Center on Law, Ethics and National Security

Essay Series
Number 15
June 23, 2022

Private Redress for Private Wrongs: Ransomware Payments as Prize

By Liam A. Murray

DUKE LAW

PRIVATE REDRESS FOR PRIVATE WRONGS: RANSOMWARE PAYMENTS AS PRIZE

LIAM A. MURRAY*

ABSTRACT

Recent legal scholarship has identified letters of marque and reprisal as a legal tool that could potentially address a range of cybersecurity threats faced by the United States. The arguments generally advocate for a 'hack-back' authority– that letters of marque and reprisal be used to allow United States persons, particularly businesses, to hack their hackers back. However, these proposals fail to adequately consider what facets of letters of marque and reprisal made them effective when they were common legal instruments. (In their original historical context?)

Letters of marque and reprisal are legal instruments that enable private parties to take specified property and, after legal process, benefit from its sale. These instruments were originally a sovereign grant of a private right to self-help, before becoming tools of public war. Two incentive structures, prize and salvage, make such a regime viable. Prize enables the holder of a letter of marque and reprisal to benefit from the sale of captured property. Salvage enables the original owner of that property to likewise benefit from that sale. These mechanisms function to incentivize parties to retake wrongfully taken property and afford relief to wronged parties in the form of restitution.

A 'hack-back' authority does not fit this model because it fails to utilize those incentives. Such an authority would be retaliatory in nature, rather than restitutionary. Nevertheless, while letters of marque and reprisal may not be effectively analogized to general hack-back authorities, they may be a viable tool for dealing with ransomware, an arena in which clear analogies to prize and salvage are readily available. This paper evaluates the legal history and status of letters of marque and reprisal in American and international law and argues that the United States may be well-served by considering the use of letters of marque and reprisal to address the problem of ransomware.

* Duke University School of Law, J.D. and LL.M. in International and Comparative Law expected May 2023; University of North Carolina at Chapel Hill, B.A. 2018. I would like to thank Major General Dunlap and Professor Stansbury for humoring this paper, which was a joy to write.

INTRODUCTION

Letters of marque and reprisal (hereinafter, LOM), though unused by the United States since the War of 1812,[1] remain an oft-proffered policy solution for many of the nation's security problems. In the post-9/11 era, LOM have been suggested as a mechanism for combatting terrorism.[2] In response to the perception of diminished United States naval superiority, LOM have been presented as a mechanism for tilting the scale of seaborne power back in its favor.[3] LOM have too been recommended to deal with modern waves of sea piracy.[4] But in particular, the notion of reintroducing LOM has taken hold in the field of cybersecurity.[5] The idea for cyber-privateering is, at its core, an application of an archaic legal concept to channel a more general policy ambition for some sort of "hacking back" authority– that is to say, granting hacked entities the right to hack their hackers back.[6] The 'hack back' has been characterized as "the worst cybersecurity policy idea that just won't die."[7] And not without reason–active cyber defenses carry serious hazards,

---

[1] William Young, Note, *A Check on Faint-Hearted Presidents*, 66 WASH. & LEE L. REV 895, 907 (2009). Note, however, that OM were issued by the Confederate States during the Civil War. *Id.* at note 83.

[2] *See, e.g.*, Robert Dewitt, Note, *Let Privateers Marque Terrorism: A Proposal for a Reawakening*, 82 IND. L. J. 131 (2007).

[3] *See, e.g.*, Peter Suciu, *Return of the Privateers: How the U.S. Navy Could Take on Russia and China*, NAT'L INTEREST (Oct. 27, 2020), https://nationalinterest.org/blog/buzz/return-privateers-how-us-navy-could-take-russia-and-china-171446.

[4] *See, e.g.*, Theodore T. Richard, *Reconsidering the Letter of Marque: Utilizing Private Security Providers Against Piracy*, 39 PUB. CONT. L. J. 411, 413–14 (2010).

[5] *See, e.g.*, Frank Colon, *Rebooting Letters of Marque for Private Sector, Active Cyber Defense*, 7 J. CYBERSECURITY & INFO. SYS. 50, 51 (2020); Christopher M. Kessinger, *Hitting the Cyber Marque: Issuing a Cyber Letter of Marque to Combat Digital Threats*, Aug. ARMY L. 4, 4 (2013); Ensign Lucian Rombado, *Grant Cyber Letters of Marque to Manage "Hack Backs"*, PROCEEDINGS (Oct. 2019), https://www.usni.org/magazines/proceedings/2019/october/grant-cyber-letters-marque-manage-hack-backs (2019); Dave Aitel, *Cyber Deterrence "At Scale"*, LAWFARE, https://www.lawfareblog.com/cyber-deterrence-scale.

[6] Stewart Baker & Victoria Muth, *Should Companies Risk Going on the Cyber Offensive?*, BRINK (July 22, 2016), https://www.brinknews.com/should-companies-risk-going-on-the-cyber-offensive/.

[7] Josephine Wolff, *Attack of the Hack Back*, SLATE (Oct. 17, 2017), https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html.

particularly given difficulties in attribution (in the technical sense, rather than the international law sense).[8]

Nevertheless, while hacking back may not be an effective policy prescription for all of the United States' cyber problems, it may be one that is well-suited to address the problem of ransomware, which is similarly, and perhaps uniquely, predisposed to being addressed within the framework of LOM. Ransomware presents a serious security risk to the international community–many nations have begun to address the issue increasingly aggressively, promising offensive action.[9] Commentators have characterized the American response as particularly, and surprisingly, restrained.[10] Perhaps this reflects a broader American strategy of tolerance to cyberattacks.[11] Nevertheless, given the costs that ransomware has wrought,[12] there have been increasing calls for world governments, including that of the United States, to act against ransomware perpetrators.[13] So while it is worthwhile to remain mindful of the limits of LOM as a cyber-policy, it may be worth considering them within the context of ransomware.

This paper will consider why LOM cannot be cleanly analogized to 'hack back' authorities, but why the LOM analogy may be a good fit for ransomware in particular and why LOM may be a tool to consider in that context. Part I will evaluate the historical and legal implementation of LOM. Part II will evaluate the implementation of a LOM regime in the 'hack back' context and in the more circumscribed ransomware context. Part III will address the limitations of the analysis of this paper, as well as the open questions and implications the paper raises.

---

[8] *See* Herbert Lin, *Attribution of Malicious Cyber Incidents*, HOOVER INST. (Sept. 26, 2016), https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.
[9] *Brits, Dutch and Aussies embrace Hounds Doctrine*, RISKY BUS. (Oct. 13, 2021) (available at https://risky.biz/RB642/)
[10] *See id.*
[11] Monica Kaminsa, *Restraint Under Conditions of Uncertainty: Why the United States Tolerates Cyber Attacks*, J. Cybersecurity 1, https://academic.oup.com/cybersecurity/article/7/1/tyab008/6162971 (forthcoming).
[12] In 2020, the "Federal Bureau of Investigation . . . received nearly 2,500 ransomware complaints with losses exceeding $29 million." Congressional Research Service, *Ransomware and Federal Law: Cybercrime and Cybersecurity* 1 (Oct. 5, 2021), https://crsreports.congress.gov/product/pdf/R/R46932. This likely grossly underestimates the scale of the problem, as many ransomware attacks simply go unreported. Alvaro Maranon & Benjamin Wittis, *Ransomware Payments and the Law*, LAWFARE (Aug. 11, 2021) https://www.lawfareblog.com/ransomware-payments-and-law.
[13] *See, e.g.*, Alvaro Maranon & Benjamin Wittis, *Ransomware Payments and the Law*, LAWFARE (Aug. 11, 2021) https://www.lawfareblog.com/ransomware-payments-and-law; Joe Tidy, *Ransomware: Should Paying Hacker Ransoms Be Illegal?*, BBC (May 20, 2021) https://www.bbc.com/news/technology-57173096.

PART I: THE BACKGROUND OF LOM AND PRIVATEERING

a. Historical

LOM have been granted by governments since perhaps the twelfth century.[14] They are a combined form of two devices, letters of marque and letters of reprisal; the former granted a right to a seizure outside of a state's jurisdiction, the latter within it.[15] In combined form, they represent a commission granted by the sovereign to private parties to take the goods and ships of another on the high seas.[16] In their early use, LOM were "for the redress of a private wrong, by the employment of private force"–this is to say, a sanctioned form of self-help.[17] They were a response to piracy: robbery on the high seas.[18] A robbed trader could apply for a LOM to get "restitution" from the individual whom had robbed him by taking his property and satisfying his private claim thereby.[19] LOM ultimately represent an attempt to institutionalize pre-existing self-help within a legal process in an otherwise anarchic system.[20]

Over time, this state-sanctioned, private self-help mechanism developed into a public war institution.[21] This shift was predicated on a theory of vicarious

---

[14] Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565, 566 (2007).

[15] J. Gregory Sidak, *The Quasi War Cases–And Their Relevance to Whether "Letters of Marque and Reprisal" Constrain Presidential War Powers*, 28 HARV. J. L. & PUB. POL'Y. 465, 473 (2005).

[16] § 34:6, Granting Letters of Marque and Reprisal, MODCONLAW.

[17] Bas v. Tingy, 3 U.S. 37, 38 (1800).

[18]Joel H. Samuels, *How Piracy Has Shaped the Relationship Between American Law and International Law*, 59 AM. U. L. REV. 1231, 1231 (2010).

[19] Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565, 566 (2007).

[20] *See* J. Gregory Sidak, *The Quasi War Cases–And Their Relevance to Whether "Letters of Marque and Reprisal" Constrain Presidential War Powers*, 28 HARV. J. L. & PUB. POL'Y. 465, 472–73 (2005) ("In the thirteenth and fourteenth centuries, as sovereigns began to fear that the waging of private warfare was getting out of hand, they created legal restrictions to inhibit the individual use of force at sea . . . . [P]irates preyed on maritime trade, and private associations were formed not only to defend commercial vessels, but also to attack the enemy. Without the protection of a strong sovereign, individual merchants who ventured beyond their local territory were forced to resort to self-help against maritime marauders. 'In the state of anarchy into which Europe saw herself plunged,' wrote de Martens in 1795, 'the principle, that war is a right belonging to a sovereign alone, was forgotten.'").

[21] William Young, Note, *A Check on Faint-Hearted Presidents*, 66 WASH. & LEE L. REV 895, 900–01 (2009).

liability; according to Grotius, "it [was] established by the law of nations that both the possessions and the acts of subjects are liable for the debt of a ruler."[22] As private individuals could redress their private claims with a state sanction, public entities could redress public wrongs with takings of private property from subjects of another sovereign. Early LOM limited the private individual to a value of capture and had an expiration period.[23] But in the age of sail, security on the high seas was of critical importance, away from the power of and outside of the jurisdiction of the sovereign. The ships necessary to ensure such security were expensive and lay heavily on sovereign budgets.[24] Prior to the late nineteenth century, tax systems tended to struggle to collect revenues practically.[25] Construction and maintenance of a navy could lead to state insolvency.[26]

So, sovereigns would offset the risk of outfitting a navy to private enterprise, in exchange for the reward of private enrichment–the taking of prize.[27] No longer were LOM issued to those in need of redress–a cause of action was no longer required.[28] Instead, in times of interstate conflict, European sovereigns would issue LOM "good against any enemy ship."[29] Those with these open-ended LOM were privateers proper.[30] These privateers became commonplace in Europe during the age of sail; famous English explorers such as Sir Francis Drake and Sir

---

[22] J. Gregory Sidak, *The Quasi War Cases–And Their Relevance to Whether "Letters of Marque and Reprisal" Constrain Presidential War Powers*, 28 HARV. J. L. & PUB. POL'Y. 465, 469 (2005).

[23] William Young, Note, *A Check on Faint-Hearted Presidents*, 66 WASH. & LEE L. REV 895, 900 (2009).

[24] *Cf.* Mauricio Drelichman & Hans-Joachim Voth, *The Sustainable Debt of Phillip II: A Reconstruction of Spain's Fiscal Position*, 1560–1598, 70 J. ECON. HISTORY 813, 818 (2010) ("Building [the Spanish Armada] cost two years' worth of revenue. When the fleet was destroyed, Spain had to rebuild its naval forces, strengthen her fortifications, and repel English and French attacks. The additional cost placed a heavy burden on royal finances . . . . [T]he king defaulted again in 1569.").

[25] Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565, 566 (2007).

[26] *See* Mauricio Drelichman & Hans-Joachim Voth, *The Sustainable Debt of Phillip II: A Reconstruction of Spain's Fiscal Position*, 1560–1598, 70 J. ECON. HISTORY 813, 818 (2010).

[27] *See* Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 8 (2007).

[28] Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565, 566 (2007).

[29] *Id.*

[30] Christopher M. Kessinger, *Hitting the Cyber Marque: Issuing a Cyber Letter of Marque to Combat Digital Threats*, Aug. ARMY L. 4, n.27 (2013).

Walter Raleigh operated as such.[31] Further, the legitimacy of privateering was ensconced into international law,[32] and the centrality of naval power to military strategy in the age of sail contributed significantly to its proliferation.[33]

Privateering proved to be critical to the success of the United States in the Revolutionary War and the early era of the Republic.[34] John Adams is purported to have called an early state privateering law, the Massachusetts Armed Vessels Act of 1775, "one of the most important documents of the Revolution."[35] By 1776, the Continental Congress had enacted a national system of LOM[36]–which also established the first "federal court" of the United States, one for the adjudication of prize cases.[37] Over the course of the Revolution, about seven-eighths of the naval capacity of the United States was in the form LOM commissioned ships; only the remaining eighth were ships of the United States Navy itself.[38] The British, an ocean away from the colonies in revolt, relied on naval supremacy to supply their forces therein, as well as to restrict the trade of goods with the colonies while maintaining their own trade.[39] The United States leveraged its privateering fleet to exact damage on the British Navy, but even more so to disrupt British trade; in January of 1777 alone, American privateers were reported as having caused £1.5

---

[31] Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565, 566 (2007).

[32] William Young, Note, *A Check on Faint-Hearted Presidents*, 66 WASH. & LEE L. REV 895, 901 (2009).

[33] *See* Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 15 (2007). ("The primary objective of war at sea, typically, was to reduce the maritime imports and exports of the enemy nation, thereby forcing it to surrender.").

[34] Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 18 (2007); Christopher M. Kessinger, *Hitting the Cyber Marque: Issuing a Cyber Letter of Marque to Combat Digital Threats*, Aug. ARMY L. 4, 6–7 (2013).

[35] C. Kevin Marshall, *Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars*, 64 U. CHI. L. REV 953, 960 (1997).

[36] *Id.* at 961.

[37] Gerard W. Gawalt, Book Review, *Bourguignon Henry J., The First Federal Court, The Federal Appellate Prize Court of the American Revolution 1775–1787*, 22 AM. J. OF L. HISTORY 271, 271 (1978).

[38] Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565, 567 (2007).

[39] *See* James Richard Wils, *"In Behalf of the Continent": Privateering and Irregular Naval Warfare in Early Revolutionary American, 1775–1777*, 75 (2012) (Thesis Paper, East Carolina University).

million in losses to British trade–accounting for inflation, £252 million in present value.[40] American privateers intercepted British ships well beyond the theatre of war, in the American Northeast, the West Indies, and on the coast of the British Isles themselves.[41] While the motives of these privateers remain a subject of historical debate, military historians seem to increasingly agree that privateering efforts were "vital" to the American Revolution.[42]

Privateers similarly played a role in the success of the fledgling United States in the Quasi War with France[43] and the War of 1812 with Britain.[44] When the Quasi War began to erupt, as a result of the publication of the XYZ dispatches,[45] the Alien and Sedition Acts permitted American vessels to "subdue and capture" French vessels, which "being brought into any port of the United States, shall and may be adjudged and condemned to their use, after due process and trial."[46] The primary theatre of operations for the conflict proved to be the Caribbean, a key trade hub between Europe and the Americas.[47] Less than two decades later, when the American naval fleet numbered at only eight ships, privateers again played a critical role in the War of 1812, in which American privateering proved to be at its "apogee."[48] In the course of the war, American vessels captured or sank 2,500 British vessels and meted out £40 million in economic damage to the British.[49]

The War of 1812 also proved to be the last use of privateers by the government of the United States,[50] although Congress would not abolish the prize

---

[40] *Id.* at 86.
[41] *Id.* at 75, 86, 91.
[42] *Id.* at 3.
[43] *See generally* Jon Paul Eclov, *Informal Alliance: Royal Navy and U.S. Navy Co-Operation Against Republican France During the Quasi-War and Wars of the French Revolution* (2013) (Thesis Paper, University of North Dakota).
[44] *See* Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 18 (2007)
[45] Jon Paul Eclov, *Informal Alliance: Royal Navy and U.S. Navy Co-Operation Against Republican France During the Quasi-War and Wars of the French Revolution*, 53 (2013) (Thesis Paper, University of North Dakota).
[46] Alien and Sedition Acts, Act of June 25, 1798, 1 Stat. 570, §§ 1–2 (1798).
[47] Jon Paul Eclov, *Informal Alliance: Royal Navy and U.S. Navy Co-Operation Against Republican France During the Quasi-War and Wars of the French Revolution*, 4 (2013) (Thesis Paper, University of North Dakota).
[48] Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565, 567 (2007).
[49] *Id.* at 571.
[50] William Young, Note, *A Check on Faint-Hearted Presidents*, 66 WASH. & LEE L. REV 895, n83 (2009).

system until 1899.[51] Many in the international community expressly agreed to cease privateering with the Paris Declaration Respecting Maritime Law, to which the United States declined to accede.[52] The reasons for the decline of privateering are the subject of debate. Economic theories tend to dominate the discourse.[53] One such theory is that as the cost of outfitting a vessel capable for military use grew, the "cost-saving advantage of privateering" was ameliorated.[54] An alternative theory is that American conceptions underpinning the justification of privateering were eroded, as a result of the "rise of liberalism, market utilitarianism, and religious humanitarianism," in conjunction with the position of the United States as a neutral power.[55] Nevertheless, whatever the reason, naval privateering and LOM have largely fallen into disuse, including in the United States, for well over a century.

b. Legal

LOM are a unique instrument of both domestic and international law. Their existence long precedes that of the United States. To understand the legal landscape of LOM, and what implementation of a LOM framework would look like, both sources of law must be evaluated.

i. Domestic Law

To determine how a LOM framework could be implemented, it needs to be ascertained how LOM were once regulated by the United States. The Constitution provides that "Congress shall have Power . . . [t]o declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water."[56] The basis for this grew out of international law, English common law, United States

---

[51] Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 90 (2007). Note, however, that the prize system also applied to captures made by the United States' public navy. *Id.*

[52] *Id.* at 10.

[53] *See generally* Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1 (2007); Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565 (2007).

[54] Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565, 575 (2007).

[55] Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 10 (2007).

[56] U.S. Const. art. I, § 8.

colonial and revolutionary practice, and provisions in the Articles of Confederation.[57] LOM were so deeply rooted in the common law inherited from Britain[58] and international law,[59] as well as the practice of the revolutionary era, that they were seen as simply one of the general war powers available to nations.[60] In Federalist 41, James Madison argued that the powers "of declaring war and granting letters of marque" are necessarily exclusive powers of the federal government to provide "[s]ecurity against foreign danger."[61]

The authority to grant LOM empowers Congress to enact statutes such as those of 1812, "Declaring War between the United Kingdom of Great Britain and Ireland and the dependencies thereof, and the United States of America and their territories"[62] and "An Act concerning Letters of Marque, Prizes, and Prize Goods."[63] These acts are largely representative of the regulatory system used for LOM in the early Republic. The acts provide a framework of commissioning and bonding, allocation of prize, and restraint on action.

By the former Act, Congress authorized the President:

"to use the whole land and naval force of the United States to carry the same into effect, and to issue to private armed vessels of the United States commissions or letters of marque and general reprisal . . . against the vessels, goods, and effects of the United Kingdom of Great Britain and Ireland, and the subjects thereof."[64]

The latter act elaborates. The President is thereby "empowered to revoke and annul at pleasure all letters of marque and reprisal which he shall . . . grant."[65] Applicants are required to provide to the Secretary of State or his officers "the name and suitable description of the tonnage and force of the vessel, and the name and place of residence of each owner . . . and the intended number of the crew."[66] The owners and commander of the ship are required to give bond and sureties to the United States; for ships with crews of less than 150, $5,000, and for ships with

---

[57] Theodore M Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 223, 224, 227 (2009).
[58] *See id.* at 223–24.
[59] *See* Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 31–32 (2007).
[60] *See* Theodore M Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 231 (2009).
[61] THE FEDERALIST NO. 41 (James Madison).
[62] Declaring War between the United Kingdom of Great Britain and Ireland and the dependencies thereof, and the United States of America and their territories, 2 Stat. 755 (1812).
[63] An Act concerning Letters of Marque, Prizes, and Prize Goods, 2 Stat. 759 (1812).
[64] 2 Stat. 755 (1812).
[65] 2 Stat. 759, § 1 (1812).
[66] *Id.* § 2 (1812).

crews of more than 150, $10,000.[67] Likewise, the commission of the LOM is conditional on the owner, officers, and crew of the vessel observing the "treaties and laws of the United States," as well as the instructions given for their conduct by regulation and the LOM itself.[68] For conduct "contrary to the tenor thereof," the owners, officers, and crew are liable to satisfy damages and injuries.[69]

Additionally, all "captures and prizes of vessels and property . . . accrue to the owners, officers, and crew of the vessels."[70] Once a condemnation has been made in court, the proceeds are then divided based on a written contract between the owners, officers, and crew, or else are divided half-and-half between the owners and the officers and crew and distributed according to a prior act,[71] the "Act for the

[67] *Id.* § 3 (1812).
[68] *Id.* § 3 (1812).
[69] *Id.* § 3 (1812).
[70] *Id.* § 4 (1812).
[71] *Id.* § 4 (1812). Note that these agreements were governed by contract and equity principles. In *The Dash*, 1 Mason 4 (Cir. D. Mass., 1815), this background distribution, described *infra* note 73, was treated as a gap-filler for an agreement as to the distribution of prize money that did not allocate shares to all crew members, while the court additionally refused admission of parol evidence as to purportedly agreed upon distribution. These private agreements, too, were important in regulating privateering vessels. Such agreements would define the relationship between the owners and the crew, the expectations of conduct onboard the vessel, and allocate shares of prizes. One such agreement follows:
"ARTICLES of AGREEMENT, made and concluded on in New-London, between the Owners, Captain, Officers and Mariners of the armed Sloop called the REVENGE, bound on a six Weeks Cruize against the Enemies of the United States of America. We, the Owners of the said Sloop do covenant to fit for Sea the said Vessel, in a warlike Manner; and provide her with Cannon, Swivels, Small-Arms, Cutlasses, sufficient Ammunition, and Provisions, with a Box of Medicines, and every other Necessary at our own Expence, for a six Weeks Cruize against the Enemies of the Thirteen United States of AMERICA; and that the said Owners shall be entitled to receive the one Half of all Prizes, Effects and Things that shall be taken during the said Cruize; the other Half to be divided amongst the Sloops Company, in the following Proportions – Captain, eight Shares; First and Second Lieutenants, Master and Doctor, four Shares each; two Masters Mates, Boatswain, Gunner and Quarter-Masters, Officers Marines and Carpenter, two Shares each; Prize-Masters, three Shares each; all lesser Officer, not more than one and half Share; Privates, one Share; and Boys, Half a Share. All Enterprizes at Sea or on Shore, shall be solely directed by the Captain. There shall be five dead Shares to be given to the most deserving Men, to be adjudged by the Committee. If any one shall loose a Leg or an Arm, in time of Action, he shall receive Three Hundred Dollars, out of the whole Effects taken. If any Person shall mutiny, or raise any Disturbance on Board, game, steal, or embezzle on, or of, any Prize, whether at Sea or in Port, disobey his Officer, prove a Coward, desert his Quarters, absent himself without the Leave of his superior Officer for the Term of twelve Hours, exercise

better government of the Navy of the United States."[72] This Act provides that prize money is to be distributed in parts allocated to sailors of different roles.[73]

Further, and critically, the Act provides that all property of citizens and residents of the United States, and those of foreign states with which the United States is "in amity," which shall be "recaptured" by commissioned vessels "shall be restored to the lawful owners, upon payment by them, of a just and reasonable salvage, to be determined by the mutual agreement of the parties concerned, or by the decree of any court having competent jurisdiction."[74] Such salvage is governed, too, by a prior act, "An Act providing for Salvage in cases of Recapture."[75] This act provides that any goods of a citizen or resident of the United States recaptured as prize under the authority of the United States shall be restored to them at salvage of one-sixth the value.[76]

---

any Cruelty or Inhumanity in cold Blood, he shall forfeit his whole Share or Shares to the Company, and be liable to such corporal Punishment as the Committee shall think fit to inflict. The Committee shall consist of the chief Commanding Officer, first and second Lieutenant and master. The Captain shall have full Power to displace any Officers as he shall think proper. LASTLY, the said Commander, Officers and Men, hereby enter our selves on the Cruize for the Term of six Weeks, if the Cruize shall last so long, or unless sooner discharged." James Richard Wils, *"In Behalf of the Continent": Privateering and Irregular Naval Warfare in Early Revolutionary American, 1775–1777*, 60 (2012) (Thesis Paper, East Carolina University).

[72] Act for the better government of the Navy of the United States, 2 Stat. 45 (1799).

[73] *Id.* Art. II, § 6 (1799) (Providing generally: to commanding officers three twentieths; lieutenants, captains of marines, and sailing masters two twentieths; to chaplains, lieutenants of marines, surgeons, pursers, boatswains, gunners, carpenters, and master's mates two twentieths; to midshipmen, surgeon's mates, captain's clerks, schoolmasters, boatswain's mates, gunner's mates, carpenter's mates, ship's stewards, sail-makers, masters at arms, armorers, cockswains, and coopers three twentieths and a half; to gunner's yeomen, boatswains's yeomen, quartermasters, quartergunners, sail-maker's mates, sergeants and corporals of marines, drummers, fifers, and extra petty officers two twentieths and a half; and to seamen, ordinary seamen, marines, and all other persons doing duty seven twentieths; all subject to certain variations. Likewise, any ships in sight of the taking of prize shares in the prize money proportionally to their size.).

[74] 2 Stat. 759, § 5 (1812). The entanglements of ownership can complicate this transaction. In *The Adeline*, 13 U.S. 244 (1815), capture was made of a vessel in possession of the British, owned by citizens of a third-party state, carrying the goods of Americans. The Supreme Court held that the prize could be libeled, but that salvage must be paid to the American owners. *Id.* at 287.

[75] An Act providing for Salvage in cases of Recapture, 2 Stat. 16 (1800).

[76] *Id.* § 1 (1800). Different values are afforded for salvage if the property belongs to the United States government or aliens. *Id.* §§ 2–3. Likewise, various statutes have set the salvage portion at various levels. One such act provided that any recapturers be awarded

There are a few additional restrictions provided for in the law for commissioned vessels. There is a prohibition on "breaking bulk," that is to say using or selling the goods from a captured vessel, until the ship returns to a friendly port for judicial proceedings.[77] The President is empowered to enact further instructions, too, for the "better governing and directing [of] the conduct of the vessels."[78] Commanding officers are required to keep logs "containing a true and exact account of his daily transactions and proceedings" including location of the vessel, the taking and estimated value of prizes, the disposal of prizes, and other information relevant to the regulation of the vessel.[79] These logs are then evaluated by customs officers at port, taken under oath of affirmation by the commanding officer, and privateers may not leave port until this process has been certified.[80] Likewise, these journals must be produced to American public ships, which may at any time search the privateering vessel;[81] failure to maintain journals, acts to destroy them, refusal to produce them on request, or fraudulent maintenance of the journals results in punitive action.[82] A commanding officer liable thereof will have the LOM revoked and will forfeit for each offense a substantial fine, which is then distributed to the United States and, in cases in which there is an informer of misconduct, to that informer.[83] Likewise, those onboard privateer vessels are liable for any violations of rules applicable to public vessels, to be tried in front of a court martial.[84]

So, the United States' statutory regime for the regulation of LOM was substantial. United States LOM laws specify which targets are valid for capture. The laws afford the President discretion to commission privateers with LOM at the receipt of a substantial bond. The laws set out how prize proceedings are to allocate prizes and how recapture of property of nationals of the United States is to be addressed. The laws substantially regulate the conduct of privateers by subjecting them to the law of nations, the law of the United States, the law of the Navy, and any additional directions determined at the discretion of the President. Further, the law requires that compliance be demonstrable by requiring that logs of privateering activities be maintained and regularly investigated; this is additionally reinforced by the provision for substantial rewards for what would today be considered

---

salvage of between one-eighth and one-half at the discretion of the court. *See* 1 Stat. 572, § 2.

[77] 2 Stat. 759, § 6 (1812).

[78] *Id.* § 8 (1812).

[79] *Id.* § 10 (1812).

[80] *Id.* § 10 (1812).

[81] *Id.* § 11 (1812).

[82] *Id.* § 11 (1812).

[83] *Id.* § 12 (1812).

[84] *Id.* § 14 (1812).

whistleblowing. Violations of the restrictions risked personal liability, revocation of the LOM, and criminal punishment.

How, then, are these laws enforced judicially? By use of the courts of admiralty.[85] The Constitution established that adjudicative power in privateering cases was to rest exclusively at the federal level.[86] This was a reflection of practice– the first 'federal' court had, indeed, been a court of admiralty[87]–and of the necessity of federal supremacy in war power affairs.[88] The only federal courts during the period of the Articles of Confederation had been admiralty courts.[89] The courts of admiralty were themselves a reflection of tradition: the first courts of admiralty in Britain were created to issue LOM and regulate privateers.[90]

The courts of admiralty had nearly full civil adjudicative authority over the privateering regime. They would adjudicate a taking of a prize and confirm its legality, [91] condemning the prize and thereby entitling the privateer to keep the proceeds of the property once sold at auction.[92] They would adjudicate claims between and amongst owners and crews of privateering vessels.[93] They would hear claims of wrongful takings against privateers[94] and salvage claims.[95] They would

---

[85] Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 41–42 (2007).

[86] U.S. Const. art. III, § 2. *See also*, Penhallow v. Doanes Adm'rs, 3 U.S. 54, 76 (1795) ("The individual States had no right to erect courts of prize, but under the authority of Congress.")

[87] Gerard W. Gawalt, Book Review, *Bourguignon Henry J., The First Federal Court, The Federal Appellate Prize Court of the American Revolution 1775–1787*, 22 AM. J. OF LEGAL HISTORY 271, 271 (1978)

[88] *Cf.* THE FEDERALIST NO. 41 (James Madison).

[89] *See* Theodore M Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 229 (2009).

[90] *See id.* at 224.

[91] *See, e.g.*, The Sally, 12 U.S. 382 (1814) (adjudicating a prize). Note further that contemporary courts considered such condemnations to be binding in rem. *See* Williams v. Armroyd, 11 U.S. 423, 432 (1813).

[92] *See* Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 3 (2007).

[93] *See, e.g.*, The Dash, 1 Mason 4 (1815) (determining the rights of crew members not signatory to a privateering vessel's agreement).

[94] *Cf.* Little v. Barreme, 6 U.S. 270 (1804) (holding that the taking of a prize was not valid and requiring restoration to its original owner).

[95] *See, e.g.*, The Adeline, 13 U.S. 244 (1815) (determining proper salvage to be paid to owners of recaptured vessel and goods onboard). *Cf.* Talbot v. Seeman, 5 U.S. 1 (1801)

judge the commissions of privateers and their compliance with their scope of authority.[96] They would recognize and enforce foreign admiralty judgments where allowed by law.[97]

Thus, the United States legal infrastructure for privateering was elaborate and comprehensive. Congress was empowered to issue LOM and prescribe laws for those commissioned thereby. The executive branch would give these commissions on the receipt of bonds, could likewise revoke the commissions, and the navy, customs authorities, and law enforcement authorities within the executive branch would monitor privateers to ensure their compliance with the law. The judiciary would likewise ensure compliance by adjudicating the takings of privateers before they could profit from their prizes, and by hearing claims against them, as well, holding them liable for their wrongdoings.

ii. International Law

LOM and privateering are products of international law and the international response to the problem of piracy. It is argued that "many of the most basic doctrines of international law have been formed either around piracy specifically or with piracy in mind."[98] At the very least, this is true of privateering. Piracy is the "unauthorized deprivation of property on the high seas."[99] Pirates have long been known as *hostis humani generis*–the enemies of mankind.[100] Outside the

(determining whether salvage was owed to foreign claimants whose property was captured by enemies of the United States).

[96] *See* Dias v. the Revenge, 7 F. Cas 637, 641 (Cir. Penn, 1814) (determining the liability of owners of a privateering vessel when the crew exceeded their commission and had been punished as pirates). *Cf.* The L'Invincible, 14 U.S. 238 (1815) (determining that while a United States court could determine whether a taking was within its commission for a commission issued by the United States, it could not do so for commissions granted by foreign powers).

[97] *See, e.g.*, Williams v. Armroyd, 11 U.S 423, 432 (1813) (holding that a French adjudication of cargo captured by a French privateer was binding on American nationals).

[98] Joel H. Samuels, *How Piracy Has Shaped the Relationship Between American Law and International Law*, 59 AM. U. L. REV. 1231, 1231 (2010).

[99] G. Edward White, *The Marshall Court and International Law: The Piracy Cases*, 83 AM. J. INT'L L. 727, 727 (1989). *But see*, Phillip A. Buhler, *New Struggle with an Old Menace: Towards a Revised Definition of Maritime Piracy*, 8 CURRENTS: INT'L TR. L.J. 61, 63 (1999) ("One would assume that the definition of "piracy" would be rather straight-forward, not unchanging over the centuries as the problem evolves. However, the history of international conventions and domestic laws addressing piracy shows a divergence of definitions, yet at the same time a curious outdated focus.")

[100] *See* Joel H. Samuels, *How Piracy Has Shaped the Relationship Between American Law and International Law*, 59 AM. U. L. REV. 1231, 1233 (2010).

jurisdiction of states and on the high seas, where sovereign protection could be impractical or impossible to afford, there existed a legal state of anarchy. Pirates *de facto* existed outside of any legal system, so states needed to work together to secure the seas for their citizens, trade, and economic development.[101] LOM, and mutual recognition of LOM between states, was one such response: recognition of private redress for prior takings on the high seas.[102] However, international law has long evolved since the founding of the United States and since the United States ceased to practice privateering. Does international law still recognize LOM?

The two sources of binding international law are treaties and customary international law.[103] Treaties are "international agreement[s] concluded between States in written form and governed by international law . . . whatever its particular designation."[104] Customary international law is that resulting "from a general and consistent practice of states followed by them from a sense of legal obligation."[105] Treaties may supersede customary international law, unless the treaty purports to violate a peremptory norm of international law, from which states may not derogate.[106]

LOM and privateering as such have their roots in what would now be considered customary international law. During the founding period, customary international law undoubtedly recognized the legitimacy of privateering: Grotius had claimed their legitimacy in the law of nations over a century before, and LOM were in regular use among the sea-faring nations of the world.[107] But in centuries

---

[101] *See Id.* at 1234.

[102] *See* Alexander Tabarrok, *The Rise, Fall, and Rise Again of Privateers*, 6 INDEP. REV. 565, 566 (2007).

[103] *See* Restatement (Third) of Foreign Relations Law, § 102 Sources of International Law; The Paquete Habana, 175 U.S. 677, 700 (1900) ("[W]here there is no treaty . . . resort must be had to the customs and usages of civilized nations").

[104] Vienna Convention on the Law of Treaties art 1(a), May 23, 1969, 1155 U.N.T.S. 331. Note that what may be considered a treaty under international law and what may be considered a treaty in United States law may differ, to the extent that international law may recognize agreements as binding upon the United States that have not undergone the Article II treaty process. *See* Restatement (Fourth) of Foreign Relations Law, § 301 Treaties as Law of the United States, Comment a.

[105] Restatement (Third) of Foreign Relations Law, § 102(2) Sources of International Law. This means that attempts to discern customary international law require looking to (a) general and consistent practice of states and (b) *opinio juris*, the sense of legal obligation.

[106] *See* Restatement (Third) of Foreign Relations Law, § 102 Sources of International Law, comment j.

[107] *See* Hugo Grotius, The Rights of War and Peace 312 (1614); *supra* Part I:A; Theodore M Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 244 (2009).

since, international law has developed, both through the development of treaty law, and perhaps through the evolution of customary international law.

In the middle of the nineteenth century, privateering had become increasingly complicated. States did not consider themselves bound to accept LOM issued from states they had not recognized,[108] and as treaties and alliances complicated, so did the uniformity with which states would recognize privateers as such, and not as pirates. As the Crimean War broke out in Europe in the 1850s, it became the view of several European states that privateering posed an increasing threat to state interests.[109]

As the war broke out, France and Britain, both of which had dominant naval forces, feared that a resurgence of privateering would threaten that dominance.[110] The primary counter-belligerent, Russia, in fact sought to issue LOM not only to Russian citizens, but to American citizens, as well.[111] France and Britain thus, in the hopes of keeping as many states neutral in the conflict as possible, first renounced their privateering claims against neutral ships carrying Russian goods, and then guaranteed not to license privateers whatsoever.[112] The strategy was largely successful, and France and Britain prevailed in the war.[113] At the subsequent peace conference in Paris, neutral parties wanted these concessions to be made permanent.[114] The concession would be mutually beneficial: France and Britain were able to maintain naval supremacy vis-à-vis any state mutually agreeing to forgo privateering, and smaller states were able to trade more freely.

Thus, along with the conclusion of the Treaty of Paris came the Paris Declaration Respecting Maritime Law (hereinafter, the Paris Declaration).[115] The treaty provides, in relevant part that "maritime law . . . has long been the subject of deplorable disputes . . . [and t]hat the uncertainty of the law . . . gives rise to differences in opinion between neutrals and belligerents which may occasion . . .

---

[108] *See, e.g.*, U.S. v. Hutchings, 26 F.Cas. 440, 442 (Cir. VA, 1817) (holding that as the United States had not recognized the independence of Buenos Ayres, it could not acknowledge commissions to which its seal was attached).
[109] *See generally* Charles H. Stockton, *The Declaration of Paris*, 14 AM. J. INT'L L. 356 (1920) (discussing the historical background of the Declaration of Paris).
[110] *See* Theodore M Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 244 (2009).
[111] Charles H. Stockton, *The Declaration of Paris*, 14 AM. J. INT'L L. 356, 357 (1920)
[112] *See* Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 57–58 (2007).
[113] *See id.* at 58.
[114] *See id.*
[115] Declaration Respecting Maritime Law, Paris, 16 Apr. 1856.

conflicts . . . [and thus p]rivateering is, and remains, abolished," to be binding among the states acceding to the treaty.[116]

The United States never acceded to the Paris Declaration.[117] Thus, as a matter of treaty law, the United States is not bound to respect the renunciation of privateering. However, whether this renunciation has crystalized into customary international law remains a subject of debate. Customary international law, as noted above, results from practice and *opinio juris*–in this case whether states have ceased privateering and whether they have done so believing it to be a matter of legal obligation. And further, customary international law additionally recognizes a persistent objector doctrine, that when a state "has persistently objected to a rule of customary international law during the course of the rule's emergence[, it] is not bound by the rule."[118]

So why did the United States not accede to the Paris Declaration? In the view of Secretary of State William L. Marcy:

"They tell us 'reserving always the right to make what havoc our overgrown navies may choose to inflict upon your tempting commerce, we demand that you exempt our commerce from the only means of retaliation you possess, the system of privateering.'

We reply, 'The terms are unfair. Equalize them by declaring your public and our private armed vessels under the same prohibitory rule, and we are with you. Otherwise, we are constrained to deny that privateering is or ought to be abolished.'"[119]

This is to say that the United States would not abide that large navies would retain their rights to capture private property and take prize, while the United States was expected to forgo its only source of naval advantage. This additionally reflected

---

[116] *Id.*

[117] Signatories to the Declaration Respecting Maritime Law. Paris, 16 April 1856, INT'L COMM. RED CROSS, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=105.

[118] David A. Colson, *How Persistent Must the Persistent Objector Be?*, 61 WASH. L. REV 957, 957 (1986).

[119] William L. Marcy, *Privateering–Secretary Marcy's Manifesto.*, N.Y. TIMES (Aug. 12, 1856), https://timesmachine.nytimes.com/timesmachine/1856/08/12/83448714.html?pageNumber=4).

uniquely American concerns about "large standing armies."[120] As such armies posed a risk to liberty, so too, did "powerful navies."[121]

The United States maintained this position in subsequent years. As the Civil War began, the United States considered joining the Paris Declaration in certain part, excluding the prohibition on privateering, but the negotiations floundered.[122] The United States did not rely on privateers during the war, but it never indicated that this was in respect of a sense of legal obligation, but rather with respect to the impracticality of their use in the blockade of the Confederacy.[123] In fact, Congress passed a bill allowing the president to issue LOM during the course of the Civil War.[124] Likewise, contemporary decisions in courts of admiralty predicate non-recognition of prizes taken by Confederate privateers not on the grounds of a prohibition on privateering, but on non-recognition of the Confederacy as a state.[125]

Subsequent disuse of LOM and privateers likewise appears to result from concerns of practicality, rather than of legal obligation.[126] In 1907, the United States refused to accede to the Hague Convention VII because it refused to renounce the possibility of privateering.[127] In 1941, President Roosevelt actively sought to arm private vessels in the Atlantic to deter German aggression.[128]

Some argue that, as the United States predicated its initial refusal to accept a prohibition on privateering on its non-application to public vessels, the United States should be understood to take the view that all takings on the high seas are

---

[120] Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 60 (2007).

[121] *Id.*

[122] Charles H. Stockton, *The Declaration of Paris*, 14 AM. J. INT'L L. 356, 364–67 (1920).

[123] *See* Nicholas Parillo, *The De-Privatization of American Warfare: How the U.S. Government Used, Regulated, and Ultimately Abandoned Privateering in the Nineteenth Century*, 19 YALE J. L. & HUMAN. 1, 66–67 (2007).

[124] 12 Stat. 758 (1863).

[125] *See* The Lilla, 15 F.Cas. 525, 529 (D. Mass, 1862) ("Most assuredly, I shall not recognize the Southern Confederates as a nation, or as having a government competent to establish prize courts. No proceedings of any such supposed tribunals can have any validity here.").

[126] *See supra* Part I:a.

[127] Brandon Schwartz, *U.S. Privateering is Legal*, U.S. NAVAL INST., https://www.usni.org/magazines/proceedings/2020/april/us-privateering-legal.

[128] Message to Congress on the Arming of Merchant Ships, Franklin D. Roosevelt, AMERICAN PRESIDENCY PROJECT, https://www.presidency.ucsb.edu/documents/message-congress-the-arming-merchant-ships ("The practice of arming merchant ships for civilian defense is an old one. It has never been prohibited by international law.")

illegal, including those done by private ships.[129] However, this does not necessitate the conclusion that the United States ceased privateering and did so because it believed privateering to be illegal. Additionally, even if it could be argued that the Paris Declaration has crystalized into customary international law, and that such law is binding on the United States despite its persistent objection to such international law, the Paris Declaration, the initial source of this obligation, nevertheless solely bans privateering as a maritime practice.[130] The Paris Declaration does not purport to ban states from granting LOM themselves–nor, then, would this purported customary international law.

PART II. LOM, HACK BACKS, AND RANSOMWARE

a. The Unique Problem of Ransomware

Ransomware is one of the many cyber threats facing the United States. The Federal Bureau of Investigations (FBI) reported that in 2020, it "received nearly 2,500 ransomware complaints with losses exceeding $29 million."[131] According to the assistant director of the FBI's Cyber Division, the FBI likewise estimates that perhaps a quarter to a third of cyber-attacks go unreported.[132] Further, the threat posed by ransomware attacks is increasing: estimates show that ransomware attacks may have "doubled in the first half of 2021."[133] The most famous of these incidents is likely the Colonial Pipeline attack, which disrupted gas supplies in the southeast United States and for which Colonial Pipeline paid $4.4 million in ransom.[134] Nevertheless, Colonial Pipeline's payout pales in comparison to that of CNA Financial, which paid $40 million just weeks later.[135] While the average payout is

---

[129] William Young, Note, *A Check on Faint-Hearted Presidents*, 66 WASH. & LEE L. REV 895, 928–29 (2009).
[130] *See* Declaration Respecting Maritime Law, Paris, 16 Apr. 1856.
[131] Congressional Research Service, Ransomware and Federal Law: Cybercrime and Cybersecurity 1 (Oct. 5, 2021), https://crsreports.congress.gov/product/pdf/R/R46932.
[132] Alvaro Maranon & Benjamin Wittis, *Ransomware Payments and the Law*, LAWFARE (Aug. 11, 2021) https://www.lawfareblog.com/ransomware-payments-and-law.
[133] Cognyte CTI Research Group, *Ransomware Attack Statistics 2021 – Growth & Analysis*, COGNYTE, https://www.cognyte.com/blog/ransomware_2021/. Ransomware attacks likewise are reported to have doubled from 2019 to 2020. Gerrit De Vynck et al., *The Anatomy of a Ransomware Attack*, WASHINGTON POST (July 9, 2021), https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/.
[134] *The 10 Biggest Ransomware Attacks of 2021*, TOURO COLLEGE ILLINOIS (Nov. 12, 2021), https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php.
[135] Brittany Chang, *One of the Biggest US Insurance Companies Reportedly Paid Hackers $40 Million Ransom after a Cyberattack*, BUSINESS INSIDER (May 22, 2021),

estimated to have been $200,000 in 2020, this is 4,000% increase from 2018's average payout of $5,000.[136] And these payouts fail to calculate for the downstream costs of ransomware, which can far exceed the cost of the ransom itself[137] and can include the loss of human life.[138]

Ransomware is a unique type of cyberattack, in that it is uniquely monetized. While a DDoS attack might attempt to knock a website offline or a Man-in-the-Middle attack might try to collect sensitive data, a ransomware attack seeks extraction of a payment.[139] Ransomware attackers use malware to encrypt the data stored on a computer or system, making it unusable without a key, and hold that data hostage until a ransom is paid.[140] These payments are generally made in cryptocurrency, as these currencies can be easier to move across borders, harder to freeze, and easier to launder.[141] Whereas in other types of cyberattacks, data tends to be the target of the attack, in the case of ransomware, the data is instead a *leverage point*–and the target is a cryptocurrency payment. Instead of reselling information, hackers use ransomware to extract a payment up front, a "more lucrative business model."[142]

Of course, ransomware is illegal. The Computer Fraud and Abuse Act (hereinafter, the CFAA) certainly covers such conduct. The CFAA forbids: **(1)** "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing]– (A) information contained in a financial record . . . [or] (B) information from any department or agency of the

---

https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5.

[136] *Ransomware Attack Trends for 2021*, VARONIS (July 6, 2021), https://www.varonis.com/blog/ransomware-statistics-2021/.

[137] *Cf. The 10 Biggest Ransomware Attacks of 2021*, TOURO COLLEGE ILLINOIS (Nov. 12, 2021), https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php.

[138] *See* Kevin Poulsen et al., *A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death*, WALL STREET J. (Sep. 30, 2021), https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116.

[139] *What Is a Cyberattack?*, CISCO, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

[140] *Ransomware: What It Is & What To Do About It*, CISA, https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf.

[141] Greg Myre, *How Bitcoin Has Fueled Ransomware Attacks*, NPR (June 10, 2021), https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks.

[142] Gerrit De Vynck et al., *The Anatomy of a Ransomware Attack*, WASHINGTON POST (July 9, 2021), https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/.

United States; or information from any protected computer;"[143] **(2)** "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access . . . further[ing] the intended fraud and obtain[ing] anything of value;[144] **(3)** "knowingly caus[ing] the transmission of a program . . . caus[ing] damage without authorization, to a protected computer;"[145] **(4)** "knowingly and with intent to defraud traffic[king] . . . in any password . . . if– (A) such trafficking affects interstate or foreign commerce;"[146] **(5)** "with intent to extort from any person any money or other thing of value, transmit[ting] . . . any communication containing any– (A) threat to cause damage. . . or (C) demand or request for money . . . in relation to damage to a protected computer."[147] These provisions would each appear to cover ransomware attacks, as might state laws and the Electronic Communications Privacy Act.[148]

However, a prosecutorial effort presumes that ransomware attackers can be identified and are likewise within the jurisdiction of the United States. But, cyberattacks can be hard to attribute,[149] and even when perpetrators can be identified, they are often far from the United States.[150] To address the problem, then, the United States must rely on businesses to take preventative measures[151] and choose which attacks it wants to use government resources to try to respond to, as

---

[143] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(1). Protected computers include those used by financial institutions and the United States government, as well as those "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 communications of the United States." 18 U.S.C. § 1030(e)(2).
[144] 18 U.S.C. § 1030(a)(4).
[145] *Id.* § 1030(a)(5)(A).
[146] *Id.* § 1030(a)(6).
[147] *Id.* § 1030(7).
[148] *See id.* § 2511.
[149] *See* Herbert Lin, *Attribution of Malicious Cyber Incidents*, HOOVER INST. (Sept. 26, 2016), https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.
[150] *See* Gerrit De Vynck et al., *The Anatomy of a Ransomware Attack*, The Washington Post, https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/ ("Many attacks come from organized groups that operate with relative impunity out of Russia, Belarus and other East European countries, according to researchers. Attackers range from enterprising individuals all the way up to groups of hundreds working directly for a nation state like North Korea.").
[151] *See Ransomware: What It Is & What To Do About It*, CISA, https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf.

when it recovered part of the Colonial Pipeline ransom payment.[152] Nevertheless, it is self-evident that such measures are insufficient, as ransomware attacks continue to become more prevalent and seek higher ransoms.

There have been several policy proposals to address this rapidly growing problem. Senators Warren and Ross introduced in October of 2021 the Ransom Disclosure Act, which would require that entities disclose certain pertinent information within forty-eight hours of payment of a ransom.[153] Alvaro Marañon and Benjamin Wittes have proposed using the Foreign Corrupt Practices Act (hereinafter, the FCPA) as a model for a prohibition on ransomware payments, with exceptions for exigent circumstances like threats to human life (e.g., in an attack on a hospital), to eliminate the supply side of the ransomware transaction.[154] The Office of Foreign Asset Control recently warned that ransomware payments made to sanctioned entities would still be subject to sanction violations penalties.[155] Senators Rubio and Feinstein have introduced the Stop and Sanction Ransomware Act, which would enable the President to designate states as state sponsors of ransomware and sanction the state.[156]

Nevertheless, these are incomplete solutions. Mandatory disclosure will help shed light on the scope of the problem, and perhaps bolster prosecutorial efforts and encourage businesses to improve their cybersecurity standards, but it will not prevent attacks. An FCPA model may limit the 'market' for targets of cybersecurity attacks–but it may also make those excepted from the prohibition the most likely to be targeted, in the sectors for which an attack would be most harmful. A sanctioned-entity restriction leaves it incumbent on businesses of all sizes to identify who is on the receiving end of a payment in the midst of a crisis, assuming that businesses would not instead simply begin to calculate the civil penalty for the

---

[152] *See* Amanda Macias et al., *U.S. Recovers $2.3 Million in Bitcoin Paid in the Colonial Pipeline Ransom*, CNBC (June 7, 2021), https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html.

[153] *See* Warren & Ross Introduce Bill to Require Disclosures of Ransomware Payments, ELIZABETH WARREN PRESS RELEASES (Oct. 5, 2021), https://www.warren.senate.gov/newsroom/press-releases/warren-and-ross-introduce-bill-to-require-disclosures-of-ransomware-payments.

[154] *See* Alvaro Maranon & Benjamin Wittis, *Ransomware Payments and the Law*, LAWFARE (Aug. 11, 2021), https://www.lawfareblog.com/ransomware-payments-and-law.

[155] Office of Foreign Asset Control, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, Department of the Treasury, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[156] *See* Rubio, Feinstein Introduce the Sanction and Stop Ransomware Act, MARCO RUBIO PRESS RELEASES (Aug 5, 2021), https://www.rubio.senate.gov/public/index.cfm/2021/8/rubio-feinstein-introduce-the-sanction-and-stop-ransomware-act.

sanction violation in as a cost of getting their systems back online. And sanctioning states presumes that states have an interest in or the capacity to prevent cybercrimes occurring within their borders. Something more is needed.

b. A LOM Framework to Address Ransomware

The LOM framework has been raised repeatedly as a possible solution to many of the United States' cybercrime problems.[157] The proposal tends to go something like this:[158] a private business entity applies for a LOM from the government. The government vets its credentials and issues the LOM if appropriate. When that business is hacked, it can conduct a 'hack back' operation against the attacker to "stop the ongoing exploits and degrade the attacker's infrastructure," within limits of proportionality.[159] The business would then be required to report its operation to a federal agency. A similar proposal would require the commissioned entity to instead conduct the 'hack back' jointly with a federal task force.[160]

The proposal for a 'hack back' authority has been rightly criticized. The most notable and consistent criticism is that the proposals fail to consider that "[c]byer actors, by comparison [to ships on the high seas], are better able to obfuscate their activity and hide who may be responsible for the criminal action."[161]

---

[157] *Supra* footnote 5.

[158] *See* Ensign Lucian Rombado, *Grant Cyber Letters of Marque to Manage "Hack Backs"*, PROCEEDINGS (Oct. 2019), https://www.usni.org/magazines/proceedings/2019/october/grant-cyber-letters-marque-manage-hack-backs.

[159] *Id.*

[160] *See* Frank Colon, *Rebooting Letters of Marque for Private Sector, Active Cyber Defense*, 7 J. CYBERSECURITY & INFO. SYS. 50, 54–56 (2020).

[161] Chris Cook, *Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook*, 29 STAN. L. & POL'Y REV. 205, 214–15 (2018). More cynical critiques, however, are not hard to come by:

"I am thunderstruck by how terrible [the 'hack back' proposal] is. At its heart it would just serve as an excuse to let anyone access anyone else's computer systems with impunity. Want to go after a competitor? Stage an attack directed at yourself coming from their servers, and then hack back! Or plant some of your sensitive files on their computers and then go in and delete them and monitor their behavior while you're at it (all in the name of building better defenses). Of course, once that company realizes what's going on, it may decide to take matters into its own hands and indulge in a little active defense directed at you. What could go wrong?"

To illustrate, imagine that an American business identifies that there is malware operating in its systems, sending files out to an unknown recipient. There are three levels of "attribution" that may need to be made: to the machine, to a human operative of that machine, and to the "ultimately responsible" party.[162] But the machine that is transmitting and receiving the data may not belong to the "ultimately responsible" party–it may instead be an innocent third party whose computer has also been infected with malware.[163] Innocent actors may be caught in the crosshairs. If that business were to try to go into the system to find where its files were 'taken' in the hopes of deleting them, they may instead be searching the files of such an innocent third party. That risk remains if it merely seeks to degrade that system, too.

But further, the notion of using LOM to conduct 'hack backs' misconstrues the nature of the LOM. A LOM was not simply a license to retaliate–it was, especially in its earliest period, a mechanism of restitution against piracy. Ransomware organizations are easy to analogize to the pirates of the age of sail–*hostis humani generis*.[164] They operate in areas in which it is difficult for states to utilize their coercive power to protect commerce.[165] They create deadweight loss in economies.[166] In the privateering era, a commissioned vessel would not simply take to the seas to find enemy vessels to destroy; it would bring such vessels to port, undergo legal process to take title, and then sell the prize.[167] If the property had once belonged to another citizen of its state, or an ally thereof, those citizens would also have a part of their loss recouped by salvage.[168]

Using LOM for 'hack backs' fails to utilize the incentive structure that made privateering viable, leaving in its place one far more perverse. For most 'hack backs,' there is no prize analogue. If a business receives a LOM, it will need to put a cyber-retaliation team on its payroll. Imagine that the business is an American

---

Josephine Wolff, *Attack of the Hack Back*, SLATE (Oct. 17, 2017), https://slate.com/technology/2017/10/hacking-back-the-worst-idea-in-cybersecurity-rises-again.html.

[162] Herbert Lin, *Attribution of Malicious Cyber Incidents* 1, HOOVER INST. (Sept. 26, 2016), https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

[163] *See id.* at 5 ("multi-stage intrusion").

[164] *See* Chris Zappone, *Pirates of the Cyber Seas: How Ransomware Gangs Have Become Security's Biggest Threat*, SYDNEY MORNING HERALD (July 2, 2021), https://www.smh.com.au/business/the-economy/pirates-of-the-cyber-seas-how-ransomware-gangs-have-become-security-s-biggest-threat-20210624-p5840c.html.

[165] *See id.*

[166] *See* Lawfare Podcast, *How Can Congress Take on the Ransomware Problem?*, LAWFARE (Aug. 16, 2021) (available at https://www.lawfareblog.com/lawfare-podcast-how-can-congress-take-ransomware-problem).

[167] *See supra* Part I:b.

[168] *See id.*

telecommunications firm that discovers its system have been breached and its proprietary technology schematics are being siphoned off.[169] The cyber team manages to successfully identify that a foreign firm is responsible for the breach and sets out to recover the files. The team breaches the foreign firm's systems–do they delete the stolen files and then leave the system? Do they go further and harm the foreign firm's systems? Steal some of the firm's files, as well? Their incentive is to do what their employer will want–the one cutting their paycheck. Government oversight will be costly and can only investigate so many retaliatory attacks, as well over half of American businesses are hit with cyberattacks each year.[170] These are not privateers, they are cyber-mercenaries by another name. LOM were designed to bring legal process to an anarchic system;[171] using them to permit 'hack backs' seems to set the stage for a less controlled internet landscape, not a more controlled one.

Nevertheless, a more circumscribed use of LOM may be appropriate, one that far more accurately fits the LOM structure and is a return to its origin: private redress for private the private wrong of ransomware. Instead of issuing LOM broadly to businesses so they may 'hack back,' LOM should instead be issued to a small, specialized set of cybersecurity firms to respond to ransomware attacks perpetrated by private actors.[172] These commissioned firms would work with targeted businesses to recoup the ransom taken, take that ransom to a cyber-prize court for condemnation, and then utilizing the salvage regime, split that recovered ransom with the business.

The federal government should harness the power of a profit incentive to allow private firms to recoup ransoms, as was done in the Colonial Pipeline incident,[173] without the need for the limited resources of government cybersecurity professionals. This utilizes the incentive of prize, instead of the incentive of payment from the firm directly, which creates the perverse incentives described

---

[169] *Cf.* Sean Lyngaas, *US Agencies Circulate Warning about 'Aggressive' Chinese Hacking Efforts to Steal Secrets from a Range of Targets*, CYBERSCOOP (July 16, 2021), https://www.cyberscoop.com/china-hacking-fbi-biden-alert-ip/.

[170] *See* Charlie Osborne, *76 Percent of US Businesses Have Experienced a Cyberattack in the Past Year*, ZDNET (Oct 8, 2019), https://www.zdnet.com/article/76-percent-of-us-businesses-have-experienced-a-cyberattack-in-the-past-year/.

[171] *See supra* note 19.

[172] *See infra* Part III:d.

[173] *See* Amanda Macias et al., *U.S. Recovers $2.3 Million in Bitcoin Paid in the Colonial Pipeline Ransom* (June 7, 2021), CNBC, https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html

above. Like bug bounty programs,[174] such a system would create a space for white-hat hackers to profit in a way that does not risk violating the aforementioned CFAA.[175]

And unlike general 'hack backs,' ransomware does not suffer the same attribution problem. A ransomware attacker necessarily identifies where the money will go: into the provided wallet.[176] There is no need to risk searching each link down a chain of infected computers on a fishing expedition for stolen data.[177] Instead, a cyber-privateer can instead follow the money down the blockchain–a difficult, but not impossible task, and certainly not one for someone seeking a prize.[178] Such a program would create deterrence against ransomware attacks, and at the very least incentivize ransomware attackers to seek smaller ransoms, to avoid being targeted. Nevertheless, even small businesses need not worry about whether or not they can afford the cyber-privateer, because they need not be able to pay. All they need is to allow the cyber-privateer to share in the recovered ransom. Likewise, the business's share of salvage helps it to recover the loss of the ransomware attack.

The "Act concerning Letters of Marque, Prizes, and Prize Goods" and the admiralty court system provide an excellent model for how such a regime would be regulated.[179] Congress would authorize the executive branch to issue and revoke LOM and exempt commissioned firms from the CFAA within a technically appropriate scope. The executive branch would collect the requisite information about the cybersecurity firm to be issued the LOM and take a large bond as surety against misconduct. The LOM's would be valid for a specified period of time and would be conditional on observance of the law and instructions given within the LOM. Like the prohibition on breaking bulk, the prize may not be disturbed until adjudicated. Logs should be kept of activities for evaluation, and failure to keep such logs will be punishable and result in revocation of the LOM. Whistleblowers

---

[174] *See* HackEDU, *What Are Bug Bounty Programs, and Why Are They Becoming so Popular*?, https://www.hackedu.com/blog/what-are-bug-bounty-programs-and-why-are-they-becoming-so-popular.

[175] *See* Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, NEW YORKER (May 7, 2018), https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

[176] *See* Gerrit De Vynck et al., *The Anatomy of a Ransomware Attack* (July 9, 2021), WASHINGTON POST, https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/.

[177] *See supra* note 164.

[178] *See* Gerrit De Vynck et al., *The Anatomy of a Ransomware Attack*, WASHINGTON POST (July 9, 2021), https://www.washingtonpost.com/technology/2021/07/09/how-ransomware-attack-works/. *See also*, Elie Burzstein et al., *How to Trace Ransomware Payments End-to-End–an Overview*, ELIE (Aug. 2017), https://elie.net/blog/security/how-to-trace-ransomware-payments-end-to-end/.

[179] *See supra* Part I:b:ii.

would be able to report misconduct of commissioned firms for a reward. The key difference would be that instead of granting a cyber-privateer the authority to take prizes of any enemy of the United States, it should instead grant them only the right to target a wallet identified by a victim of a ransomware attack and wallets laundering the ransom–closer to the original model of LOM. Further, instead of allowing negotiations for salvage *ex post* on recovery of a vessel, the agreement for the allocation of the recovery of the ransom payment would be *ex ante* between the victim and the commissioned firm.

Once a cyber-privateer has recovered a ransom, it will need to be taken to a court with jurisdiction for condemnation. Although the Constitution does not extend exclusive jurisdiction of cyber-prize cases to Article III courts,[180] exclusive federal jurisdiction can be achieved by statute.[181] These cyber-prize courts would operate much like an admiralty court would. The cyber-prize courts would confirm the legality of a taken prize, entitling the privateer to sell the cryptocurrency and distribute the proceeds accordingly. These courts can hear claims of wrongful takings against cyber-privateers to protect against misconduct. They can likewise confirm that these cyber-privateers have acted within the scope of their commissions.

Additionally, this is all likely viable under international law. While some could argue that there may be extraterritoriality concerns for a LOM ransomware regime, this is not the case. Leave aside the metaphysical complications of 'where' cyberattacks take place and 'where' a wallet may be. Irrespective, when privateers of the age of sale operated on the high seas, they were never truly beyond territorial jurisdiction–"a ship is like land, in that it falls within the jurisdiction of the nation whose flag it flies."[182] International recognition of LOM and privateering necessarily required recognition that privateers would operate extraterritorially by boarding vessels of ships flagged to enemy states, and therefore in the territory thereof. Furthermore, the United States is likely not bound by any international law, either treaty or customary international law, prohibiting privateering. Even if it were bound by the Paris Declaration as a matter of customary international law, which it likely is not, the prohibition only extends to maritime privateering–not to the issuance of LOM as such.[183]

Furthermore, LOM as ransomware policy need not be mutually exclusive of the policies mentioned above; rather, such a policy could be additive. The

---

[180] *Cf.* Const. Art. III (granting exclusive jurisdiction over admiralty cases to the Article III courts).

[181] *Cf.* 28 U.S.C. § 1338(a) (providing exclusive jurisdiction over patent and copyright cases to federal courts).

[182] Kiobel v. Royal Dutch Patroleum Co., 569 U.S. 108, 130 (Breyer, J., concurring, 2013).

[183] *See supra* Part I:b:ii.

disclosure model[184] fails to recover any ransom for a harmed business but could facilitate in the gathering of information for cyber-privateers to operate more effectively. The FCPA model[185] necessarily has an exception for payments made in exigent circumstances, so targets will remain, and ransomware payments will almost certainly continue to be paid by the most vulnerable of organizations, like hospitals. The sanctioned entity model[186] likewise is not a full prohibition on payments, but rather only on certain payments, leaving a space for cyber-privateers to operate. The state sanctioning model[187] operates on an international level and does not address specific cybercriminals, in the hopes of pressuring states to better address cybercrime occurring within its borders.

Issuing LOM will likely create additional leverage for the United States against these states–if they do not want American cyber-privateers operating in their virtual space, they need to address cybercrime themselves. The message would be similar to Marcy's in response to the Declaration of Paris: it is time for states to cooperatively and collectively protect private property in cyberspace. In the meantime, the process afforded by the LOM regime could help bring a modicum of legal order and the possibility of restitution to those suffering in the anarchic system at play.

PART III: LIMITS OF ANALYSIS AND OPEN QUESTIONS

This paper analyzes the possible role of LOM in the cybersecurity context in light of their historical use, legal background, and legal status. However, there are limits to the analysis afforded, which leave room for further research and development, particularly for the recommended regime to be implemented. Likewise, these limits and open questions may leave room for criticism; for that reason, any consideration of the policy advocated by the paper is best served by explicating these limits. The key limits to the analysis presented by this paper relate to technological feasibility, political questions, and certain treatment of international law.

a. Technological Feasibility

First, this paper is predominantly a legal analysis. It does not address, at least substantially, the technological feasibility of private, commissioned actors recovering ransomware payments. Instead, it operates on the assumption that it is the case that such recovery is possible, given that the United States government has

[184] *See supra* note 152.
[185] *See supra* note 153.
[186] *See supra* note 154.
[187] *See supra* note 155.

previously recovered ransom payments.[188] The paper takes the view that United States security would be best served if the security and military organs of the state utilize their finite resources–human capital, computer systems, and assets like zero-day exploits[189]–for higher priority security matters.[190] Therefore, if private actors can perform a similar function, as they might in a LOM regime, American security is better served. How many cyber-actors there are in the United States capable of private recovery of ransomware payments is unclear. How many could perform this task as a profitable enterprise is likewise so. However, at the very least, this question could be answered by the market–if LOM do not enable profitable enterprises, actors will not seek the commissions out.

b. International Use of Force

Likewise, this paper proceeds on the assumption that cyber-attacks do not constitute an "armed attack" as contemplated in the U.N. Charter–that they are legally distinct from kinetic attacks.[191] This assumption seems reasonable given

[188] *E.g.*, Amanda Macias et al., *U.S. Recovers $2.3 Million in Bitcoin Paid in the Colonial Pipeline Ransom*, CNBC (June 6, 2021), https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html.

[189] Zero-day exploits are flaws in computer systems that exist from their release, and once used, are liable to be patched and resolved by the system developers. *See What is a Zero-Day Exploit?*, FIREEYE, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html. This means that zero-day exploits are expendable; once utilized, it may be unclear how many times the exploit can still be used. *Id.* So, the government may be best served preserving these powerful tools for the most exigent of circumstances. A notable recent example of the use of a zero-day exploit is the SolarWinds attack. *See* Ryan Naraine, *SolarWinds Confirms New Zero-Day Flaw Under Attack*, SECURITY WEEK (July 12, 2021) https://www.securityweek.com/solarwinds-confirms-new-zero-day-flaw-under-attack.

[190] *See, e.g.*, Sean Lyngaas, *US Cyber Officials Issue Sweeping Directive Requiring Federal Agencies to Update Systems Vulnerable to Hacking*, CNN (Nov. 3, 2021), https://www.cnn.com/2021/11/03/politics/cyber-systems-update-hacking-federal-agencies/index.html.

[191] U.N. Charter art. 51.

commentary and state practice,[192] but certainly this is an area of developing law.[193] If cyberattacks constitute a use of force within the meaning of the U.N. Charter, the legal analysis underpinning this paper may change significantly. In the first instance, this would mean that cyberattacks could be uses of force to which states may respond with measures of self-defense. This also raises questions of attribution of ransomware attacks to states and the present status of the international law of self-defense (namely, whether due diligence standards or willing and able standards would justify what could be considered a use of force in a foreign state). These are each substantial questions in presently evolving areas of law which are not addressed in this analysis.

c. Potential Concerns of the Military and Intelligence Community

As a practical matter, it is possible that the United States military and Intelligence Community (hereinafter, the IC) may have limits to which they are comfortable with potentially parallel cyber operations. United States state cybersecurity actors may want to ensure that commissioned cyber-privateers do not target hostile foreign cyber actors that they themselves are targeting. Perhaps parallel action could draw such foreign actors' attention to exploitable flaws in their system, or simply put their guard up. It is possible that American state organs could create a white-list system of acceptable targets, or a black-list system of prohibited targets, but such a mechanism could likewise risk putting hostile actors on notice. Serious governmental consideration of a LOM regime would require input from the military and IC to ensure that commissioned actors could operate in such a way as to not interfere, knowingly or unknowingly, with government cyber operations, if these organs so desire.

---

[192] *See, e.g.*, Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 574 (2011) (discussing how U.N. Charter Article 51 is unlikely to contemplate cyber operations); *cf.* David E. Sanger et al., *Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China*, N.Y. TIMES (Mar. 7, 2021), https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html (discussing the United States' response to Russian and Chinese hacking, notably not including kinetic uses of force, but rather "day-to-day, short-of-war" cyber operations, along with tools like diplomacy, countermeasures, etc.).

[193] *See, e.g.*, Dimitar Kostadinov, *Invoking Article 51 (Self-Defense) of the UN Charter in Response to Cyber Attacks – II*, INFOSEC (Jan. 28, 2013), https://resources.infosecinstitute.com/topic/invoking-article-51-of-un-charter-response-cyber-attacks-ii/ (arguing that Article 51 could be "stretch[ed]" to encompass cyber-attacks).

d. State Involvement and Cyber-Flags

A key facet of the analysis in this paper is that the potential use of LOM herein extends only to non-state ransomware perpetrators. At this time, states generally do not claim ransomware operations as their own, although it is possible that some ransomware perpetrators may be connected to states.[194] Were the United States to commission cyber-privateers, however, ransomware attackers may begin to seek their own protection from states. These ransomware operators may even seek for their states to utilize a LOM regime to do so, albeit one closer to the later LOM regime in which all goods of all enemies are liable for taking.

The limitation of this paper's analysis on the question of attribution is addressed above,[195] but an additional consequence of this could be that ransomware operators would begin to make their identities and nationalities clearly known, rather than attempting to conceal them. Commentators have previously noted the ways in which the progressive regulation of digital spaces reflects previous developments of regulation in analogous spaces in the analogue world.[196] It is worth considering that if the United States looks to historical maritime law to bring law to digital spaces, it may create a sort of path dependency in which digital spaces increasingly resemble maritime spaces. Perhaps the need to claim nationality may lead to a system that resembles flagging (*i.e.*, a system resembling ships carrying flags of their state). Perhaps digital flags would likewise be used to confer jurisdiction over online actors,[197] to avoid the questions raised by the 'location' of what transpires in digital spaces. In considering whether a LOM regime should be implemented as a response to ransomware, the United States should likewise consider whether it is in its interest to encourage what might be called the maritimization of digital law–what the consequences of further analogization may be.

---

[194] *See* Matt Streib, *What's Driving the Surge in Ransomware Attacks?*, N.Y. MAG. (Sep. 7, 2021), https://nymag.com/intelligencer/article/ransomware-attacks-2021.html.
[195] *See supra* Part III:b.
[196] *See* Michael Held, *U.S. Regulations and Approaches to Cryptocurrencies*, Remarks at the BIS Central Bank Legal Experts' Meeting, Basel, Switzerland, https://www.newyorkfed.org/newsevents/speeches/2019/hel191212 (drawing analogies between present developments in cryptocurrency with the history of banking and noting how regulatory agencies can consider past regulatory practices when devising present-day policy).
[197] *Cf.* Tamo Zwinge, *Duties of Flag States to Implement and Enforce International Standards and Regulations–and Measures to Counter Their Failure To Do So*, 10 J. INT'L BUSI. & L. 297, 298 (2011) (discussing flag state control over a ship).

CONCLUSION

LOM are not a panacea for the United States' cybersecurity problems. Their broad
spectrum application would likely result in increased, rather than decreased, disorder in cyberspace and carry escalation risks both therein and in the United States' international relations. Nevertheless, a LOM regime, one closer to the original model of private redress for private wrongs, does appear to be a promising potential mechanism to address the rapidly escalating problem of ransomware. This regime is viable under American, likely so under international law, and is one for which decades of legal authority exist to look to for insights as to how to make such a system effective. Such a regime would leverage profit motive to utilize extant, but presently illegal, white-hat hacking operations to deter ransomware attacks and afford victims of these attacks a measure of restitution. Additionally, such a regime could be implemented cumulatively with other policy proposals recommended to address the issue of ransomware, to build a comprehensive response thereto.