time that may not be available to other actors.[20] Nation-states may conduct operations directly or may outsource them to third parties, including front companies, patriotic hackers, or other surrogates, to achieve their objectives.[21] This monograph identifies these third parties as semi-state actors. Non-state threats are formal and informal organizations not bound by national borders, including legitimate nongovernmental organizations (NGOs) and illegitimate organizations such as criminal organizations, violent extremist organizations, or other enemies and adversaries.[22]

Meta-theoretical Perspectives on Historical Analogies

Kornprobst argues that a set of key epistemological assumptions underpin any argument about the usefulness of a historical analogy. He offers three points of view to interpret historical analogies: positivist, post-structuralist, and pragmatist. He contends that the pragmatist perspective is best suited for meta-theoretically sound scrutiny of the usefulness of a particular historical analogy.

Positivists use historical analogies to describe, explain, and predict an objective reality.[23] They believe that the discovery of the truth is possible through correct research methods.[24] This causes several problems when using historical analogies from a positivist research perspective. First, an analogical comparison must involve two very different situations that are not strictly comparable, and second, the data that is relied upon is often produced by actors that do not share

---

[20] US Joint Staff, JP 3-12 (2018), II-11.

[21] US Joint Staff, JP 3-12 (2018), II-11.

[22] US Joint Staff, JP 3-12 (2018), II-11.

[23] Markus Kornprobst, "Comparing Apples and Oranges? Leading and Misleading Uses of Historical Analogies," *Millennium: Journal of International Studies* 36, no. 1 (2007): 33.

[24] Kornprobst, "Comparing Apples and Oranges," 33.

a positivist rule-set for producing the research.[25] Kornprobst contends that the positivist view is problematic because the actual historical fact is the basis from which to build the analogy.

Post-structuralists do not experience this difficulty, though they face other problems. They avoid endorsing particular historical analogies or aspects of them as a useful vocabulary to make sense of the world. Their emphasis is not on making the world intelligible but on deconstructing dominant ways of how the world is made intelligible.[26] For post-structuralists, inquiry lies in the deconstruction of dominant discourses, often using genealogy to do so.[27] Genealogical accounts use analogies as "tools for denaturalizing discursive constructs," divesting from broader, contextual evidence that may provide insight to adjudicate between plausible and implausible analogies.[28] For pro-structuralists, historical analogies are tools for critique, not building blocks of an alternative picture about the world.[29]

Pragmatists, in contrast to positivists, reject claims of objective truth, and in contrast to post-structuralists, are concerned with introducing new analogies that help make the world more intelligible. To pragmatists, the purpose of the inquiry is the generation of useful knowledge.[30] Analogies can be used to gain a better understanding of the world. Useful knowledge is not objectively true, but through open debate and agreement, it comes to constitute a working truth.[31] The pragmatist understanding matches the concepts provided in this monograph. Kornprobst asserts that a historical analogy consists of two building blocks: tenor and vehicle. He claims that

---

[25] Kornprobst, "Comparing Apples and Oranges," 33-34.

[26] Kornprobst, "Comparing Apples and Oranges," 34.

[27] Kornprobst, "Comparing Apples and Oranges," 34.

[28] Kornprobst, "Comparing Apples and Oranges," 34.

[29] Kornprobst, "Comparing Apples and Oranges," 34.

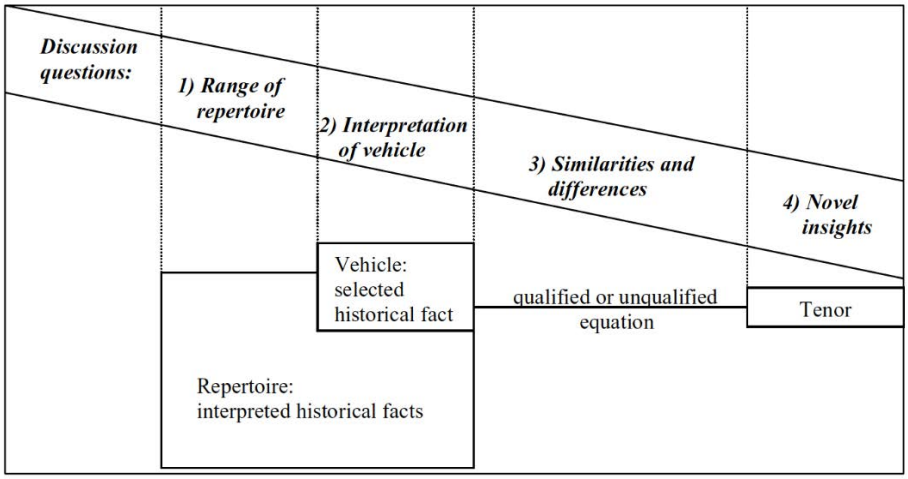
[30] Kornprobst, "Comparing Apples and Oranges," 34.

[31] Kornprobst, "Comparing Apples and Oranges," 34.

the tenor is "the phenomenon that we want to make intelligible to ourselves."[32] The vehicle is an interpretation of a historical event, series of events, or era.[33] The vehicle is selected from a more considerable repertoire of vehicles.[34] The historical analogy makes sense of the tenor in light of the vehicle by equating the former and the latter in a more or less qualified manner. This monograph uses a recent Russia-sponsored cyber operation as its tenor. The vehicle consists of American privateering characteristics during the War of 1812. Building upon a pragmatic epistemological stance, this monograph uses Kornprobst's methodological framework for discussions about historical analogies, see table 1. The framework consists of four questions:

1. What is the range of the repertoire of historical interpretations from which a particular phenomenon is selected as vehicle?
2. How is the vehicle interpreted?
3. What are the similarities and differences between vehicle and tenor?
4. How does the vehicle help us see the tenor in a new light?[35]

Table 1. Methodological Framework for Discussing Historical Analogies



Source: Markus Kornprobst, "Comparing Apples and Oranges? Leading and Misleading Uses of Historical Analogies," *Millennium: Journal of International Studies* 36, no. 1 (2007): 40.

[32] Kornprobst, "Comparing Apples and Oranges," 31.

[33] Kornprobst, "Comparing Apples and Oranges," 31.

[34] Kornprobst, "Comparing Apples and Oranges," 37.

[35] Kornprobst, "Comparing Apples and Oranges," 33.

A Case Study for Historical Analogy

Range of the Repertoire: Privateering during the Age of Sail

The range of the repertoire for this study encompasses privateering during the age of sail. Although privateering provided those involved with the opportunity to obtain wealth, and from the perspective of the state, the primary objective was to weaken its enemies. Privateering complemented mercantilist theory since the destruction of enemy merchant ships reduced competition and, therefore, improved the nation's opportunity for garnering wealth.[36] Adam Smith postulates in *The Wealth of Nations* that "fleets and armies are maintained, not with gold or silver, but with consumable goods. The nation which, from the annual produce of its domestic industry, from the annual revenue arising out of its lands, labor, and consumable stocks, has the wherewithal to purchase those consumable goods in distant countries, can maintain foreign wars there."[37] Smith believed that the ability of a nation to wage war depended on its productive capacity.

Bryan Mabee argues in "Pirates, Privateers and the Political Economy of Private Violence" that piracy and privateering during the age of sail flourished due to the political-economic usefulness of the actors. Pirates and privateers were embedded in a broader political economy of violence which needed and actively promoted "private" violence in a broader pursuit of power, both by newly forming states that relied on naval power and by economic actors who

---

[36] Corbet, *Sir Francis Drake*, 9.

[37] Edward Mead Earl, "Adam Smith, Alexander Hamilton, Fredrich List: The Economic Foundations of Military Power," in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 1986), 221-222.

relied on violence as a form of protection.[38] In the emerging European naval forces, these two aspects went hand in hand, as forms of a mercantilist driven state-building.

Mabee contends that the delegitimization of privateering is the consequence of a number of interlinked political-economic trends, such as the development of public protection of merchant shipping (through the growth of centralized navies), the move away from trade monopolies to inter-imperial trade, and, the gradual development of capitalism and industrialism.[39] To Mabee, the embedding of privateering in a logic of state-building manifested by a mercantilist global economy where plunder and predation were part of the logic of war, but also part of the logic of commerce.[40]

During the 1880s, Captain Alfred Mahan developed a sea power theory to emphasize the United States' potential in the maritime domain. Mahan recognized America's potential to attain great power status at sea and identified the characteristics required to develop and maintain effective maritime operations. The first chapter of *Influence of Sea Power Upon History, 1660-1783*, describes how standing navies existed to protect national commercial interests at sea. Mahan argues that states established navies to protect maritime commerce between coastal bases and colonies abroad.[41] He describes that a commerce-destroying, or *guerre de course*, on the sea was an aspect of maritime warfare that weakened an enemy's economic objectives.[42] *Guerre de course* was directed against usually defenseless merchant vessels by a small amount of military

---

[38] Bryan Mabee, "Pirates, Privateers and the Political Economy of Private Violence," *Global Change, Peace & Security* 21, no 2 (June 2009): 140, accessed January 20, 2020, https://www.doi.org/10.1080/14781150902871994.

[39] Mabee, "Pirates, Privateers and the Political Economy of Private Violence," 140.

[40] Mabee, "Pirates, Privateers and the Political Economy of Private Violence," 140.

[41] Alfred Thayer Mahan, *The Influence of Sea Power Upon History, 1660-1783* (Boston, MA: Little, Brown and Company, 1890), 26, accessed November 23, 2019, http://www.gutenberg.org/files/13529/13529-h/13529-h.htm.

[42] Mahan, *The Influence of Sea Power Upon History*, 8.

force. Nearby ports and harbors provided refuge to would-be privateers to attack these commercial vessels. Navies provided the support to protect these defenseless ships at sea.[43]

In *The Jeune École: The Strategy of the Weak,* Arne Roksund argues that destruction or capture of the enemy's trade was nothing new to maritime warfare. To destroy the enemy's trade has been a critical objective for belligerents since at least the fifteenth-century.[44] The motives were often to cut off supplies essential for the enemy's ability to wage war or to secure them for oneself to improve one's fighting capability.[45] Arne describes that commerce raiding could be conducted in two principally different ways: either the belligerents could organize parts of their navy into squadrons that raided enemy commerce, or this work could be contracted out to private entrepreneurs. He explains that often commerce raiding was conducted by both naval and private raiders.[46] *Guerre de course* was often an option that governments fell back on if the state faced superior opposition against its foe on the sea.[47]

Interpretation of Vehicle: American Privateering in the War of 1812

The vehicle in this study is American privateering during the War of 1812. During this period, privateering was governed by a substantial system of legislation enforced through admiralty courts, prize courts, and bonds. These special mechanisms allowed private means to be dedicated to public wars. Under the "war powers" of Article I, Section 8, Clause 11, the framers of the US Constitution granted Congress the power "to declare war, grant letters of marque and reprisal, and make rules concerning captures on land and water."[48] In essence, letters of marque

---

[43] Mahan, *The Influence of Sea Power Upon History*, 30.

[44] Arne Roksund, *The Jeune École: The Strategy of the Weak* (Leiden, Netherlands: Brill Academic Publishers, 2007), 34, accessed December 20, 2019, http://ebookcentral.proquest.com/lib/carl-ebooks/detail.action?docID=468356/.

[45] Roksund, *The Jeune École*, 34.

[46] Roksund, *The Jeune École*, 35.

[47] Roksund, *The Jeune École*, 34.

[48] US Constitution, art. 1, sec. 8, cl. 11.

allowed specified individuals to commit what would otherwise be considered criminal acts (piracy) against targets of specified nationalities for particular offenses. They also restricted the time, place, and manner of the authorized "reprisal." As a fledgling nation, the US Government lacked funds with which to build a large navy and relied on privateers to protect its coasts and trade routes. International disputes required the United States to invoke forms of economic sanctions, including the granting of authority through letters of marque and reprisal to protect its maritime commercial enterprise. Because of this, privateering was critical for the American effort during the war.

Congress declared war on Great Britain on June 18, 1812, and began to issue letters of marque and reprisal.[49] On June 26, 1812, Congress followed its declaration of war with greater detail on how privateers would be regulated.[50] During this period, acquiring a privateer's license, called a commission, was the first step required by law in outfitting a privateer. Without a commission and oversight by a court, the privateer could not sell its prizes. A privateer's license was recognized as valid by courts throughout the world.

When a privateer captured a valuable prize, it was operated by a prize master and crew and instructed to set sail for the nearest friendly port. From the moment a prize arrived, its new owners were subject to rules regulating how they profited from the ship and its holdings. The privateer relied on the captured ship's papers, and the court would question the prize's captured

---

[49] Annals of Congress, 12th Cong., 1st sess.,1812, pt. Appendix: 2322-2323, accessed January 22, 2020, http://memory.loc.gov/cgi-bin/ampage?collId=llac&fileName=024/llac024.db&recNum=570&itemLink=r%3Fammem%2Fhlaw%3A%40field%28DOCID%2B%40lit%28ac0241%29%29%230240594&linkText=1. The act referenced in this note, An Act Declaring War Between the United Kingdom of Great Britain and Ireland and the Dependencies Thereof, and the United States of America and Their Territories, is the authoritative guidance by the 12th Congress to issue commissions of marque and reprisal to private, armed United States vessels during this conflict with Great Britain and associated states.

[50] Annals of Congress, 12th Cong., 1st sess.,1812, pt. Appendix: 2327-2328. The act referenced in this note, An Act Concerning Letter-of-Marque, Prizes, and Prize Goods, explains the legal details and procedures for documenting and managing those agents who would be issued Letters-of-Marque.

officers, crew, and passengers.[51] If the prize was found to be lawful, the court could order the owners of the privateer to pay restitution to those harmed by the capture.[52] Taxes, duties, and payments to auctioneers typically absorbed half the value of a prize, but the crew could still profit handsomely. While privateering was a high-risk, high-reward profession for crew members, a privateering venture's financial backers could obtain consistent returns.

Congress required privateers to respect the persons, property, and ships of neutral nations and legislated to incentivize the proper treatment of neutrals.[53] Privateers often were required to pay a performance bond, a financial instrument whereby the purchaser forfeits the value if he violates the rules of the agreement. The performance bond ensured that privateers would follow the rules laid down by Congress and the law of nations or face a sizeable financial penalty—the value of the bond.[54] Also, the privateering ship itself was a form of collateral that could be sold by the courts to pay an adverse judgment.[55] The letter of marque contained regulations and articulated the recipient's duties and responsibilities; the bond linked the recipient's profit motivation to those obligations.

If the crew was short and the prize was far from a friendly port, the privateer could ransom the captured ship back to its captain, who would agree on behalf of the prize's owners to pay the ransom at a later date. The privateer would then release the prize and crew with papers that guaranteed the prize's safety if intercepted by another American privateer. The ransom took the form of a bond—a promise from the owners of the ship to the privateer, with the captain of

---

[51] Tabarrok and Nowrasteh, "Privateers! Their History and Future," 56.

[52] Annals of Congress, 12th Cong., 1st sess.,1812, pt. Appendix: 2327-2328.

[53] Annals of Congress, 12th Cong., 1st sess.,1812, pt. Appendix: 2327-2328.

[54] Tabarrok and Nowrasteh, "Privateers! Their History and Future," 56.

[55] Tabarrok and Nowrasteh, "Privateers! Their History and Future," 56.

the merchant ship as the surety.[56] Ransoms were contracts enforceable in courts. If a merchant refused to pay a ransom, his ship could be legally seized by the privateer in foreign ports through a process called repossession.[57] Privateers often took a hostage, usually the captain of the ship or another officer, who would be released after the ransom was paid.[58] For privateers, the reliability of ransom as a business option reduced the relative attractions of violence, mitigating the loss of life, and the destruction of property. Those same benefits also accrued to enemy merchants, who easily preferred ransom costs to the destruction of property.

A privateer would parole a vessel of too low a commercial value to be worth sending back to port as a prize, allowing the crew of the captured ship to go free along with prisoners from previous prizes. The advantages of parole were many. For privateers, granting parole could increase the length and range of cruises. For enemy merchants, parole decreased the costs of being captured but still imposed a significant burden. States, however, had to balance the greater freedom afforded its privateers versus the fact that parole did not decrease the supply of sailors available to the enemy.[59]

The vehicle provides valuable insight into the conceptual understanding of privateers and their relation to the state. This monograph deduces three fundamental relationships from American privateering operations during the War of 1812: (1) privateering allowed the US Government to recruit skilled personnel to enhance its maritime capability against enemies; (2) privateering was an economic venture, diminishing the commerce capacity of a declared enemy state, while incentivizing the privateer and the United States with potential profit from prizes and

[56] Tabarrok and Nowrasteh, “Privateers! Their History and Future,” 56.

[57] Tabarrok and Nowrasteh, “Privateers! Their History and Future,” 56.

[58] Tabarrok and Nowrasteh, “Privateers! Their History and Future,” 56.

[59] Tabarrok and Nowrasteh, “Privateers! Their History and Future,” 57.

tax revenue; and (3) the state provided the administrative processes to commission privateers and arbitrate the prizes. This paper will use these characteristics to evaluate the tenor.

The Tenor: A Case of Russia-Sponsored Cyber Actors

For years, American intelligence officials tracked numerous Russian state-sponsored hacking units as they successfully penetrated the computer networks of critical infrastructure operators across North America and Europe.[60] Research has uncovered several sub-pockets of the cybercriminal underworld that could not continue to exist, were there not, at least tacit, support from Russian state officials.[61] Many analysts have pointed to the political enablement of Russian cybercrime. Supporting evidence for this is how cybercriminals have become active in Russian political interests and engage in selective targeting, deliberately avoiding touching on Russian law enforcement interests.[62] A recent indictment by the US Justice Department documents a joint operation between Russian government officials and Russian hackers that closely resembles privateering-like structures.

In 2017, the US Justice Department indicted Russian Federal Security Service (FSB) officers Dmitry Aleksandrovich Dokuchaev and Igor Anatolyevich Sushchin, as well as career cybercriminals, Alexsey Alexseyevich Belan and Karim Baratov, for hacking Yahoo Inc. and

---

[60] Andrew E. Kramer, "How Russia Recruited Elite Hackers for Its Cyberwar," *The New York Times*, December 29, 2016, accessed November 30, 2019., https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elitehackers-for-its-cyberwar.html/.

[61] Mark Galeotti, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*, (London, UK: European Council on Foreign Relations, 2017), 2, accessed January 20, 2020, https://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

[62] Nikolas K. Gvosdev, "The Bear Goes Digital: Russia and Its Cyber Capabilities," in *Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 180.

other webmail providers between 2014 and 2016.[63] According to the allegations of the indictment, the FSB officer defendants, Dokuchaev and Sushchin, protected, directed, facilitated, and paid the criminal hackers to collect information through computer intrusions in the United States and elsewhere. They worked with co-defendants Alexsey Belan and Karim Baratov to obtain access to the email accounts of thousands of individuals.[64] The Justice Department charged the four men with several offenses, including conspiracy to commit economic espionage, theft of trade secrets, and a range of *Computer Fraud and Abuse Act* (CFAA) offenses. The indictment shed light on the level of collaboration between criminal hackers and FSB officers, who worked for the FSB Center for Information Security.[65]

The defendants used unauthorized access to Yahoo's systems to steal information from about at least 500 million Yahoo accounts and then used some of that stolen information to obtain unauthorized access to the contents of accounts at Yahoo, Google, and other webmail providers, including accounts of Russian journalists, US and Russian government officials and private-sector employees of financial, transportation and other companies. Baratov even exploited his access to Yahoo's network for his financial gain, by searching Yahoo user communications for credit card and gift card account numbers, redirecting a subset of contracts of at least 30 million Yahoo accounts to facilitate a spam campaign.[66]

Previously, the Federal Bureau of Investigation issued an Interpol red notice (arrest alert) for Belan in 2012, but he escaped and subsequently traveled to Russia. Instead of acting on the

---

[63] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," press release no. 17-278, March 15, 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions/.

[64] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

[65] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

[66] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

US Government's Red Notice and detaining Belan after his return, Dokuchaev and Sushchin subsequently used him to gain unauthorized access to Yahoo's network. By the end of December 2014, Belan stole a copy of at least a portion of Yahoo's user database (UDB), a Yahoo trade secret that contained, among other data, subscriber information including users' names, recovery email accounts, phone numbers and certain information required to manually create account authentication web browser "cookies" for more than 500 million Yahoo accounts. Belan also obtained unauthorized access on behalf of the FSB conspirators to Yahoo's account management tool (AMT), which Yahoo uses to make alterations to user accounts. Belan, Dokuchaev, and Sushchin then used the stolen UDB copy and AMT access to locate Yahoo email accounts of interest and to create cookies for those accounts, enabling the co-conspirators to access at least 6,500 such accounts without authorization.[67]

According to the inditement, the FSB officers facilitated Belan's other criminal activities, by providing him with sensitive FSB law enforcement and intelligence information that would have helped him avoid detection by the United States and other law enforcement agencies outside Russia, including information regarding FSB investigations of computer hacking and FSB techniques for identifying criminal hackers.[68] Additionally, while working with his FSB conspirators, Belan used his access to steal financial information such as gift card and credit card numbers from webmail accounts, gain access to more than 30 million accounts whose contacts were then stolen, and earn commissions from fraudulently redirecting a subset of Yahoo's search engine traffic.[69]

---

[67] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

[68] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

[69] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

When Dokuchaev and Sushchin learned that a target of interest had accounts at webmail providers other than Yahoo, including through information obtained as part of the Yahoo intrusion, they tasked their co-conspirator, Baratov, a resident of Canada, with obtaining unauthorized access to more than eighty accounts in exchange for commissions.[70] Compared to the operation with Belan, these webmail hacking assignments were more transactional in purpose. The FSB officers tasked Baratov with specific e-mail addresses, which he would then acquire the credentials for, usually through spear-phishing. In return, the FSB paid him Can $100 per account.[71]

Baratov kept a large online footprint by marketing his services online on various websites, kept an active social media profile, and used his substantial income on luxury cars.[72] Living in Canada, and as the only member of the conspiracy outside of Russia, the twenty-two-year-old was arrested by the Canadian police in March 2017. Canada extradited Baratov to the United States on November 28, 2017, Baratov pleaded guilty and admitted to his role in the conspiracy.[73] Baratov pleaded guilty to one count of conspiracy to commit computer fraud and abuse, and eight counts of aggravated identity theft and is currently serving a five-year sentence.[74] As a part of his plea agreement, Baratov not only admitted to agreeing and attempting

---

[70] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

[71] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

[72] US Department of Justice, "International Hacker-For-Hire Who Conspired with and Aided Russian FSB Officers Sentenced to 60 Months in Prison," press release no. 18-703, May 29, 2018, accessed January 20, 2020, https://www.justice.gov/opa/pr/international-hacker-hire-who-conspired-and-aided-russian-fsb-officers-sentenced-60-months/.

[73] US Department of Justice, "Canadian Hacker Who Conspired with and Aided Russian FSB Officers Pleads Guilty," press release no.17-1341, November 28, 2017, assessed January 20, 2020, https://www.justice.gov/opa/pr/canadian-hacker-who-conspired-and-aided-russian-fsb-officers-pleads-guilty/.

[74] US Department of Justice, "International Hacker-For-Hire Who Conspired with and Aided Russian FSB Officers Sentenced to 60 Months in Prison."

to hack at least eighty webmail accounts on behalf of one of his FSB co-conspirators, but also to hacking more than 11,000 webmail accounts in total from 2010 until his arrest by Canadian authorities in March 2017.[75] This case may substantiate a privateering-like structure that incorporates Russian cybercrime and departments within the Russian government.

Similarities and Differences Between the Vehicle and Tenor

Evidence provided in both the vehicle and tenor demonstrates that semi-state actors increased a state's capacity against adversaries. When the United States went to war against Britain in June 1812, the US Navy had about fifteen warships in commission.[76] Throughout the war, US Navy warships captured approximately 250 vessels, but American privateers took at least five times the number of British merchant vessels—at least 1,200.[77] The tenor demonstrates that the FSB officers also employed Belan and Baratov for a critical capability: their cyber expertise. Several accounts substantiate that Russia hires skilled hackers from criminal networks, sometimes under threat of a court case.[78] Rather than rely on military personnel working out of isolated bunkers, Russian government recruiters have scouted a wide range of programmers, placing prominent ads on social media sites, offering jobs to college students and professional coders, and even speaking openly about looking in Russia's criminal underworld for potential talent.[79] Unlike the vehicle, however, Dokuchaev and Sushchin directed Belan and Baratov not to

---

[75] US Department of Justice, "Canadian Hacker Who Conspired with and Aided Russian FSB Officers Pleads Guilty."

[76] Frederick C. Leiner, "Yes, Privateers Mattered," *Naval History Magazine* 28, no. 2 (March 2014): 18, accessed January 20, 2020, https://www.usni.org/magazines/naval-history-magazine/2014/march/yes-privateers-mattered/.

[77] Leiner, "Yes, Privateers Mattered," 18.

[78] Kramer, "How Russia Recruited Elite Hackers for Its Cyberwar."

[79] Kramer, "How Russia Recruited Elite Hackers for Its Cyberwar."

target a declared adversary, but instead to collect information on Russian journalists, US and Russian government officials and private-sector employees for intelligence purposes.[80]

The vehicle demonstrates that American privateering during the War of 1812 was an economic venture, diminishing the commerce capacity of Britain while incentivizing the privateer and the US with potential profit from prizes and tax revenue. When a privateer captured a valuable prize, a prize master and crew operated it and set sail for the nearest friendly port. A court would then verify the lawfulness of the prize.[81] Once auctioned, the US Government received taxes and duties on the prize, and the privateer received the remaining value as profit. In contrast to the vehicle, the tenor depicts an exchange between the FSB officers and the cyber actors for services rendered. The cyber exploitation operations executed by Belan and Baratov appear to be symbiotic with respect to Russian government objectives. Belan gained from the protection and information that the FSB officers allegedly provided him to elude law enforcement officers, as all as the tacit support to steal financial information, gain access to more than 30 million accounts, and earn commissions from fraudulently redirecting a subset of Yahoo's search engine traffic.[82] Dokuchaev and Sushchin paid Baratov Can $100 for each webmail account he hacked.[83] Unlike the vehicle, which explains that US-sanctioned privateers attacked an enemy's commerce capacity, the tenor does not demonstrate this behavior. Belan and Baratov executed cyber exploitation operations against multiple targets across the world, not an enemy of Russia.

The vehicle also demonstrates the US provided the administrative processes to commission privateers and arbitrate the prizes during the War of 1812. Congress granted

---

[80] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

[81] Tabarrok and Nowrasteh, "Privateers! Their History and Future," 56.

[82] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

[83] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

commissions to authorize the seizure of prizes on the sea. These commissions were tools to deputize and regulate private actors operating internationally as agents of the state. In the military context, the intent behind the letter of marque was for governments to retain control over commissioned vessels while simultaneously expanding military capabilities. When privateers exceeded their commission, they were no longer under the governmental authority and could be treated like criminals. US privateering courts arbitrated prizes once privateers returned from sea to verify the seizure's legality.

The tenure does not demonstrate the administrative structure that the vehicle depicts. The indictment does not provide any information about the contractual relationship between the FSB officers and Belan. From the information provided in the indictment, it is conceivable that the two FSB officers assisted Belan to avoid arrest in return for providing his cyber expertise, and there is no indication of how voluntary such an agreement might have been. Baratov's case depicts that Dokuchaev and Sushchin informally contracted him as a hacker-for-hire to execute targeted cyber exploitation operations against specified targets.[84]

Novel Insights About the Tenor

Privateering was an accepted institution during the age of sail.[85] The practice had evolved over centuries, and European powers accepted the behavior as an aspect of naval warfare. Letters of marque and reprisal, granted since the twelfth century, were designed to transform the anarchy of retaliation in war into lawful methods of seeking restitution.[86] The state provided the administrative infrastructure to enable privateering operations, issuing letters of marque and

---

[84] US Department of Justice, "International Hacker-For-Hire Who Conspired with and Aided Russian FSB Officers Sentenced to 60 Months in Prison."

[85] Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (New York, NY: Doubleday, 1966), 72. Berger and Luckman expound upon the development of institutions in social context, describing that institutionalization occurs whenever there is a reciprocal typification of habitualized actions by types of actors.

[86] Tabarrok and Nowrasteh, "Privateers! Their History and Future," 56.

reprisal to raid enemy ships during wartime or periods of heightened international tensions, and creating a legal system to arbitrate and tax seized prizes. These special mechanisms allowed private means to be dedicated to public wars and increased the state's naval capacity against its enemies.

The tenor does not demonstrate that such an institution exists in cyberspace. Rather, the evidence depicts that both Belan and Baratov were semi-state actors hired by Dokuchaev and Sushchin to conduct cyber exploitation operations on behalf of the Russian government. Belan used the information and resources provided by the two FSB officers to not only execute operations on behalf of the Russian government but for personal gain. The Russian officials were likely aware of Belan's profiteering efforts but did not enforce laws that would have prevented him from executing those operations.[87] Both Dokuchaev and Sushchin paid Baratov for each webmail account he exploited on behalf of the FSB.

The analogy of privateering proves to be most similar to Belan's relationship to Dokuchaev and Sushchin. As the indictment case shows, the FSB likely benefited from the intelligence value of Belan's cyber operations. Belan benefited from the Russian government's efforts to help him evade capture from international authorities and personally profit from the resources provided by the FSB. Unlike privateering, however, there is no evidence that the FSB or Russian government commissioned Belan to specifically execute offensive cyber operations against Russian adversaries to diminish their economic capacity. It appears that Belan's profiteering operations were instead targets of opportunity.

[87] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

US Privateers in Cyberspace

The Congress of Paris abolished privateering as a naval practice following the Crimean War in 1856, enacting the *Paris Declaration Respecting Maritime Law*. The law named Britain, the dominant sea power at the time, to commit to the protection of neutral commerce. In return, other powers relinquished the right to privateering. The settlement also represented a move against the United States, which still relied on turning its large merchant cruisers into privateers in case of naval conflict.[88] To this day, the US Government has never signed the agreement, and the letters of marque and reprisal clause still exist in the US Constitution. This section answers the question, can the US Government commission cyber privateers in the current operating environment?

Current United States Policy for Operational Contract Support

Privateering commissions were tools to deputize and regulate private actors operating internationally as agents of the state. Contemporary contractual interactions between private military companies and the US Government may offer a similar association. Title 32 of the United States *Code of Federal Regulations* (CFR) is the principal set of rules and regulations issued by federal agencies of the United States regarding national defense. Part 158 of Title 32 outlines the policy, assigns responsibilities, and provides procedures for Operational Contract Support (OCS), including OCS program management, contract support integration, and integration of defense contractor personnel into contingency operations outside the United States.[89]

---

[88] Jan Martin Lemnitzer, *Power, Law and the End of Privateering* (Basingstoke, UK: Palgrave Macmillan, 2014), 48-51.

[89] "Operational Contract Support," *Code of Federal Regulations*, title 32, sec. 158 (2020).

Title 32 defines a contingency contract as a legally binding agreement for supplies, services, and construction let by government contracting officers in the operational area, as well as other contracts that have a prescribed area of performance within a designated operational area.[90] Contingency contractor personnel are the individual contractors, individual subcontractors at all tiers, contractor employees, and sub-contractor employees at all tiers under all contracts supporting the military services during contingency operations.[91]

According to Title 32, the US government may utilize contracted services in applicable contingency operations for all functions that are not inherently governmental. US forces operating in such operations must designate these contractors as "contractors authorized to accompany the force" (CAAF) and provide these contractors with an appropriate identification card pursuant to the Geneva Convention Relative to the Treatment of Prisoners of War.[92] CAAF status does not apply to contractor personnel supporting domestic contingencies.[93]

The regulation explains what type of contract support may be applicable to combat operations. Contractor personnel may support appropriate contingency operations such as by providing communications support, transporting munitions and other supplies, performing maintenance functions for military equipment, providing private security services, providing foreign language interpretation and translation services, and providing logistic services such as billeting and messing.[94] The US government prohibits contractors from conducting offensive military operations. When armed for personal protection, contingency contractor personnel are only authorized to use force for individual self-defense. Unless immune from local jurisdiction by

---

[90] "Operational Contract Support," CFR, title 32, sec. 158 (2020).

[91] "Operational Contract Support," CFR, title 32, sec. 158 (2020).

[92] "Operational Contract Support," CFR, title 32, sec. 158 (2020).

[93] "Operational Contract Support," CFR, title 32, sec. 158 (2020).

[94] "Operational Contract Support," CFR, title 32, sec. 158 (2020).

an international agreement or international law, the contract shall include language advising contingency contractor personnel that the inappropriate use of force could subject them to the United States and local prosecution, as well as civil liability.[95]

Current United States Policy for Private Security Contractors

While Part 158 offers insight on operational contract support, Part 159 of Title 32 establishes policy, assigns responsibilities, and provides procedures for the regulation of the selection, accountability, training, equipping, and conduct of personnel performing private security functions under a covered contract. It also assigns responsibilities and establishes procedures for incident reporting, use of and accountability for equipment, rules for the use of force, and a process for administrative action or the removal, as appropriate, of Private Security Contractors (PSCs) and their personnel.[96] During contingency operations, a PSC is a company employed by the Department of Defense (DoD) performing private security functions. In a designated area of combat operations or other significant military operations, the term "PSC" expands to include all companies employed by US Government agencies performing private security functions under a covered contract.[97]

The selection, training, equipping, and conduct of PSC personnel, including the establishment of appropriate processes, shall be coordinated between the DoD and the Department of State. Part 159 mandates that coordination shall encompass the contemplated use of PSC personnel during the planning stages of contingency operations so as to allow guidance to be developed. Geographic combatant commanders will provide tailored PSC guidance and procedures for the operational environment in their area of responsibility (AOR). In a designated

---

[95] "Operational Contract Support," CFR, title 32, sec. 158 (2020).

[96] "Private Security Contractors Operating in Contingency Operations," *Code of Federal Regulations*, title 32, part 159 (2020).

[97] "Private Security Contractors Operating in Contingency Operations," CFR, title 32, sec. 159 (2020).

area of combat operations or other significant military operations, the relevant chief of mission will be responsible for developing and issuing implementing instructions for non-DoD PSCs and their personnel consistent with the standards set forth by the geographic combatant commander. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01B guides the standing rules of engagement and establishes standing rules for the use of force for DoD operations worldwide, to include PSC personnel.[98]

Inherently Governmental Responsibilities

The sociologist and political economist Max Weber defined the state as having a monopoly on the legitimate use of physical force.[99] He emphasized that a primary concern overusing any type of private security in the modern era is the argument that their military-like service is inherently governmental.[100] This argument posits that governments should have a monopoly on the military profession and national security. Peter Singer warns that when a state privatizes a sovereign function and transfer that power to private entities, the state is forever expatriated as the sole legitimate right to force and organized violence. An important precedent has taken place. PSCs simultaneously strengthen the state as they disassemble them.[101]

Department of Defense Instruction (DODI) 1100.22, *Policy and Procedures for Determining Workforce Mix*, establishes policy, assigns responsibilities, and prescribes

---

[98] Chairman of the Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces* (Washington, DC: Government Printing Office, 2005), 1, accessed January 20, 2020, https://www.jag.navy.mil/distrib/instructions/CJCSI%203121.01B13Jun05.pdf. CJCSI 3121.01B outlines the standing rules of engagement and establishes standing rules for the use of force for DoD operations. For security purposes, the US government classifies CJCSI 3121.01B (2018) as secret.

[99] Max Weber, *The Theory of Social and Economic Organization*, ed. Talcott Parsons, trans. Talcott Parsons and A. M. Henderson (1948; repr., New York, NY: The Free Press, 1964), 315.

[100] Weber, *The Theory of Social and Economic Organization*, 154.

[101] Peter W. Singer, "Corporate Warriors: The Rise and Ramifications of the Privatized Military Industry," *International Security* 26, no. 3 (Winter 2001-2002): 187, accessed January 20, 2020, https://www.jstor.org/stable/i355580/.

procedures for determining the appropriate mix of the workforce (military and DoD civilian) and private sector support.[102] Most importantly, DODI 1100.22 provides guidance on which workforce actions are inherently governmental and which can be performed by private entities. Its guidance distinctly summaries the role of government actions in combat.

Outlined by DODI 1100.22, combat operations authorized by the US Government are inherently governmental and designated for military execution. The US Government has exclusive responsibility for discretionary decisions concerning the appropriate, measured use of combat power, including the offensive use of destructive or deadly force on behalf of the United States. Combat operations authorized by the US Government entail the exercise of sovereign government authority and involve substantial discretion.[103] The appropriate, measured use of combat power during hostilities is of critical national interest.

DODI 1100.22 explains that under certain circumstances, the United States can be liable for its misuse or compelled to make restitution due to its unintended collateral effects. The Department of Defense safeguards US sovereign authority and reduces the risk of misusing destructive or disruptive force by delegating responsibility for combat operations only to military commanders through the military chain of command and holding military commanders and their forces accountable for the appropriate and controlled use of combat power and adherence to rules of engagement and the law of war.[104] Because of these mitigation measures, the US Government will not delegate responsibility for combat operations to private entities.

---

[102] US Department of Defense, Under Secretary of Defense for Personnel and Readiness, Department of Defense Instruction (DODI) 1100.22, Change 1, *Policy and Procedures for Determining Workforce Mix* (Washington, DC: Government Printing Office, 2017), 1.

[103] US Department of Defense, USD (P&R), DODI 1100.22, Change 1, 1.

[104] US Department of Defense, USD (P&R), DODI 1100.22, Change 1, 1.

DODI 1100.22 states explicitly that the planned use of destructive combat capabilities is part of the mission assigned to this organization (including destructive capabilities involved in offensive cyber operations, electronic attack, missile defense, and air defense) is inherently governmental. The *Federal Activities Inventory Reform Act of 1998* defines that an inherently governmental function is "a function so intimately related to the public interest as to require performance by Federal Government employees."[105] Inherently governmental functions include manpower located both inside and outside a theater of operations if the personnel operate a weapon system against an enemy or hostile force (e.g., bomber crews, inter-continental ballistic missile crews, and unmanned aerial vehicle operators). DODI 1100.22 allows the private sector to provide technical advice on the operation of weapon systems or other support of a non-discretionary nature performed in direct support of combat operations.[106]

DODI 1100.22 warns that activities closely associated with inherently governmental functions may become inherently government because of the way they are performed or the circumstances under which they are performed. Decisions as to whether a function is inherently government should emphasize the degree to which the conditions or facts restrict or put at risk the discretionary authority, decision-making responsibility, or accountability of Defense officials. When an activity is so closely associated with an inherently governmental function that it cannot be separated or distinguished from the inherently governmental function, it should be identified as inherently governmental to preclude transferring governmental authority, responsibility, or accountability to the private sector.[107]

---

[105] Federal Activities Inventory Reform Act of 1998, Public Law 105-270, *US Statutes at Large* 112 (1998): 2382-2385.

[106] US Department of Defense, USD (P&R), DODI 1100.22, Change 1, 19.

[107] US Department of Defense, USD (P&R), DODI 1100.22, Change 1, 19.

Computer Fraud and Abuse Act

The CFAA was enacted in 1986 as an amendment to the first federal computer fraud law to address computer hacking. The law amended Section 1030, Title 18 of the US Code, which Congress had previously established in 1984 to address federal computer-related offenses.[108] In addition to clarifying a number of the provisions in the original Section 1030, the CFAA Broadened the definition of "protected computer" to the full extent of Congress's commerce power by including those computers used in or affecting interstate or foreign commerce or communication. Because of this, the measure effectively bans any future cyber privateering operations.

The law identifies the term "computer" as an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such equipment. The term "protected computer" means a computer exclusively for the use of a financial institution or the US Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the US Government and the conduct constituting the offense affects that use by or for the financial institution or the government; or which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.[109]

---

[108] US Department of Justice, Computer Crime and Intellectual Property Section, *Prosecuting Computer Crimes: Computer Crime and Intellectual Property Section Criminal Division*, OLE Litigation Series, ed. Scott Eltringham, 2nd ed. (Washington, DC: Executive Office for United States Attorneys, 2010), 1-3, accessed January 20, 2020, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[109] Fraud and Related Activity in Connection with Computers, *US Code 18* (1984), § 1030, Legal Information Institute, Cornell Law School, accessed January 19, 2020, https://www.law.cornell.edu/uscode/text/18/1030/.

In 2008, Congress amended the definition of "protected computer" to make clear that this term includes computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States."[110] The changes to 18 USC § 1030(e)(2)(B) (2001) address situations where an attacker within the United States attacks a computer system located abroad and situations were individuals in foreign countries route communications through the United States as they hack from one foreign country to another.[[111] Therefore, both situations can be violations of Section 1030.

The CFAA prohibits any individual or organization from knowingly or unintentionally accessing a protected computer without authorization, and as a result of such conduct, causes damage. It also outlaws the trafficking of passwords and similar information relating to interstate trade or foreign commerce with the intent to defraud and criminalizes cyber extortion.[112] The current version of the CFAA includes seven types of criminal activity, outlined in table 2.

Table 2. Summary of CFAA Penalties

Offense	Section	Sentence*
Obtaining National Security Information	(a)(1)	10 (20) years
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 (10)
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 (20)
Negligently Causing Damage & Loss by Intentional Access	(a)(5)(C)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Computers	(a)(7)	5 (10)

* The maximum prison sentences for second convictions are noted in parentheses.

Source: US Department of Justice, Computer Crime and Intellectual Property Section, *Prosecuting Computer Crimes: Computer Crime and Intellectual Property Section Criminal Division*, OLE Litigation Series, ed. Scott Eltringham, 2nd ed. (Washington, DC: Executive Office for United States Attorneys, 2010), 3, table 1, accessed January 20, 2020, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

---

[110] US Department of Justice, Computer Crime and Intellectual Property Section, *Prosecuting Computer Crimes*, 4.

[111] US Department of Justice, Computer Crime and Intellectual Property Section, *Prosecuting Computer Crimes*, 4.

[112] Fraud and Related Activity in Connection with Computers, *US Code 18* (1984), § 1030.

The Issue with Pillaging

During the age of sail, letters of marque and reprisal allowed privateers to pillage enemy commerce ships on behalf of the issuing sovereign. When a privateer captured a valuable prize, a prize master and crew operated it and set sail for the nearest friendly port. From the moment a prize arrived, its new owners were subject to rules regulating how they profited from the ship and its holdings. The cargo and ship could not be legally disturbed until the privateer had proven in a court of law that the vessel was owned by the enemy.[113] The privateer relied on the captured ship's papers, and the court would question the prize's captured officers, crew, and passengers. If the prize was found to be lawful, it was sold in a court-ordered auction.[114]

Rules of warfare, however, have changed since then. Rule 52 of the customary International Humanitarian Law (IHL) specifies that pillaging is prohibited. Pillage (or plunder) defined as "the forcible taking of private property by an invading or conquering army from the enemy's subjects."[115] The International Criminal Court's (ICC) publication, *Elements of Crimes*, specifies that pillaging occurs when a "perpetrator intends to deprive the owner of property and to appropriate it for his private or personal use."[116] As such, the prohibition of pillage is a specific application of the general principle of law prohibiting theft. This prohibition is to be found in national criminal legislation around the world. Pillage is generally punishable under military law or general penal law.

---

[113] Tabarrok and Nowrasteh, "Privateers! Their History and Future," 56.

[114] Tabarrok and Nowrasteh, "Privateers! Their History and Future," 56.

[115] *Black's Law Dictionary*, s.v. "Pillage," 1033.

[116] International Criminal Court, "Article 8 (2) (b) (xvi)," in *Elements of Crime* (The Hague, Netherlands: International Criminal Court, 2011), 26, https://www.icc-cpi.int/NR/rdonlyres/336923D8-A6AD-40EC-AD7B-45BF9DE73D56/0/ElementsOfCrimesEng.pdf; International Criminal Court, "Article 8 (2) (e) (v)," in *Elements of Crime* (The Hague, Netherlands: International Criminal Court, 2011), 36, https://www.icc-cpi.int/NR/rdonlyres/336923D8-A6AD-40EC-AD7B-45BF9DE73D56/0/ElementsOfCrimesEng.pdf.

Pillage is also prohibited under all circumstances under the Hague regulations.[117] Pillage is identified as a war crime in the *Report of the Commission on Responsibility* set up after the First World War, as well as by the Charter of the International Military Tribunal of Nuremberg established following the Second World War.[118] The Fourth Geneva Convention also prohibits pillaging.[119] Under the Statute of the International Criminal Court, "pillaging a town or place, even when taken by assault," constitutes a war crime in international armed conflicts.[120]

Legal Assessment

Though the Constitution empowers Congress to grant letters of marque, current domestic and international laws prevent the employment of cyber privateers by the US Government. Title 32 allows the federal government to hire both OSCs and PSCs to support combat operations, but both are unauthorized to perform inherently government functions. DODI 1100.22 further clarifies that operating a weapon system against an enemy or hostile force is an inherently

---

[117] International Peace Conference, The Hague, *Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907*, January 26, 1910, Article 28, accessed January 22, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/195-200038?OpenDocument; International Peace Conference, The Hague, *Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907*, January 26, 1910, Article 47, accessed January 22, 2020, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=FA13E789FD4EAFF0C12563CD005168CC.

[118] United Nations, *Report of the Commission on the Responsibility of the Authors of the [First World] War and on Enforcement of Penalties, March 29, 1919*, 159, accessed January 20, 2020, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1917&context=ils; United Nations, *United Kingdom of Great Britain and Northern Ireland, United States of America, France, Union of Soviet Socialist Republics: Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, Signed at London, August 8, 1945*, Article 6 (b), 288, accessed January 20, 2020, https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.2_Charter%20of%20IMT%201945.pdf.

[119] International Committee of the Red Cross, *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 12 August 1949*, October 21, 1950, 75 U.N.T.S. 287, Article 33, 180, accessed January 22, 2020, https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=AE2D398352C5B028C12563CD002D6B5C.

[120] International Criminal Court, "Article 8 (2) (b) (xvi)," 26.

governmental responsibility. The CFAA prevents the employment of cyber privateers since the law prohibits individuals and organizations from attacking "protected computers" abroad. Seizing prizes from enemies during cyber privateering operations qualify as pillaging, which the IHL, ICC, Hague regulations, and the Fourth Geneva Convention specifically prohibit in combat operations. Under the current construct of international and domestic regulations and laws, US privateering is unfeasible in the cyber domain.

US-sponsored privateers would also violate national cyber policy objectives. The *National Cyber Strategy of the United States of America* explains that the United States will promote a framework of responsible state behavior in cyberspace built upon international law, adherence to voluntary, non-binding norms of responsible state behavior that apply during peacetime, and the consideration of practical confidence-building measures to reduce the risk of conflict stemming from malicious cyber activity.[121] It further describes how principles should form a basis for cooperative responses to counter irresponsible state actions inconsistent with this framework.[122] The inherent nature of seizing prizes from privateering operations is against international law, and thus, incompatible with US national policy.

Conclusion and Recommendations

During the age of sail, naval powers issued privateering licenses to shipowners, allowing and encouraging them to raid enemy commerce during periods of war. Privateering provided those involved with the opportunity to obtain wealth by seizing bounty from enemy vessels and supporting the national interests of the sovereigns that hired them. This monograph followed a pragmatist methodology to pursue the use of a historical analogy and compare characteristics of privateering to a recent Russia-sponsored cyber operation. The indictment of Dokuchaev,

---

[121] Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, 2018), 20.

[122] Trump, *National Cyber Strategy of the United States of America*, 20.

Sushchin, Belan, and Baratov demonstrates an example of semi-state actors acting on behalf of state interests. The privateering analogy proves to be most similar to Belan's relationship with elements of the Russian government. The FSB benefited from the intelligence value of Belan's cyber operations, and Belan benefited from the Russian government's efforts to help him evade capture and profit from the resources provided by the FSB. Unlike privateering, however, there is no evidence that the FSB or Russian government commissioned Belan and Baratov to specifically execute offensive cyber operations against Russian adversaries to diminish their economic capacity. Rather, Dokuchaev and Sushchin likely directed Belan and Baratov to target individuals for intelligence purposes.[123] Privateering was also an institution during the age of sail, and European powers accepted the behavior as an aspect of naval warfare. There is currently no formalized institution in cyberspace that recognizes such relationships between state and semi-state actors.

Although the Constitution empowers Congress to grant letters of marque and reprisal, both domestic and international would prohibit efforts by the UG government to introduce the practice in cyberspace. The US Government specifies that offensive cyber operations are an inherently governmental function, outlined by DODI 1100.22. The CFAA prohibits private individuals and organizations from conducting offensive cyber operations against state and non-state actors. Furthermore, the potential prizes seized in cyber privateering operations would likely qualify as violations of international law under the Hague conventions, Rome Statute of the ICC, and of norms established during the Nuremberg Tribunal after World War II.

Recommendations

An international agreement is a possible way to regulate the proliferation of semi-state actors in cyberspace, similar to how the Congress of Paris of eliminated privateering in 1856 with

[123] US Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts."

the passage of the *Paris Declaration Respecting Maritime Law*. In June 2017, the fifth UN Group of Governmental Experts (UN GGE) was unable to agree on a consensus report that would have brought additional clarity to how international law regulates cyberspace.[124] Cyberspace remains absent of international law. Voluntary, non-binding norms of responsible state behavior attempt to reduce risks to international peace, security, and stability. Norms reflect the expectations of the international community, set standards for responsible state behavior and allow the international community to assess the activities and intentions of states.[125] A future researcher should explore why there is a current absent of law in cyberspace, who benefits from the absence of international law, and what measures should be taken, if any, by the international community to safeguard the cyber domain.

Cyber threats to the United States are persistent. A study from the University of Maryland describes that every thirty-nine seconds, a computer connected to the internet is attacked by cybercriminals.[126] In response to the growing cyber threat the Secretary of Defense directed the establishment of a new military command devoted to cyber activities in 2009. US Cyber Command's stated mission is to "direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure United

---

[124] Anders Henriksen, "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019), accessed February 15, 2020, https:/www.doi.org/10.1093/cybsec/tyy009/.

[125] Peter J. Katzenstein, "Introduction: Alternative Perspectives on National Security," in *The Culture of National Security: Norms and Identity in World Politics*, ed. Peter J. Katzenstein (New York, NY: Columbia University Press, 1996) 5.

[126] Michel Cukier, "Study: Hackers Attack Every 39 Seconds," A. James Clark School of Engineering, University of Maryland, February 9, 2007, accessed January 20, 2020, https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds/.

States/Allied freedom of action in cyberspace and deny the same to our adversaries."[127] The DoD began to build a National Cyber Mission Force (NCMF) in 2012 to carry out DoD's cyber missions. The NCMF consists of 133 teams that are organized to meet DoD's three cyber missions: Offensive Cyberspace Operations, Defensive Cyberspace Operations, and DoD Information Network Operations. The NCMF reached full operational capacity at over 6,200 individuals in May 2018.[128]

Though the employment of US privateers in cyberspace is unfeasible, cyber contractors may offer an alternative to augment offensive US cyber operations during conflict. Other states have already sought to employ contractors to both defend their cyber infrastructure and execute offensive cyber operations against adversaries.[129] Compared to the number of attacks the United States confronts in the cyber domain, the size of the NCMF is relatively small. A future researcher should explore the possibility of cyber contractors conducting offensive operations on behalf of the US Government. Alterations to Title 32 CFR, DODI 1100.22, and CFAA may enable cyber contractors with the necessary authorities to execute offensive cyber operations. The use of bonds may also play a role, ensuring that contractors carefully execute operations in accordance with the guidelines outlined in their contracts.

---

[127] US Library of Congress, Congressional Research Service, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary, IF10537 (January 14, 2020), 1, accessed January 20, 2020, https://crsreports.congress.gov/product/pdf/IF/IF10771/.

[128] US Library of Congress, CRS, *Defense Primer: Cyberspace Operations*, 1.

[129] Ellen Nakashima, "As Cyberwarfare Heats Up, Allies Turn to US Companies for Expertise," *The Washington Post*, November 22, 2012, accessed February 15, 2020, https://www.washingtonpost.com/world/national-security/as-cyberwarfare-heats-up-allies-turn-to-us-companies-for-expertise/2012/11/22/a14f764c-192c-11e2-bd10-5ff056538b7c_story.html/.

Bibliography

Berger, Peter L., and Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. New York, NY: Doubleday, 1966.

Black's Law Dictionary, 5th ed. St. Paul, MO: West Publishing, 1979.

Chairman of the Joint Chiefs of Staff. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces* (Washington, DC: Government Printing Office, 2005), 1. Accessed January 20, 2020. https://www.jag.navy.mil/distrib/instructions/CJCSI%203121.01B13Jun05.pdf.

Corbet, Julian. *Sir Francis Drake*. 1890. Reprint, Coppell, TX: CreateSpace Independent Publishing Platform, 2016.

Cukier, Michel. "Study: Hackers Attack Every 39 Seconds." A. James Clark School of Engineering, University of Maryland. February 9, 2007. Accessed January 20, 2020. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds/.

Earl, Edward Mead. "Adam Smith, Alexander Hamilton, Fredrich List: The Economic Foundations of Military Power. In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, edited by Peter Paret, 221-222. Princeton, NJ: Princeton University Press, 1986.

Gaddis, John. *Landscape of History: How Historians Map the Past*. New York, NY: Oxford University Press, 2004.

Galeotti, Mark. *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*. London, UK: European Council on Foreign Relations, 2017. Accessed January 20, 2020. https://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

Golden Hind. "The Circumnavigation, 1577-1580." 2019. Accessed November 30, 2019. https://goldenhind.co.uk/pages/history/the-circumnavigation-1577-1580/106/.

Gvosdev. Nikolas K. "The Bear Goes Digital: Russia and Its Cyber Capabilities." In *Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012.

Henriksen, Anders. "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace." *Journal of Cybersecurity* 5, no. 1 (2019). Accessed February 15, 2020. https://doi.org/10.1093/cybsec/tyy009.

Hume, David. *The History of England*. Indianapolis, IN: Liberty Fund, Incorporated, 1983.

International Committee of the Red Cross. *Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 12 August 1949*. October 21, 1950, 75 U.N.T.S. 287, Article 33. Accessed January 22, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=AE2D398352C5B028C12563CD002D6B5C.

International Criminal Court. “War Crime of Excessive Incidental Death, Injury, or Damage” Elements of Crimes. Accessed January 20, 2020. https://www.icc-cpi.int/resourcelibrary/official-journal/elements-of-crimes.aspx#article8-2b-iv/.

———. “War Crime of Pillaging.” Accessed January 20, 2020. https://www.icc-cpi.int/resourcelibrary/official-journal/elements-of-crimes.aspx#article8-2e-v/.

International Peace Conference. *The Hague, Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land*. The Hague, October 18, 1907, January 26, 1910, Article 28. Accessed January 22, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/195-200038?OpenDocument.

———. *The Hague, Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land*. The Hague, October 18, 1907, January 26, 1910, Article 47. Accessed January 22, 2020. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Article.xsp?action=openDocument&documentId=FA13E789FD4EAFF0C12563CD005168CC.

Katzenstein, Peter J. “Introduction: Alternative Perspectives on National Security.” In *The Culture of National Security: Norms and Identity in World Politics*. Edited by Peter J. Katzenstein. New York: Columbia University Press, 1996, 5.

Kramer, Andrew E. “How Russia Recruited Elite Hackers for Its Cyberwar.” *The New York Times*. December 29, 2016. Accessed November 30, 2019. https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elitehackers-for-its-cyberwar.html/.

Leiner, Frederick C. “Yes, Privateers Mattered.” *Naval History Magazine* 28, no. 2 (March 2014): 16-21. Accessed January 20, 2020. https://www.usni.org/magazines/naval-history-magazine/2014/march/yes-privateers-mattered/.

Lemnitzer, Jan Martin. Power, *Law and the End of Privateering* (Basingstoke, UK: Palgrave Macmillan, 2014), 48–51.

Mabee, Bryan. “Pirates, Privateers and the Political Economy of Private Violence” *Global Change, Peace & Security* 21, no. 2 (June 2009): 139-152. Accessed January 20, 2020. https://www.doi.org/10.1080/14781150902871994.

Mahan, Alfred Thayer. *The Influence of Sea Power Upon History, 1660-1783*. Boston, MA: Little, Brown and Company, 1890. Accessed November 23, 2019. http://www.gutenberg.org/files/13529/13529-h/13529-h.htm.

Merriam-Webster Dictionary, accessed January 20, 2020, https://www.merriam-webster.com/dictionary/analogy.

Nakashima, Ellen. “As Cyberwarfare Heats Up, Allies Turn to US Companies for Expertise.” *The Washington Post*. November 22, 2012. Accessed February 15, 2020. https://www.washingtonpost.com/world/national-security/as-cyberwarfare-heats-up-allies-turn-to-us-companies-for-expertise/2012/11/22/a14f764c-192c-11e2-bd10-5ff056538b7c_story.html/.

Roksund, Arne. *The Jeune École: The Strategy of the Weak*. Leiden, Netherlands: Brill Academic Publishers, 2007. Accessed December 20, 2019. http://ebookcentral.proquest.com/lib/carl-ebooks/detail.action?docID=468356/.

Rome Statute of the International Criminal Court, art. 8(2)(b)(xvi). https://www.icc-cpi.int/NR/rdonlyres/ADD16852-AEE9-4757-ABE7-9CDC7CF02886/283503/RomeStatutEng1.pdf/.

Shomette, Donald Grady. *Privateers of the Revolution: War on the New Jersey Coast, 1775-1783*. Atglen, PA: Schiffer Publishing, 2016.

Singer, Peter W. "Corporate Warriors: The Rise and Ramifications of the Privatized Military Industry," *International Security* 26, no. 3 (Winter 2001-2002): 186-220. Accessed January 20, 2020. https://www.jstor.org/stable/i355580/.

Tabarrok, Alexander, and Alex Nowrasteh. "Privateers! Their History and Future." *Fletcher Security Review 2*, no. 1 (Jan 2015): 55-84.

Theohary, Catherine A. IF10537. *Defense Primer: Cyberspace Operations*. Washington, DC: Congressional Research Service, January 14, 2020. Accessed January 20, 2020. https://crsreports.congress.gov/product/pdf/IF/IF10771/.

Trump, Donald J. *National Cyber Strategy of the United States of America*. Washington, DC: The White House, 2018.

United Nations. *United Kingdom of Great Britain and Northern Ireland, United States of America, France, Union of Soviet Socialist Republics: Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis, Signed at London, August 8, 1945*, Article 6 (b), 288. Accessed January 20, 2020. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.2_Charter%20of%20IMT%201945.pdf.

United Nations. *Report of the Commission on the Responsibility of the Authors of the [First World] War and on Enforcement of Penalties, March 29, 1919*. Accessed January 20, 2020, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1917&context=ils.

US Department of Defense, Joint Staff. *DOD Dictionary of Military and Associated Terms*. Washington DC, Government Printing Office, 2018.

———. Joint Staff, Under Secretary of Defense for Personnel and Readiness. Department of Defense Instruction (DODI) 1100.22, *Policy and Procedures for Determining Workforce Mix*. Change 1. Washington, DC: Government Printing Office, 2017.

———. Joint Staff. Joint Publication (JP) 3-12, *Cyberspace Operations*. Washington, DC: Government Printing Office, 2018.

———. Joint Staff. Joint Publication (JP) 3-32, *Joint Maritime Operations*. Washington, DC: Government Printing Office, 2020.

US Department of Justice. Computer Crime and Intellectual Property Section, Criminal Division Office of Legal Education Executive Office for United States Attorneys. *Prosecuting Computer Crimes*. OLE Litigation Series. Edited by Scott Eltringham, 2nd ed. Washington, DC: Executive Office for United States Attorneys, 2010. Accessed January 20, 2020. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf/.

———. "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts." Press release no. 17-278. March 15, 2017. Accessed January 20, 2020. https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions/.

———. "International Hacker-For-Hire Who Conspired with and Aided Russian FSB Officers Sentenced to 60 Months in Prison." Press release no. 18-703. May 29, 2018. Accessed January 20, 2020. https://www.justice.gov/opa/pr/international-hacker-hire-who-conspired-and-aided-russian-fsb-officers-sentenced-60-months/.

———. "Canadian Hacker Who Conspired with and Aided Russian FSB Officers Pleads Guilty." Press release no.17-1341. November 27, 2017. Assessed January 20, 2020. https://www.justice.gov/opa/pr/canadian-hacker-who-conspired-and-aided-russian-fsb-officers-pleads-guilty/.

Annals of Congress. 12th Cong., 1st sess., 1812, pt. Appendix: 2322-2323. Accessed January 22, 2020.http://memory.loc.gov/cgibin/ampage?collId=llac&fileName=024/llac024.db&recNum=570&itemLink=r%3Fammem%2Fhlaw%3A%40field%28DOCID%2B%40lit%28ac0241%29%29%230240594&linkText=1.

US Library of Congress. Law of Customs of War on Land (Hague, IV), art. 28 and art. 47. Accessed January 20, 2020. https://www.loc.gov/law/help/us-treaties/bevans/m-ust000001-0631.pdf/.

US Secretary of Defense. US Department of Defense. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*. Washington, DC: Government Printing Office, 2018.

Weber, Max. *The Theory of Social and Economic Organization*. Edited by Talcott Parsons and translated by Talcott Parsons and A.M. Henderson. 1948. Reprint, New York, NY: The Free Press, 1964.

Wombwell, James A. *The Long War Against Piracy: Historical Trends*. Occasional Paper 32. Fort Leavenworth, KS: Combat Studies Institute Press, 2010.