MILITARY LAW REVIEW

Volume 232 **Issue 2**

High Seize—From Sail to Cyber
Utilizing the Law of Prizes to Counter Threats in Cyberspace

LIEUTENANT COMMANDER NABIL J. HEMMATI*

Study the past if you would define the future.[1]

I. Introduction

There is no domain as expansive or encompassing as cyberspace.[2] Billions of people across the world use the internet daily for economic

* Judge Advocate, United States Coast Guard. Presently assigned as Prevention Law Branch Chief, United States Coast Guard Southeast District, Miami, Florida. L.L.M., 2024, The Judge Advocate General's Legal Center and School; J.D., 2011, University of Houston Law Center; B.A., 2008, University of Texas at Austin. Previous assignments include Student, 72nd Judge Advocate Officer Graduate Course, The Judge Advocate General's Legal Center and School, United States Army, Charlottesville, Virginia, 2023-2024; Senior Special Victims' Counsel, Office of Member Advocacy, Coast Guard Headquarters, District of Columbia, 2021–2023; Legal Advisor, United States Cyber Command, Fort Meade, Maryland, 2019–2021; Response Duty Attorney, Office of Maritime & International Law – Response Division, Coast Guard Headquarters, District of Columbia, 2018–2019; Attorney Advisor, Coast Guard Office of General Law, Coast Guard Headquarters, District of Columbia, 2016–2018. Member of the Bar of Texas. This paper was submitted in partial completion of the Master of Laws requirements of the 72nd Judge Advocate Officer Graduate Course.

[1] JAMES ALEXANDER, THE BEST CONFUCIUS QUOTES 23 (2015) (EBOOK).

[2] WHITE HOUSE OFF., EXEC. OFF. OF THE PRESIDENT, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATION INFRASTRUCTURE i (2009) [hereinafter 2009 CYBERSPACE POLICY REVIEW] ("Cyberspace touches practically everything and everyone.").

exchanges, social interaction, and political discourse.[3] Warfare is becoming digital as well, with "advances in robotics, autonomy, connectivity, data in secure cloud, and AI" revolutionizing the nature of armed conflict.[4] This rapid evolution of cyber technology has resulted in gaps in international law that cybercriminals leverage to plunder the world economy with relative impunity.[5] The body of international law currently in effect has not adequately developed to address relatively novel issues presented by the internet, cybercrime, and cyberspace activity.[6]

Specifically, U.S. cyber operations may involve the seizure of vast financial assets belonging to cybercriminal organizations, which could act under the direction or authorization of unknown state actors.[7] While customary international law attributes acts by "organs of a state" or persons and entities operating under the authority of a state to that state, identifying the entity behind a cyber incident for attribution is exceptionally challenging.[8] The internet inherently fosters an atmosphere of anonymity, which creates an ideal environment for cyber actors

---

[3] Melanie J. Teplinsky, *Fiddling on the Roof: Recent Developments in Cybersecurity*, 2 AM. U. BUS. L. REV. 225, 227–28 (2013); see also Brandon T. Parker, *Piracy on the Internet High Seas: Using Hostis Humani Generis to Combat Cybercriminals*, 29 GEO. MASON L. REV. 593, 594 (2022) ("More than three billion people across the planet use the internet, and over ninety-seven percent of telecommunication utilizes the internet's infrastructure.").

[4] Richard Barrons, *The Age of Digital, Transparent Warfare Is Here*, WIRED (Jan. 06, 2023, at 07:00 AM), https://www.wired.com/story/digital-warfare/ [https://perma.cc/5VGX-BKAC].

[5] Christian Payne & Lorraine Finlay, *International Law Cannot Keep Up with Cyber-Criminals*, WORLD ECON. F. (Feb. 25, 2019), https://www.weforum.org/agenda/2019/02/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks/ [https://perma.cc/HKC9-RSXG] (stating that "[t]echnological advances continue to outpace legal developments" and discussing the "problem of attribution" as "one of the most significant hurdles" to holding cybercriminals accountable).

[6] William M. Stahl, *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity*, 40 GA. J. INT'L & COMP. L. 247, 260–61 (2011) (contending that "no comprehensive international legal framework addressing cybersecurity exists").

[7] Press Release, U.S. Dep't of Just., Justice Department Announces Seizure of Over $2.8 Million in Cryptocurrency, Cash, and other Assets (Aug. 24, 2025), https://www.justice.gov/opa/pr/justice-department-announces-seizure-over-28-million-cryptocurrency-cash-and-other-assets [https://perma.cc/PX8V-CPG8].

[8] Brian J. Egan, *International Law and Stability in Cyber Space*, 35 BERKELEY J. INT'L L. 169, 176–77 (2017).

engaged in malicious activity to thrive.[9] Additionally, states that operate in cyberspace often utilize technology to mask their identities to evade attribution purposefully.[10]

This article proposes a possible solution that looks to the past to solve the challenges of the future. A previously established customary international law tradition—the Law of Prizes under Admiralty Law—provides a viable legal framework for the U.S. government to seize cryptocurrency or other financial assets from criminal organizations operating in the cyber domain, regardless of attribution. Just as it was applied during the Age of Sail to seize pirates' treasure, prize law can hit cybercriminals where it hurts the most—their wallets.

This article proceeds in four parts. Section II focuses on the current threat posed by cybercriminals and proposes treating such actors as modern-day pirates. Section III examines the inadequacy within the current body of international law to combat malicious cyber activity, specifically ransomware attacks. Section IV explores the historical development and application of prize law. Finally, Section V concludes by laying out a practical proposal for how the United States may utilize prize law to deter and combat modern cybercriminals.

II. The Growing Cyber Threat

Over the past few decades, the threat of malicious cyber activity against the United States has risen alarmingly despite the government's recognition of the danger. In May 2009, within four months of taking office, the Obama Administration published a concerning report expressing doubt that the United States could protect itself against cyber threats.[11] This report found that the United States' internet-based digital

---

[9] Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 PENN ST. L. REV. 1005, 1013–14 (2015).

[10] *See, e.g.*, John P. Carlin, *Detect, Disrupt, Deter: A Whole-Of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 409 (2016) ("An attacker in Eastern Europe that uses a botnet of compromised computers in the Middle East to conduct a DDoS attack against a U.S. target creates a false narrative that actors located in the Middle East were responsible for that act.").

[11] 2009 CYBERSPACE POLICY REVIEW, *supra* note 2 ("Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations.").

infrastructure was "not secure or resilient," and the government was not adequately organized to address threats in cyberspace "now or in the future."[12] A month later, the then-titled Secretary of Defense Robert Gates issued a memorandum directing the creation of United States Cyber Command (USCYBERCOM) to confront the threats faced in cyberspace.[13]

Despite the U.S. government's efforts to counter the threat of malicious cyber activity, cybercrime is on the rise.[14] Some of these activities involve data theft, such as the complex cyber intrusion of the SolarWinds Orion software in 2020, which gave foreign hackers access to an unprecedented amount of U.S. government information.[15] Some of them are politically motivated, such as the North Korean-affiliated hack of Sony Pictures in 2014, which cost Sony an estimated $110 million in loss of confidential data.[16] While these examples are notable, malicious cyber activity is not only a threat to large companies and the U.S. government. Cybercriminals compromise the credit card information of individual U.S. consumers and cause millions of dollars in losses to banks

---

[12] *Id.*

[13] Memorandum from Sec'y of Def. to Sec'ys of the Mil. Dep'ts et al., subject: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (June 23, 2009).

[14] Heather L. Meadows, *Keeping Your Firm Cyber-Safe: Solutions Born of Experience*, 83 ALA. LAW. 28, 29 (2022) (The FBI's Cyber Division received a 400% increase in the number of cyber-related complaints since the outset of the COVID-19 pandemic.).

[15] Kari Paul & Lois Beckett, *What We Know – and Still Don't – About the Worst-Ever US Government Cyber-Attack*, THE GUARDIAN (Dec. 19, 2020, at 02:57 PM), https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government [https://perma.cc/Y9EV-9GHY]. For a technical summary of the SolarWinds compromise, *see The SolarWinds Cyber-Attack: What You Need to Know*, CTR. FOR INTERNET SEC. (Mar. 15, 2021), https://www.cisecurity.org/solarwinds [https://perma.cc/WCE9-YLQJ].

[16] Brent Lang, *Sony Could Lose $75 Million on 'The Interview' (Exclusive)*, VARIETY (Dec. 18, 2014, at 05:38 PM), https://variety.com/2014/film/news/sony-could-lose-75-million-on-the-interview-exclusive-12011382506/ [https://perma.cc/2KA8-Z654] (explaining the $75 million loss included production and promotion costs); *see also* Robert Lemos, *Sony Pegs Initial Cyber-Attack Losses at $35 Million*, EWEEK (Feb. 5, 2015), https://www.eweek.com/security/sony-pegs-initial-cyber-attack-losses-at-35-million/ [https://perma.cc/E783-DEAH] (citing Sony's CFO announcement that Sony would pay $35 million in investigation and remediation fees, though the actual cost is expected to be closer to $100 million).

and other businesses.[17] These threats will continue to grow, with the global cost of cybercrime expected to rise exponentially from $9.22 trillion in 2024 to $13.82 trillion by 2028.[18]

A. The Devastating Proliferation of Ransomware

In this rising field of cybercrime, one tactic poses the greatest threat to order and stability in cyberspace.[19] This is the utilization of "Ransomware-as-a-Service" (RaaS) as a business model by cybercriminal organizations to develop and release malicious software to any customer willing to pay for their services.[20] These subscription-based services enable third parties to utilize pre-packaged ransomware tools to carry out malicious cyber activities.[21] The popularity of RaaS has skyrocketed, with global ransomware attacks increasing by 102% from 2020 to 2021, occurring an estimated every 11 seconds.[22] In the United States alone, there were approximately 145.2 million ransomware attacks in 2020, increasing 139% from 2019.[23] Globally, reported ransomware attacks

---

[17] B. Nathaniel Garrett, *Taming the Wild Wild Web: Twenty-First Century Prize Law and Privateers as a Solution to Combating Cyber-Attacks*, 81 U. CIN. L. REV. 683, 692 (2013); s*ee also* Lemos, *supra* note 16 (discussing $148 million in losses to Target due to theft of credit card and personal information in 2013 and $62 million cost to Home Depot as a result of a data breach of 56 million consumer records in September 2014).

[18] Anna Fleck, *Cybercrime Expected to Skyrocket in Coming Years*, STATISTA (Feb. 22, 2024), https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/ [https://perma.cc/2K2Q-MAKV].

[19] Jake C. Porath, *Typing a Terrorist Attack: Using Tools from the War on Terror to Fight the War on Ransomware*, 50 PEPP. L. REV. 139, 148 (2023) (claiming "the greatest national security threat to the United States come from the "Ransomware-as-a-Service (RaaS) model").

[20] *Id.*

[21] Meadows, *supra* note 14, at 33.

[22] Steve Morgan, *Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) By 2021*, CYBERCRIME MAG. (Oct. 21, 2019), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/ [https://perma.cc/6WFD-F3PG]; *see also* Check Point Research Team, *The New Ransomware Threat: Triple Extortion*, CHECK POINT (May 12, 2021), https://blog.checkpoint.com/security/the-new-ransomware-threat-triple-extortion/ [https://perma.cc/RQZ3-G7XL].

[23] Clare Stouffer, *115 Cybersecurity Statistics and Trends You Need to Know in 2021*, NORTON (Aug. 9, 2021), https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html [https://perma.cc/YW8Y-7628] (citing 2020 research conducted by SonicWall in *New SonicWall Research Finds Aggressive*

increased nearly 104% from 2022 to 2024.[24] Ransomware is now the most prevalent form of cybercrime.[25]

Cybercriminals providing RaaS facilitate a troubling increase in cybercrime by enabling other criminals, who are otherwise technologically unsophisticated, to conduct devastating, malicious cyber activities.[26] Attribution is especially difficult, as these non-state cyber actors may not have any known official ties or affiliation to a foreign government.[27] These non-state actors operate as cybercriminal gangs or terrorist organizations for hire, conducting ransomware attacks against government and private sector entities alike.[28] These groups are generally motivated financially rather than ideologically, and often operate out of foreign jurisdictions, making it especially challenging to enforce laws against their cybercriminal activity.[29] In some cases, these jurisdictions

---

Growth in Ransomware, Rise in IoT Attacks, SONICWALL (Oct. 29, 2020), https://www.sonicwall.com/news/new-sonicwall-research-finds-aggressive-growth-in-ransomware-rise-in-iot-attacks [https://perma.cc/A7C8-MW65]).

[24] CYBER THREAT INTEL. INTEGRATION CTR., OFF. OF THE DIR. OF NAT'L INTELLIGENCE, WORLDWIDE RANSOMWARE, 2024: INCREASING RATE OF ATTACKS TEMPERED BY LAW ENFORCEMENT DISRUPTIONS (Feb. 2025) (reporting that 2024 also saw a $75 million ransom paid to the Dark Angels cybercriminal group by a Fortune 50 company, currently the largest known cyber ransom in history).

[25] Liam P. Bradley, *Was the Colonial Cyberattack the First Act of Cyber War Against the U.S.? Finding the Threshold of War for Ransomware Attacks*, 96 ST. JOHN'S L. REV. 487, 488 (2022).

[26] Meadows, *supra* note 14, at 33.

[27] Tomohiro Mikanagi, *Application of the Due Diligence Principle to Cyber Operations*, 97 INT'L L. STUD. 1019, 1025 (2021) ("A State conspiring to conduct malicious cyber operations but hoping to hide its involvement would use a person or group of persons ostensibly not working for it.").

[28] Porath, *supra* note 19, at 172.

[29] Marian K. Riedy & Bartlomiej Hanus*, It is Just Unfair Using Trade Laws to "Out" Security Software Vulnerabilities*, 48 LOY. U. CHI. L.J. 1099, 1103 (2017) (stating the majority of cybercriminals are motivated by "direct or indirect financial gain" while other motivations such as ideology "rarely play a role"); *see* Mary Greer & Tara Mobaraki, *#CyberspaceIRL: Rule of Law Approaches to Virtual Threats*, 2019 A.B.A. RULE L. INITIATIVE 15 ("Without a consensus on applicable law and coordinating strategies, offenders may be able to evade prosecution across international borders by taking advantage of enforcement gaps, or weak or conflicting laws."); *see also* Porath, *supra* note 19, at 146 (noting "the majority of cyberattacks are launched from Russia and other former Soviet-bloc countries, where diplomatic ties are frayed and no extradition agreements exist").

may even provide a "safe harbor" for cybercriminals to operate RaaS as long as they ensure that their operations are not unleashed domestically.[30]

The 2021 ransomware attack against Colonial Pipeline demonstrates the devastating potential of RaaS.[31] In May 2021, Colonial Pipeline, a U.S. oil pipeline system, was the victim of a ransomware attack that caused the company to shut down operations that provided the East Coast of the United States with nearly half of its fuel.[32] Colonial Pipeline's operations were halted for six days until a $5 million ransom was paid to hackers.[33] While a non-state cyber actor, DarkSide, was identified as providing the RaaS behind the Colonial Pipeline attack, the affiliate that actually purchased the malware to execute the attack has not been publicly identified.[34] The individuals who belong to DarkSide are also not publicly known, though the group is suspected to be based in Russia or Eastern Europe.[35] In an interesting twist, DarkSide released a public statement criticizing its affiliate's targeting of Colonial Pipeline, further evidencing that non-state actors do not necessarily share the ideology of those who hire them.[36] Eventually, the Federal Bureau of Investigation (FBI) was able to recover the encryption key associated with the account to which

---

[30] Dustin Carmack, *What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast*, HERITAGE FOUND. (May 20, 2021), https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hacker-group-just-wreaked-havoc [https://perma.cc/N9MK-GT87] (cites the example of Russia as a country that allows cybercriminals to operate in such a manner).

[31] Joe Walsh, *Ransomware Attack Shuts Down Massive East Coast Gasoline Pipeline*, FORBES (May 8, 2021, at 02:18 PM), https://www.forbes.com/sites/joewalsh/2021/05/08/ransomware-attack-shuts-down-massive-east-coast-gasoline-pipeline/?sh=54f23a466625 [https://perma.cc/BF9Y-A2LF].

[32] Kim Lyons, *Colonial Pipeline Says Operations Back to Normal Following Ransomware Attack*, THE VERGE (May 15, 2021, at 01:44 PM), https://www.theverge.com/2021/5/15/22437730/colonial-pipeline-normal-ransomware-attack-fuel [https://perma.cc/FPM6-PQF2].

[33] *Id.* (reporting that Colonial Pipeline resumed operations after a six-day shutdown and paying $5 million to hacking group DarkSide).

[34] Porath, *supra* note 19, at 144.

[35] *Compare* Timothy Gardner, *Cyberattack Exposes Lack of Required Defenses on U.S. Pipelines*, REUTERS (May 12, 2021, at 03:07 PM), https://www.reuters.com/technology/cyberattack-exposes-lack-required-defenses-us-pipelines-2021-05-12/ [https://perma.cc/7XQM-DD5S], *with* Carmack, *supra* note 30 (indicating DarkSide "is part of a constellation of criminal actors . . . that emanate from Russia and its former Soviet states, as well as North Korea, China, Syria, and Iran").

[36] Porath, *supra* note 19, at 158.

the ransom money was paid, as well as approximately half of the money ($2.3 million).[37]

B. State Actors in Cybercrime

Though the case of Colonial Pipeline resulted in some ransom money recovery, the question is still unresolved: Who hired DarkSide for the malware to carry out the attack? While the Biden Administration avoided blaming Russia for the attack, President Biden assigned some responsibility to Russia to hold the hackers accountable.[38] This highlights the issue of state involvement, either directly or permissively, in cybercrime.

Over five dozen countries are known to be developing cyber capabilities.[39] These states often utilize proxies to carry out unlawful activities to avoid accountability under international law and "assert plausible deniability."[40] Foreign state actors such as Russia, China, Iran, and North Korea pose a cyber threat to U.S. national security, utilizing cyber operations as a powerful force multiplier, giving them an advantage in an asymmetric conflict against a traditionally more powerful U.S. military.[41] These foreign state actors tend to use cyber-attacks to target U.S. military technology, critical infrastructure, and the defense industrial

---

[37] Vanessa Romo, *How a New Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back*, NPR (June 8, 2021, at 02:08 AM), https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac [https://perma.cc/24L3-MGRR].

[38] Lauren Egan, *Biden Says No Evidence Russian Government was Involved in Pipeline Hack*, NBC NEWS (May 10, 2021, at 03:25 PM), https://www.nbcnews.com/politics/white-house/biden-says-no-evidence-russian-government-was-involved-pipeline-hack-n1266866 [https://perma.cc/BGB2-UF7H]; *see also* Morgan Chalfant, *Biden Administration Says Russia Arrested Colonial Pipeline Hacker*, THE HILL (Jan. 14, 2022, at 05:31 PM), https://thehill.com/homenews/administration/589850-biden-administration-says-russia-arrested-colonial-pipeline-hacker/ [https://perma.cc/UM88-DWAB] (discussing Russia's arrest of one of the hackers alleged to be behind the Colonial Pipeline attack).

[39] Bagdasarova, *supra* note 9, at 1020 (quoting Shane Harris, *China Reveals Its Cyberwar Secrets*, DAILY BEAST (Mar. 18, 2015), https://www.thedailybeast.com/china-reveals-its-cyberwar-secrets/ [https://perma.cc/6RHP-K2NX]).

[40] Carter D. Westphal, *Cyber Enablement and Control: Rehabilitating State Responsibility in Cyberspace*, 126 PENN ST. L. REV. 809, 812 (2022).

[41] U.S. DEP'T OF DEFENSE, SUMMARY: 2023 CYBER STRATEGY OF THE DEPARTMENT OF DEFENSE 4-5 (2023) [hereinafter 2023 CYBER STRATEGY].

base.[42] Russia's Federal Security Service (FSB)[43] is a prime example of such a cyber adversary, notable for its involvement in cyber espionage against states and private companies.[44] One of the FSB's components, Center 18, is believed to be behind several instances of cyber espionage against the United States and the United Kingdom.[45] The FSB has also been identified as the source behind a major hack of Yahoo and has been involved in "intrusion campaigns against U.S. and international oil refineries, nuclear facilities, and energy companies."[46] Russia's military intelligence service, the Main Intelligence Directorate (GRU), has also been identified by the U.S. Department of Justice as the source behind several cyber operations that targeted electrical grids, elections, and hospital systems.[47]

While generally operating to further their national strategic goals, state actors also have a strong financial incentive to engage in cybercriminal activity due to the "low cost and high yield" of such tactics.[48] For example,

---

[42] 2023 CYBER STRATEGY, *supra* note 41*;* U.S. DEP'T. OF DEF., DEFENSE INDUSTRIAL BASE CYBERSECURITY STRATEGY 2024, at 5 (2024).

[43] Robert W. Pringle, *Federal Security Service*, BRITANNICA (Dec. 19, 2023), https://www.britannica.com/topic/Federal-Security-Service [https://perma.cc/UG7L-L2Y7] (defining the FSB as Russia's internal security and counterintelligence service, and a successor agency to the Soviet KGB).

[44] Gordon Corera, *Russia Hacking: 'FSB in Years-Long Cyber Attacks on UK', Says Government*, BBC (Dec. 07, 2023, at 07:27 AM), https://www.bbc.com/news/uk-politics-67647548 [https://perma.cc/3LG4-M56V] (noting the FSB is suspected to be involved in cyber espionage since at least 2015, including stealing U.S.-U.K. trade documents in 2019).

[45] *Id.*

[46] Jacob Rasch, *Justice Department Announces Indictments of Russian Hackers in Yahoo Hacks*, 33 INT'L ENF'T L. REP. 108 (2017) (discussing that in 2017, a U.S. federal court charged two FSB officers for hacking Yahoo); *see also* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, DEP'T OF HOMELAND SEC., JOINT CYBERSECURITY ADVISORY: TACTICS, TECHNIQUES, AND PROCEDURES OF INDICTED STATE-SPONSORED RUSSIAN CYBER ACTORS TARGETING THE ENERGY SECTOR 1 (2022), https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-083a [https://perma.cc/LN3W-GUU6] (discussing the Department of Justice unsealed indictments of three FSB officers for involvement in cyber operations against U.S. critical infrastructure).

[47] Bradley, *supra* note 25, at 493 (citing an example of six GRU officers charged by the U.S. Department of Justice for crimes related to "causing blackouts in the Ukrainian electrical grid, interference in French elections, and delays in Pennsylvania hospital systems").

[48] Xu Manshu, *Beyond Public Cyber Attribution: Reflections and Responses*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Mar. 28, 2022), https://carnegieendowment.org/research/2022/03/managing-us-china-tensions-over-public-cyber-attribution?lang=en [https://perma.cc/4TY3-YFXA].

North Korea is known to utilize cryptocurrency stolen from ransomware attacks to fund its nuclear missile program.[49] Despite state involvement in malicious cyber activity, it can be challenging to determine whether a given hacker group is a proxy for government cyber activity or if they are an independent entity operating at the direction of the foreign government.[50] Unlike a physical domain, there are no flags or uniforms worn in cyberspace that can officially tie a malicious cyber group to a specific state.[51] The existence of cyber technology is also much more difficult to detect than conventional weapons that could make attribution to a particular state easier.[52] Investigators of cybercrime must often rely on analyzing the tactics and tools used in a particular cyber intrusion to associate it with a specific state actor.[53] This leads to the challenge of determining attribution, which continues to cloud the distinction between state actors like the FSB, non-state criminal organizations like DarkSide, and state-affiliated or proxy actors.

C. The Proxy-State Actors

While states may have their own agencies conducting cyber operations, they may contract any number of cybercriminal organizations to carry out malicious cyber activity at their direction in order to obscure

---

[49] Sean Lyngaas, *Half of North Korean Missile Program Funded by Cyberattacks and Crypto Theft, White House Says*, CNN (May 10, 2023, at 11:23 AM), https://www.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html [https://perma.cc/NTG8-ANQA] (quoting a White House official that "up to a third" of North Korea's missile program is funded by malicious cyber activity, as North Korean hackers have stolen billions of dollars from banks and cryptocurrency firms, constituting a major revenue stream for the government).

[50] 2023 CYBER STRATEGY, *supra* note 41, at 5 ("Ostensibly independent hackers in the PRC, for instance, target U.S. companies that produce technology relevant to the PRC's military priorities.").

[51] Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J. L. & TECH. 376, 417 (2018) ("After all, hackers do not wear uniforms in cyberspace.").

[52] Stephen Moore, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C.J. INT'L L. & COM. REG. 223, 243 (2013) ("Perhaps for this reason, to date, no cyber attack has been conclusively attributed to a state.").

[53] Tran, *supra* note 51, at 394–98 (discussing the 2014 Sony Hack, which contained noted similarities to North Korea's DarkSeoul attack against South Korean banks, and the 2016 Democratic National Convention hack, where the hackers utilized cyber tools and code that were identical to tools known to be used by the Russian FSB).

their involvement.[54] States may also support non-state groups that are not officially affiliated with a state, but who operate with that state's tacit approval and coordination.[55] These proxy groups are sometimes identified by colorful nicknames like Cozy Bear, Helix Kitten, the Lazarus Group, or Double Dragon.[56] They may be ideologically motivated but have financial incentives as well.[57] This category of cybercriminals could include non-state actors providing RaaS that have been hired by a state,[58] or a nationalist 'hacktivist' group defacing a foreign website to show support for their government.[59] These groups are incentivized to act due to foreign state support and protection of their illicit cyber activities.[60] If modern cybercriminals are likened to pirates, then state-affiliated actors are privateers, conducting sanctioned piracy with spoken or unspoken permission from the state.[61]

---

[54] COLIN ANDERSON & KARIM SADJADPOUR, IRAN'S CYBER THREAT: ESPIONAGE, SABOTAGE, AND REVENGE 1 (Carnegie Endowment for Int'l Peace, 2018), https://carnegieendowment.org/research/2018/01/irans-cyber-threat-espionage-sabotage-and-revenge?lang=en [https://perma.cc/HJW7-FPSE] (stating "Tehran often masks its cyber operations using proxies to maintain plausible deniability"); *see also* Clare Duffy, *Here's What We Know So Far About the Massive Microsoft Exchange Hack*, CNN (Mar. 10, 2021, at 07:04 AM), https://www.cnn.com/2021/03/10/tech/microsoft-exchange-hafnium-hack-explainer/index.html [https://perma.cc/96KF-L6TD] (discussing the Microsoft Exchange hack attributed to a Chinese state-sponsored group, Hafnium, despite the Chinese Ministry of Foreign Affairs announcing China "firmly opposes and fights all forms of cyber-attacks and thefts in accordance with the law"); *see also* Rasch, *supra* note 46 (stating "the Russian government utilizes hackers for hire" in order to maintain "plausible deniability").

[55] ANDERSON & SADJADPOUR, *supra* note 54, at 17 (stating "the relationships between proxies and governments can range from passive support to complete control").

[56] Edvardas Mikalauskas, *The World's Most Dangerous State-Sponsored Hacker Groups*, CYBERNEWS (Feb. 16, 2021), https://cybernews.com/editorial/the-worlds-most-dangerous-state-sponsored-hacker-groups/ [https://perma.cc/3XUM-V49N].

[57] 2023 CYBER STRATEGY, *supra* note 41, at 5 ("U.S. interests in cyberspace are also threatened by *profit-motivated* transnational criminal organizations: ransomware gangs, hacktivists, and state-sponsored cyber mercenaries.") (emphasis added); *but see* ANDERSON & SADJADPOUR, *supra* note 54, at 24 (indicating that Iran threat actors "may be nationalists or ideologically aligned with the regime, [but] they do not appear to be enrolled members of the military or security apparatus").

[58] *See supra* notes 18–35 and accompanying text.

[59] *See infra* note 63 and accompanying text.

[60] 2023 CYBER STRATEGY, *supra* note 41, at 5 ("Russia, Iran, and North Korea all provide safe havens to ransomware gangs and their own state employees involved in cybercrime.").

[61] Garrett, *supra* note 17, at 701 (drawing on the metaphor of hackers as privateers to describe some state-backed hacker groups who go after malicious cyber actors).

The Islamic Republic of Iran, in particular, is known for its extensive use of state-affiliated actors to carry out its malicious cyber campaigns.[62] Drawing upon amateur hacking groups engaged in political cyber vandalism and motivated by nationalism, the Iranian regime evolved these originally independent defacement activities into state-affiliated activities.[63] From late 2012 to mid-2013, the Islamic Revolutionary Guard Corps contracted two private Iranian computer security companies, ITSecTeam and Mersad Company, to launch distributed denial of service (DDoS) attacks against U.S. banks, causing tens of millions of dollars in remediation costs.[64] One of these hackers also accessed the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam in New York.[65] Several members of these Iranian companies were also part of the Sun Army and Ashiyane Digital Security Team (ADST), Iranian hacking groups that have publicly claimed to have hacked U.S. government computer servers.[66] Notably, ADST has publicly claimed to have performed cyber operations on behalf of the Iranian government.[67] These convoluted, but interrelated, relationships between individual Iranian hackers, various hacker groups, and the Iranian government demonstrate the challenges of identifying state-affiliated cyber actors.[68]

---

[62] ANDERSON & SADJADPOUR, *supra* note 54, at 23 ("Iran uses cutout or proxy organizations, allowing it to keep some distance from the disruptive incidents and propagandistic defacements.").

[63] *Id.* at 22 ("This transition from patriotic hackers to state-aligned threat actors, and the ambiguity between civic nationalism and state involvement, mirrors the apparent development of cyber communities in China and elsewhere.").

[64] Press Release, U.S. Dep't of Just., Seven Iranians Working for the Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged [https://perma.cc/9BRK-3FGS].

[65] *Id.*

[66] Sealed Indictment at 10, United States v. Fathi et al., 1:16-cr-00048 (S.D.N.Y. Jan. 21, 2016). The Sun Army specifically claimed to have hacked National Aeronautics and Space Administration (NASA) servers and defaced nine NASA websites in 2012. *Id.*

[67] *Id.*

[68] *See e.g.*, ANDERSON & SADJADPOUR, *supra* note 54, at 25 (offering the example of an Iranian hacker indicted for attempting to extort HBO for personal financial gain who was also alleged to have targeted military systems and infrastructure on behalf of the Iranian government).

D. Cybercriminals as Modern Pirates

Today's cybercriminals launching ransomware attacks on financial institutions operate much like the pirates who sailed the high seas centuries ago, attacking and plundering merchant vessels while hiding behind the expanse of the ocean and beyond the jurisdiction of any one sovereign nation.[69] Both groups threaten the peace and security of the international community of their time and move through a domain that is used by all nations.[70]

Imagining these various categories of malicious cyber actors as modern pirates and cyberspace as the high seas in applying international law is not a novel proposition.[71] B. Nathaniel Garrett wrote in 2012 that "[h]ackers are essentially modern day pirates . . . the modern day Blackbeard and Captain Kidd of our time."[72] He compares the Internet to the ocean in several key ways.[73] Both the Internet and the ocean "revolutionized human interaction, commerce, and political interaction" and are critical to the global economy.[74] Both are also inherently lawless domains and are challenging to regulate.[75] Garrett argues that the internet today presents identical problems to the U.S. military as the ocean did in the 18th century.[76] According to Garrett, this is because the United States has not yet established the same level of dominance as it has in the other strategic domains of land, sea, air, and space.[77] In a more recent article, Brandon T. Parker presents the argument that universal jurisdiction, just as it was applied to prosecute pirates, should be applied to hold cybercriminals accountable.[78]

Treating malicious cyber actors as pirates whose crimes are an affront to all nations under international law addresses jurisdictional issues that

---

[69] Garrett, *supra* note 17, at 686–87.
[70] Parker, *supra* note 3, at 616.
[71] *Id.* at 613 (proposing that the same theories which establish international law governing the high seas can be applied in creating "an analogous legal structure that would govern cyberspace").
[72] Garrett, *supra* note 17, at 692.
[73] *Id*. at 690.
[74] *Id.*
[75] *Id.*
[76] *Id.* at 691.
[77] *Id.*
[78] Parker, *supra* note 3, at 597–98.

challenge countries when attempting to prosecute them.[79] The nature of cyberspace also includes several parallels to the high seas, which make these comparisons appropriate for building a legal framework on which to prosecute them. The following section discusses these similarities in more detail and explores how customary international law traditions can be applied to resolve the issue of attribution in cyberspace.

III. Applying Customary International Law to Cyberspace

The current body of international law does very little to regulate state conduct in cyberspace.[80] Without a well-established foundation from which they can base their practices, States may also hesitate to apply forward-leaning interpretations of international law to cyber in their relations with other states.[81] However, over the past decade, a growing consensus of cyber experts and academics has popularized the position that customary international law—defined as international law that "results from a general and consistent practice of states followed by them from a sense of legal obligation"[82]—applies to cyberspace.[83] In 2013, an international team of cyber experts at the NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia reached the unanimous consensus that "general principles of international law applied to cyberspace."[84] The United States has generally adopted this view, concluding that long-established international norms, such as customary

---

[79] *Id.* at 596–97 (arguing for universal jurisdiction under the doctrine of *hostis humani generis* be applied to cybercriminals as the "[c]urrent jurisdictional schemes do not allow for the prompt prosecution of those responsible for such acts, and thus do not function as adequate deterrents against future cybercrimes").

[80] Tran, *supra* note 51, at 384.

[81] *Id.*

[82] RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(2) (A.L.I. 1987).

[83] Egan, *supra* note 8, at 170 (confirming that "established principles of international law apply to cyberspace" while citing Harold Koh's 2012 "International Law in Cyberspace" speech at USCYBERCOM's Cyber Legal Conference). (Additionally, the author cites the 15-state United Nations Group of Governmental Experts who, in 2013, "recognized the applicability of existing international law to States' cyber activities."); *see also* Tran, *supra* note 51, at 384 (highlighting the academic view that the law of armed conflict could be applied to cyber, though it has not yet been invoked in response to a cyber-attack).

[84] Ira E. Hoffman, *International Cooperation in Combating Cyberthreats and U.S. Law*, 47 MD. BAR J. 36, 39 (2014) (citing TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 13 (Michael N. Schmitt ed., 2013)).

international law, also apply in cyberspace.[85] While these trends support applying customary international law to cyberspace, customary international law, even if applied, currently does not adequately deter malicious cyber activity.[86] A modern application of prize law, leveraging the parallels between cyberspace and the oceans, can serve as such a deterrent.

A. The Uncharted Cyber Seas

There are parallels between cyberspace and the high seas that are relevant to understanding how maritime international law can be applied to governing existing issues in cyberspace.[87] The laws of the sea were first established millennia ago as the ancient Greeks, Egyptians, and Phoenicians began trading across Mediterranean ports.[88] As these diverse political communities interacted, common legal principles governing navigation and trade needed to be established.[89] The ocean remains a venue for commerce, transportation, and communication that is available for use by all nations. However, the vast size of the high seas and its existence outside of national borders have historically rendered it a haven for "lawless" activity such as piracy.[90] Maritime law has developed to regulate this unique space and, to the extent possible, deter criminal activity by establishing laws against piracy and introducing prize law.[91]

Cyberspace presents "legal challenges similar to those encountered in maintaining order in the use of the world's oceans."[92] Cyberspace also manifests as an international space used by all nations and is, like the ocean, a "global commons" that should be governed by shared international principles.[93] Much like the high seas, cyberspace offers new

---

[85] *Id.* (citing WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 9 (May 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [https://perma.cc/KY7G-XDZZ]).

[86] *Id.* (stating "international law does little to thwart cyber-intrusions and, as many observers believe, that is not likely to change").

[87] Stahl, *supra* note 66, at 267.

[88] Gerard J. Mangone, *Commerce by Water*, 11 DEL. LAW. 28 (Spring 1993).

[89] *Id.*

[90] Garrett, *supra* note 17, at 686.

[91] *Id.* at 687–88.

[92] Stahl, *supra* note 6, at 267.

[93] Timothy Steigelman, *The Promise and Perils of Prize Law*, 19 WORLD HIST. CONNECTED 1, 17 (2022).

venues for trade and commerce that are collectively shared by the international community.[94] It, too, is vast in size, and this vastness affords cybercriminals the anonymity that encourages malicious cyber activity.[95]

However, while the Law of the Sea developed to resolve the challenges created by the oceans, the body of international law currently in effect is still insufficient to adequately address the relatively novel issues presented by the internet, cybercrime, and cyberspace activity.[96] This is where existing maritime international law can bridge the current gaps in cyber law to address these cyberspace issues.[97] For example, the United Nations Convention on the Law of the Sea (UNCLOS) establishes a duty for all nations to combat piracy as an international crime, even if that crime occurs outside that nation's territory.[98] Continuing the analogy of malicious cyber actors to pirates, UNCLOS and other customary international law traditions can "provide meaningful guidance in developing international obligations related to cybersecurity."[99] One such tradition is the practice of leveraging universal jurisdiction against criminal entities that were labeled as *hostis humani generis* by the international community.[100]

---

[94] Bagdasarova, *supra* note 9, at 1022 ("Users access the Internet for banking, entertainment, news, technological innovation, education, and consumer shopping, among other things."); *see also* Stahl, *supra* note 6, at 267 ("the Internet is shared globally and the consequences of actions taken by an Internet user in one jurisdiction can be borne globally").

[95] Bagdasarova, *supra* note 9, at 1013 ("Another characteristic of cyberspace that poses a challenge to effective regulation is the anonymity it provides to its users.").

[96] Stahl, *supra* note 6, at 260–63 ("no comprehensive international legal framework addressing cybersecurity exists"); *see also* Parker, *supra* note 3, at 596 ("Current jurisdictional schemes do not allow for the prompt prosecution of those responsible for such acts, and thus do not function as adequate deterrents against future cybercrimes.").

[97] Stahl, *supra* note 6, at 251 ("the international community should use existing international legal instruments and principles as guidance in developing a comprehensive legal framework to combat cyberaggression."). Specifically, Stahl highlights the United Nations Convention on the Law of the Sea as such an international legal document. *Id.*

[98] *Id.*; *see also* U.N. Convention on the Law of the Sea art. 100, Dec. 10, 1982, 1833 U.N.T.S. 397 ("All States shall cooperate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any State.").

[99] Stahl, *supra* note 6, at 251.

[100] *See generally* Parker, *supra* note 3 (arguing that universal criminal juristicion should be expanded to cyberspace).

B. Cybercriminals as *Hostis Humani Generis*

Cyber actors conducting criminal activity in cyberspace, similar to pirates operating during the age of sail, should be treated as *hostis humani generis,* where any nation can exercise jurisdiction over them based on their illicit activity.[101] The doctrine of *hostis humani generis*, or "enemy of all mankind," allows nations to prosecute certain criminals "based not on their nationality, location, or criminal target, but upon the very offense itself."[102] This concept of universal jurisdiction over certain crimes first became widely adopted against pirates in the 16th century.[103] Despite the widespread state practice of "sanctioned piracy" or privateering, which can be likened to the state-sponsored cyber activity today, piracy was viewed as an especially heinous crime that threatened the legitimacy of all states and one that was "outside the bounds and powers of a single state" to prosecute.[104] Brandon T. Parker does an exceptional, in-depth analysis of why cybercriminals should fall under the label of *hostis humani generis* today by looking at how cybercrime threatens the authority and stability of states as well as the jurisdictional challenges created by cyberspace.[105] Should cybercriminals be treated as the pirates of today, they can be prosecuted by any jurisdiction under the doctrine of *hostis humani generis*, including seizing their assets and potentially disposing of them in a prize court.[106]

C. Current Cyber Law

While binding international law is based on both customary international law and treaties, there is still no "Law of Cyberspace" in the same fashion as we have the "Law of the Sea."[107] The relatively new nature of cyberspace presents challenges to determining appropriate state behavior, as there is still very little state-admitted practice in cyberspace

---

[101] *Id.*
[102] *Id.* at 597.
[103] *Id.* at 602.
[104] *Id.* at 602–03.
[105] *Id.* at 616.
[106] Parker, *supra* note 3, at 601 (stating "should a pirate be caught, it did not matter where they were from, who they were targeting, or where effects were felt. Once caught, a pirate could be tried, convicted, and likely executed by any state.").
[107] Westphal, *supra* note 40, at 815; *see also* Tran, *supra* note 51, at 384 ("No international laws or treaties expressly regulate the use of cyber-attacks.").

that would lead to an *opinio juris* for modeling state practices.[108] Additionally, the very nature of cyberspace makes it difficult for states to establish a universal structure to regulate.[109] However, states still tend to follow established international law principles when conducting cyber operations.[110] While there is a limited cyber-specific framework based on international treaties and domestic laws, discussed below, the additional lack of cyber-specific customary international law requires the general application of customary international principles to fill in gaps in the framework.[111]

1. Domestic Cyber Framework

In 1986, Congress introduced the Computer Fraud and Abuse Act (CFAA) as an amendment to the Comprehensive Crime Control Act of 1984.[112] The CFAA criminalized computer "trespassing" and provided specific protections to federal government computer systems, banks, and internet use against causing damages, issuing threats, espionage, or fraud.[113] Today, the CFAA is the principal instrument used by the federal government to prosecute cybercrimes.[114] It provides for forfeitures to the United States of "[a]ny personal property used or intended to be used to commit or to facilitate the commission of any violation of [the CFAA]" and "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate [the CFAA]."[115] While the CFAA provides the United States with a framework for criminalizing certain conduct and forfeiture of assets, it does not provide any guidance on determining the source of such

[108] Westphal, *supra* note 40, at 815; *see also* Egan, *supra* note 8, at 171 (discussing the *Tallinn Manual* as an example of an initiative to help fill in gaps due to the lack of *opinio juris* concerning cyber activities).
[109] Tran, *supra* note 51, at 391 ("The internet's structural design, the tools for masking online activity, the limitation of attribution to machines, and the limits on attributing individual conduct to states comprise the numerous hurdles, technological and legal, that have often been cited as the barrier to the creation of a legal regime for regulating cyber-attacks.").
[110] Egan, *supra* note 8, at 180.
[111] Westphal, *supra* note 40, at 815.
[112] Greer & Mobaraki, *supra* note 29, at 11.
[113] *Id.* (citing 18 U.S.C. § 1030(a)).
[114] Bradley, *supra* note 25, at 492.
[115] 18 U.S.C. § 1030(j).

conduct.[116] Nearly three decades later, Congress passed the Cybersecurity Information Sharing Act (CISA), which provided an avenue for private companies and the government to share cyber threat indicators.[117] Unfortunately, the existing framework of U.S. law has proven ineffective at deterring cybercrime, especially when attempting to apply domestic laws extraterritorially against foreign entities.[118]

2. International Cyber Framework

Though the international community recognizes the need to develop a formal legal structure to govern cyberspace, this domain, by nature, is particularly difficult to regulate.[119] The first and currently only binding international treaty concerning cybersecurity is the Council of Europe Convention on Cybercrime, also referred to as the Budapest Convention.[120] The Budapest Convention provides "a legal roadmap to countries to strengthen their ability to investigate and prosecute cybercrime."[121] The Budapest Convention focuses on harmonizing the parties' domestic criminal laws on cybercrime to establish a consensus on what constitutes a crime in cyberspace.[122] Although it originally entered

---

[116] Greer & Mobaraki, *supra* note 29, at 11 (laying out the various prohibited activities criminalized by the CFAA).
[117] *Id.* at 11–12.
[118] Eric Blinderman & Myra Din, *Hidden by Sovereign Shadows: Improving the Domestic Framework for Deterring State-Sponsored Cybercrime*, 50 VAND. J. TRANSNAT'L L. 889 (2017); *see also* Bradley, *supra* note 25, at 497:

> While cybercriminals are indicted, they are usually judgment-proof. For example, Russian cybercriminals cannot be prosecuted because the U.S. lacks jurisdiction over them, and they cannot be prosecuted in Russia because hacking U.S. entities is not a violation of Russian law. Furthermore, documents which expose DOJ and FBI methodologies are revealed to the public when used as evidence in court, which can frustrate their efforts to combat cybercrime.

Id.
[119] Bagdasarova, *supra* note 9, at 1012 ("However, four characteristics of cyberspace, and their interactions with one another, pose challenges to the development of effective cybersecurity regimes. Cyberspace is: (1) global and decentralized, (2) anonymous, (3) pervasive, and (4) constantly and rapidly evolving.").
[120] Convention on Cybercrime, Nov. 23, 2001, S. TREATY DOC. NO. 108-11, 2296 U.N.T.S. 167 [hereinafter Cybercrime Convention]; Greer & Mobaraki, *supra* note 29, at 9.
[121] *Id.* at 10.
[122] *Id.*

into force for members of the Council of Europe, a growing number of states have acceded and signed on as parties, including the United States.[123] Both Russia and China refuse to sign the Budapest Convention, arguing it violates state sovereignty.[124]

While the Budapest Convention contributes to building the international consensus on what cyber actions should be criminally punished, it does not address the issue of attribution.[125] The question of attribution presents a serious problem for the international community, as cybercriminals can leverage this gap in the existing, limited framework of cyber law to operate with impunity and without deterrence.

D. The Problem of Attribution

While there is no universal consensus among governments on what constitutes a "cyber-attack" or what law would govern such an attack, the growing view among practitioners of international law is that customary international law applies.[126] However, the problem of attribution, or identifying the source of a cyber-attack, remains one of the most challenging hurdles in cyberspace for holding malicious cyber actors accountable.[127] This challenge is fundamentally based on the structure of the internet, which involves a web of networks where information moves across multiple jurisdictions.[128] While many states criminalize certain cyber activities, enforcing those laws on individuals who reside under one jurisdiction, mask their identity, and utilize the network of a third jurisdiction to conduct their illicit activities poses a challenge that the still-

---

[123] *Id.* For a list of current countries that have joined the Budapest Convention, see also *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUR.: TREATY OFF., https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty num=185 [https://perma.cc/ZAM8-RP74] (last visited Nov. 11, 2025).
[124] Greer & Mobaraki, *supra* note 29, at 10.
[125] *See* Cybercrime Convention, *supra* note 120.
[126] Moore, *supra* note 52, at 234.
[127] Tran, *supra* note 51, at 386 ("the technological architecture of the internet makes attribution an exceedingly difficult problem").
[128] *Id.* at 387 ("Attributing cyber-attacks to their source is difficult for a number of reasons. First, the structural design of the internet and the nature of information transmission across networks complicates attribution efforts.").

developing body of cyber law does not adequately address.[129] Further complicating attribution is the absence of clear evidentiary standards under international law for holding other states accountable for their behavior.[130]

This issue of attribution first arose in the wake of the 2007 DDoS cyber-attack against Estonia, where the country's information technology (IT) infrastructure was overwhelmed over a period of 22 days.[131] Estonia blamed Russia for the attacks, though investigators suggested unaffiliated hackers were behind the cyber incident.[132] These attacks demonstrated how "focused, persistent cyber-attacks . . . could be a low-cost, but highly disruptive tool or weapon . . . designed to make attribution difficult, if not impossible."[133] The challenge of attributing cyber-attacks has led the United States to adopt the view that attribution is a political, rather than legal, decision.[134] Other scholars have advocated for the adoption of an "arsonist principle" where the international community would hold a state responsible for the actions of a non-state actor if that state "knowingly harbors" that non-state actor.[135]

These alternative approaches to attribution are problematic. Publicly attributing a cyber-attack as a political decision may be important diplomatically and have some deterrent effect,[136] but ignoring the legal aspects limits the use of courts to enforce accountability.[137] While the arsonist principle is an interesting proposal, there is no existing basis for it under international law, which applies two different tests for assigning

---

[129] Egan, *supra* note 8, at 177 (noting that the law of state responsibility under customary international law, while applicable to cyber, does not clearly establish standards or burdens for establishing legal attribution).

[130] Kristin E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 524 (2020) ("Attributing responsibility for cyberattacks to states, on the other hand, intersects with secondary international law rules regarding the evidence states must provide when accusing other states of internationally wrongful acts—an area of law that is notoriously underdeveloped even outside the cybersecurity context.").

[131] Hoffman, *supra* note 84, at 38.

[132] *Id.*

[133] *Id.*

[134] Eichensehr, *supra* note 130, at 525–26 ("the United States, United Kingdom, and most recently France and the Netherlands have asserted that publicly attributing state-sponsored cyberattacks is a political decision, not a legal one").

[135] Moore, *supra* note 52, at 245.

[136] Eichensehr, *supra* note 130, at 552, 578.

[137] *Id.* at 578.

state responsibility.[138] While, from a strictly legal perspective, states are responsible for cyber acts committed by their proxies, the tests currently utilized by the international community to assign state responsibility are especially ineffective in cyberspace.[139]

1. *Law of State Responsibility*

Customary international law on state responsibility could be examined as a basis for attribution for acts committed in cyberspace.[140] However, this approach is still imperfect due to the nature of cyber operations, where states often mask their involvement or deny responsibility.[141] Under the law of state responsibility, malicious cyber activity originating in a particular state would be attributable to that state if the perpetrators acted "pursuant to the State's instructions or under the State's direction or control, or when the State later acknowledges and adopts the operations as its own."[142] This view is consistent with the International Court of Justice's (ICJ's) opinion in *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, which established the "effective control test" for assigning state responsibility to non-state actors.[143] Under this view, it would need to be proven that a state had "total control" over a proxy for the activities of the proxy to be attributed to the state.[144] This is an onerous

[138] Catherine Lotrionte, *State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825, 855–56 (2012) (these tests being the "effective control test" and the "overall control test" which are both explored in the following section).
[139] Egan *supra* note 8, at 177 ("States cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies.").
[140] *Id.* ("From a legal perspective, the customary international law of state responsibility supplies the standards for attributing acts, including cyber acts, to States.").
[141] Lotrionte, *supra* note 138, at 899 ("A state's unwillingness to suppress cyber attacks originating within its territory has been used as a shield to deny responsibility for state action, thereby limiting the victim state's right of self-defense.").
[142] Egan, *supra* note 8, at 177.
[143] Westphal, *supra* note 40, at 823 (referencing Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27)).
[144] Collin S. Allan, *Attribution Issues in Cyberspace*, 13 CHI.-KENT J. INT'L & COMP. L. 55, 67 (2013) ("The effective control test requires a state to essentially be in total control of the non-state actors, and the state must specifically direct or enforce violations of international law.").

burden to meet even outside of cyberspace.[145] The International Criminal Tribunal for the former Yugoslavia (ICTY) also established a broader "overall control test," under which a non-state actor must be under the overall control of a state, which involves not only equipping and funding the non-state actor but also coordinating and planning its activities.[146] In 2007, the ICJ affirmed its effective control test over the ICTY's overall control test in *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnian Genocide*).[147] However, while these two tests have been applied to kinetic attacks,[148] whether they would apply to cyber operations is unestablished.

The limitations of applying the law of state responsibility to cyber operations are underscored by the absence of an established or standardized burden of proof for determining attribution in cyberspace.[149] While cyber experts have attempted to address the issue of cyberspace attribution in the latest iteration of the *Tallinn Manual*,[150] the problem remains unresolved.

2. The Tallinn Manual

In 2017, the NATO cyber initiative from Tallinn provided an updated report from experts, reflecting the development of the international community's views on cyber.[151] This "Tallinn Manual 2.0" is lauded as "the leading guide on the rules of cyberwar and codifies the customary law of cyberwarfare."[152] The *Tallinn Manual 2.0* introduced a new rule specifically addressing the issue of attribution of cyber operations

---

[145] Oona A. Hathaway, Emily Chertoff, Lara Domínguez, Zachary Manfredi, & Peter Tzeng, *Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors*, 95 TEX. L. REV. 539, 546 (2017) ("The ICJ has embraced the "effective control" test, which draws a very high bar for triggering state responsibility.").
[146] Westphal, *supra* note 40, at 824 (referencing Prosecutor v. Tadić, Case No. IT-94-1-A, Appeal Judgment, ¶ 131 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).
[147] Hathaway et al., *supra* note 145, at 550 (referencing Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶¶ 208–09, 400–01 (Feb. 26)).
[148] Westphal, *supra* note 40, at 823.
[149] Egan, *supra* note 8, at 177.
[150] Westphal, *supra* note 40, at 825.
[151] Eichensehr, *supra* note 130, at 546.
[152] Bradley, *supra* note 25, at 505–06.

conducted by non-state actors.[153] While this rule is nonbinding, it states "[c]yber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operation as its own."[154] The practical application of this rule is limited. States involved in malicious cyber activity are unlikely to acknowledge responsibility for such attacks.[155] The anonymity provided by the Internet and the plausible deniability that comes from using proxies are often what make cyber operations appealing to state actors.[156] For the first part of this rule, the *Tallinn Manual 2.0* applies the effective control test adopted by the ICJ.[157] However, as previously discussed, the effective control test's practical application in cyberspace has serious shortcomings.[158]

Treating malicious cyber actors, regardless of state affiliation, as *hostis humani generis* avoids the issue of attribution that the law of state responsibility and the *Tallinn Manual 2.0* struggle to resolve. Doing so also sets a foundation for applying prize law to the seizure of assets from malicious cyber actors.

---

[153] Westphal, *supra* note 40, at 825 (refencing rule 17 within "Tallinn Manual 2.0").

[154] INT'L GRP. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEFENCE CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 94 (Michael N. Schmitt ed., 2nd ed. 2017) [hereinafter TALLINN MANUAL 2.0]; *but see* Westphal, *supra* note 40, at 826 ("States are not legally bound by the Tallinn Manual 2.0.").

[155] Westphal, *supra* note 40, at 825 (noting that admitting to wrongdoing would eliminate a bad-faith actor's plausible deniability).

[156] *Id.* at 826 ("Consequently, the effective control test remains the ICJ standard for State responsibility, even in cyberspace, where States and non-State actors enjoy an added layer of obscurity and therefore, plausible deniability."); *see also* Moore, *supra* note 52, at 242 (quoting Remarks, Harold Koh, Legal Advisor, U.S. Dept't of State, International Law in Cyberspace (Sep. 18, 2012), https://2009-2017.state.gov/s/l/releases/remarks/197924.htm [https://perma.cc/6LYF-XKTU] ("cyberspace significantly increases an actor's ability to engage in attacks with 'plausible deniability,' by acting through proxies.")).

[157] Westphal, *supra* note 40, at 825 (citing TALLINN MANUAL 2.0, *supra* note 154).

[158] *Id.* at 833 (In order to articulate the limitations of the "effective control test," Westphal presents a hypothetical cyber scenario where "State A" suffers a cyber-attack attributed to a "Hacking Group (HG)" located in and suspected to be sponsored by "State B." He writes "[e]ven if it could be shown that State B funded, organized, supplied, equipped, selected targets for, and planned the above operation, the evidence would still be insufficient to satisfy the effective control test.").

IV. The Development of Prize Law

Revitalizing prize law to address current threats in cyberspace has received some advocacy within the past decade.[159] Timothy Steigelman suggests that prize law can be a precedent for governments to hire private companies to defend against cyberattacks.[160] B. Nathaniel Garrett examines this concept in depth, arguing that letters of marque and reprisal issued to private hackers could effectively counter cybercriminals.[161] While Garrett briefly touches on the topic of prize courts, the discussion is limited to the general need for "a special court" or "some other monitoring body" to regulate disputes in the scope of letters of marque and reprisal and to temper the conduct of potentially unethical hackers.[162] This article shifts into new territory by focusing on what these modern prize courts could look like and exploring the historical foundation on which they could be built.

A. The History of Prize Law

The Law of Prizes originated in England and France during the 13th and 14th centuries as an economic tool of warfare.[163] Other countries would soon follow suit, with Japan, Egypt, China, and the Barbary States of North Africa all developing their own systems of prize law.[164] Prize law sanctioned the wartime seizure of property on the high seas, both by the government and private individuals.[165] Merchant vessels flying the flag of an enemy nation or neutral vessels engaged in trade with the enemy could be seized, and their goods lawfully possessed through an adjudicative process governed by a prize court.[166] Private citizens working on behalf of

---

[159] Garrett, *supra* note 17, at 685–89; *see also* Steigelman, *supra* note 93, at 16–17.
[160] Steigelman, *supra* note 93, at 17.
[161] Garrett, *supra* note 17, at 685.
[162] *Id.* at 706.
[163] Andrew Clapham, *Booty, Bounty, Blockade, and Prize: Time to Reevaluate the Law*, 97 INT'L L. STUD. 1200, 1201 (2021).
[164] Steigelman, *supra* note 93, at 12 (noting that these systems generally developed later than the American, French, and British prize court systems).
[165] Garrett, *supra* note 17, at 687–88.
[166] J. Gregory Sidak, *The Quadi 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 (2005) (citing French legal scholar Georg Friedrich von Marten, who wrote in

the government, or privateers, in possession of letters of marque and reprisal, could lawfully capture and obtain title of the goods seized.[167] Privateers did not obtain ownership over the goods or vessels captured until they were condemned in a prize court.[168] The function of the prize court was to ensure the capture was considered lawful by determining the nationality of the vessel and the destination or origin of the goods, as well as providing the owners of a merchant vessel an opportunity to protest.[169] Since prize law provided a personal economic incentive for capturing civilian vessels, the prize court played an important role in legitimizing such takings.[170]

Prize law is rooted in the "rule of vicarious liability," where individual citizens were liable for the debts of their rulers.[171] In 1625, Hugo Grotius wrote that under the law of nations, "both the possessions and the acts of subjects are liable for the debt of a ruler."[172] By the 19th century, it was widely accepted that taking civilian merchant vessels as prizes was a

---

1795 that, according to Horne's translation, privateering consisted of "*attacking the enemy*, and preventing neutral subjects or friends from carrying on with the enemy a commerce regarded as illicit."); *see also* Clapham, *supra* note 163, at 1217 ("The captured property might also include enemy goods on neutral vessels, neutral goods on enemy vessels, contraband of war, or vessels caught breaching a Blockade."); *see also* Steigelman, *supra* note 93, at 3 ("[P]rizes were civilian vessels flying the enemy's flag, or even neutral colors, and their port of origin or destination may (or may not) make the ship a lawful prize.").

[167] Steigelman, *supra* note 93, at 3–4; *see* Sidak, *supra* note 166, at 468 (explaining that letters of marque were "legal authorization for private parties . . . to use force [against] a nation's enemy" while letters of reprisal were the legal authorization of "securing redress for a debt incurred by a foreign government by forcibly taking the private property of its subjects."); *but see* Garrett, *supra* note 17, at 688–89 (explaining the difference between letters of marque and letters of reprisal; the former authorizes the capture of goods outside the jurisdiction of the State while the latter applies within the jurisdiction).

[168] Tara Helfman, *The Dread Pirate Who? Challenges in Interpreting Treaties and Customary International Law in the United States*, 90 TUL. L. REV. 805, 822 (2016); *see also* Garrett, *supra* note 17, at 688 ("Once a capture had been committed on the oceans, the privateer was required to bring the captured vessel or cargo into prize courts to be condemned.").

[169] Steigelman, *supra* note 93, at 2–3.

[170] *Id.* at 4 ("It is precisely this interplay of public and private motives that required prize courts to carefully adjudicate whether captured vessels were lawful prize.").

[171] Sidak, *supra* note 166, at 469–70.

[172] 2 HUGO GROTIUS, DE JURE BELLI AC PACIS, bk. III, ch. 2, § 2, at 624 (Francis W. Kelsey trans., Clarendon Press 1925) (1625) (cited by Sidak, *supra* note 166).

Belligerent Right during naval warfare.[173] In addition to the wealth generated by such captures, there were also practical reasons for seizing civilian merchant vessels, as they could easily be impressed into the naval service and outfitted for war.[174]

Following the end of the Crimean War in 1856, the seven warring powers signed the Paris Declaration Respecting Maritime Law (Paris Declaration), abolishing privateering and prohibiting letters of marque and reprisal.[175] The Paris Declaration also prohibited the capture of enemy ships carrying neutral goods or neutral ships carrying enemy goods, with an exception for "contraband of war."[176] Though an additional 55 states would sign the Paris Declaration, the United States was not a signatory and has preserved its right to issue letters of marque and reprisal.[177] While the Paris Declaration is commonly misunderstood as marking the end of privateering and prize law, the United States has maintained a rich history of prize law, both before and after 1856.[178]

---

[173] Clapham, *supra* note 163, at 1217; *see also id.* at 1215 (stating "maritime warfare has traditionally included a Belligerent Right to capture enemy merchant (civilian) ships and aircraft").

[174] *Id.* at 1205 (emphasizing that "historically it was considered that all merchant sailors could be easily redeployed to the armed forces, and that merchant ships could potentially easily be requisitioned for the war effort").

[175] Declaration Respecting Maritime Law, Apr. 16, 1856, 46 BSP 26 (U.K.) [hereinafter Paris Declaration]; *see also* Garrett, *supra* note 17, at 689 (providing a general discussion of the backdrop which produced the Paris Declaration).

[176] Paris Declaration, *supra* note 175, art. 2.

[177] *State Parties and Signatories to the Paris Declaration*, Apr. 16, 1856, INT'L HUMANITARIAN L. DATABASES, https://ihl-databases.icrc.org/en/ihl-treaties/paris-decl-1856/state-parties [https://perma.cc/35PK-7B5L] (last visited Dec. 25, 2025) (containing a list of the 55 state parties and signatories); *see also* Garrett, *supra* note 17, at 689 (noting that the United States was not a signatory of the Paris Declaration and "preserved its ability to use letters of marque and reprisal in the future").

[178] Anna Price, *Pirates, Privateers, and Civil War Maritime Laws*, LIBR. OF CONG. BLOGS, (May 28, 2020), https://blogs.loc.gov/law/2020/05/pirates-privateers-and-civil-war-maritime-laws/ [https://perma.cc/K2XB-FMJP] (arguing that "[t]he practice of privateering was all but eliminated by" the Paris Declaration); *but see* Steigelman, *supra* note 93, at 14 ("It is a common opinion that the Paris Declaration abolished privateering, but that opinion is both a misunderstanding of fact, and a misapprehension of the nature of international law.").

B. Prize Law in the United States

Prize law was introduced to the New World when England established prize courts (known then as "colonial vice admiralty courts") in the American colonies to adjudicate seizures during the Seven Years' War.[179] Though the issuance of letters of marque and reprisal began to fade in Europe towards the end of the 18th century, the practice persisted in America during and immediately after the Revolutionary War.[180] The use of privateers by the American colonies was critical in their struggle for independence, as these colonies lacked the military strength and financial resources of the European powers.[181] American privateers augmented the might of the Continental Navy, but more importantly, helped fill the young nation's treasury by seizing over $10 million in British property.[182]

The importance of prize law during the foundation of America is demonstrated by the inclusion of letters of marque and reprisal as an enumerated power of Congress in both the Articles of Confederation and the U.S. Constitution.[183] The Articles of Confederation granted Congress the authority to issue letters of marque and reprisal "in times of peace."[184] The U.S. Constitution grants Congress the power "[t]o declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water."[185] Though the power to grant letters of marque and reprisal appears linked to Congress's power to declare war, its specific inclusion as a separate power reflected the Framers' understanding that issuing letters of marque and reprisal was not inherently included in the power of war.[186] During the Quasi-War with France, which followed from 1798 to 1800, a formal declaration of war did not exist, but Congress

---

[179] Steigelman, *supra* note 93, at 8.
[180] Sidak, *supra* note 166, at 474.
[181] *Id.*; *see also* Garrett, *supra* note 17, at 694 ("The United States may never have won the American Revolution without the help of naval-privateer assistance.").
[182] Sidak, *supra* note 166, at 475 (this would be "roughly $100 million to $200 million in 2003 dollars").
[183] *Id.* at 476–80.
[184] ARTICLES OF CONFEDERATION of 1781, art. IX, para. 1.
[185] U.S. CONST. art. I, § 8, cl. 11.
[186] Jules Lobel, *Covert War and Congressional Authority: Hidden War and Forgotten Power*, 134 U. PA. L. REV. 1035, 1060 (1986) ("the original drafts of the Constitution had not mentioned letters of marque and reprisal at all" but were introduced by Elbridge Gerry due to the belief they were not included in the power of war); *see also* Sidak, *supra* note 166, at 477 ("Gerry's proposed addition passed unanimously in committee.").

authorized reprisals against any vessel engaged in trade with France.[187] The United States also issued letters of marque and reprisal against British vessels during the War of 1812.[188] While the United States declined to sign the Paris Declaration ban on privateering, it has not issued letters of marque and reprisal to privateers since the War of 1812.[189] However, during the American Civil War, the Confederacy continued to rely heavily on letters of marque and reprisal issued to privateers to target Union shipping.[190] Though the Union did not utilize privateers, the Union Navy responded by seizing Confederate vessels as prizes.[191] Both sides litigated these maritime captures in prize court.[192] Nevertheless, both the Union and the Confederacy formally prohibited the seizure of neutral property on enemy ships and enemy property on neutral ships, in alignment with the principles of the Paris Declaration.[193]

Though the Civil War marked an end to American privateering, the use of prize courts to adjudicate the capture of civilian vessels by the government persisted.[194] U.S. naval warships captured prizes through combat during the Spanish-American War in both the Atlantic and

---

[187] Sidak, *supra* note 166, at 481 ("In the Quasi War of 1798 to 1800, President John Adams did not seek and Congress did not issue a formal declaration of war against France in response to her seizure of American ships. Instead, Congress authorized reprisals against French vessels.").

[188] Lobel, *supra* note 186, at 1045.

[189] C. Kevin Marshall, *Putting Privateers in Their Place: The Applicability of the Marque and Reprisal Clause to Undeclared Wars*, 64 U. CHI. L. REV. 953, 954 (1997) ("[T]he United States has not issued letters of marque and reprisal since the War of 1812."); *see* Garrett, *supra* note 17, at 694 (expressing the view that as the American Navy grew in strength, the need for privateers diminished).

[190] Lobel, *supra* note 186, at 1045.

[191] Steigelman, *supra* note 93, at 14 ("During the American Civil War soon after the Paris Declaration, there was Confederate privateering, as well as prize-taking and prize litigation in both the United States and the Confederacy."); *see also* Theodore M. Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 247 (2009) ("Although Congress granted President Lincoln the authority to issue letters of marque and reprisal, he declined to issue them.").

[192] Steigelman, *supra* note 93, at 14; *see also* Cooperstein, *supra* note 191 ("Many prizes were taken by United States Navy warships however, and found their way into the federal courts.").

[193] Clapham, *supra* note 163, at 1221 ("[I]n the American Civil War, both the North and the South formally approved the rules prohibiting the seizing of enemy property on neutral ships and neutral property on enemy ships, in their relations with neutral shipping from France and Great Britain.").

[194] Steigelman, *supra* note 93, at 14.

Pacific.[195] In the landmark prize case *The Paquete Habana*, the Supreme Court applied customary international law to rule that Cuban fishing vessels captured at the outset of the Spanish-American War were exempt from seizure as prize.[196] World War I also generated some "prize and prize-related litigation" in U.S. federal courts.[197] One notable case, arising prior to the United States entry into the war, involved a German vessel bringing a captured British vessel to a U.S. port to be condemned as prize.[198] The vessel and cargo were returned to the British, with the U.S. Supreme Court ruling that Germany violated American neutrality by bringing the vessel into the United States for prize adjudication.[199] The last U.S. prize court case arose out of the 1941 capture of the German blockade runner *Odenwald* by the U.S. Navy.[200]

Though prize-taking by the United States has not occurred since the 1940s, the Vietnam War generated new interest in prize law as it related to the President's authority to conduct war.[201] In 1961, the Office of Legal Counsel of the Department of Justice released a memorandum suggesting that Cuban vessels violating a blockade could be seized as prizes if "deemed to have been made 'during war.'"[202] This interest in prize law has continued to arise periodically in the United States to the present. In

---

[195] *Id.* ("Naval combat in the Spanish-American war resulted in (for-profit) prize litigation."); *see also* Jonathan M. Gutoff*, Original Understandings and the Private Law Origins of the Federal Admiralty Jurisdiction*, 30 J. MAR. L. & COM. 361, 403 (1999) ("The Spanish-American War was fought on two oceans and generated prize litigation that lasted into the early 20th century.").

[196] Helfman, *supra* note 168, at 850 ("This was the case in *The Paquete Habana*, in which the Court examined centuries of treaties, diplomatic correspondence, state papers, court decisions, and scholarly writings for evidence of a norm exempting coastal fishing vessels from capture as prize during times of blockade."). For a full reading of the Court's discussion in applying customary international law, *see generally* The Paquete Habana, 175 U.S. 677 (1900).

[197] Gutoff, *supra* note 195, at 403.

[198] Berg v. British & African Steam Nav. Co., 243 U.S. 124 (1917).

[199] *Id.* at 155–56.

[200] Hamburg-American Line v. United States, 168 F.2d 47, (1st Cir. 1948). The United States was awarded $72,212.40 in salvage and costs while each crew member involved in the boarding and salvage received $3,000. *Id* at 52. All other crew members received two months' pay and allowance). *Id. See also* Gutoff, *supra* note 195, at 403 n.175 (citing the capture of the *Odenwald* as "[t]he last case of prize to be reported").

[201] Garrett, *supra* note 17, at 694 ("It was not until around the Vietnam War that interest in the letters of marque and reprisal arose again briefly as scholars examined presidential authority in conducting war.").

[202] Authority of the President to Blockade Cuba, 1 Op. O.L.C. Supp. 195 (Jan. 25, 1961) (citing 10 U.S.C. §§ 7651–7652 (1958)).

2001 and 2007, Representative Ron Paul introduced failed bills to authorize the President to issue letters of marque and reprisal in response to the 9/11 hijackings.[203] In February 2022, the House introduced a bill in Congress to authorize the President to issue letters of marque and reprisal to seize the assets of Russian citizens who are on the Office of Foreign Assets Control List of Specially Designated Nationals and Blocked Persons.[204] These developments indicate prize law is not outdated and can still be applied, with a modern twist, as a tool against cybercrime.[205]

V. The Application of Prize Law to Cyber Crimes

The United States has an existing structure of prize courts that can easily be refitted to adjudicate the seizure of cryptocurrency or other assets taken from cybercriminals. With the right application of customary international law and federal legislation, U.S. prize courts can be set up to be powerful and effective deterrents to malicious cyber activity.

A. The Existing Structure of Prize Courts in the United States

The underlying framework establishing U.S. prize courts exists under Titles 10 and 28 of the U.S. Code.[206] Pursuant to this framework, U.S. district courts have original jurisdiction over prize cases.[207] For a particular district court to have jurisdiction over a prize case, there must be a captured vessel or aircraft taken "during war by authority of the

---

[203] Garrett, *supra* note 17, at 694–95; *see also* H.R. 3076, 107th Cong. (2001); *see also* H.R. 3216, 110th Cong. (2007).
[204] H.R 6869, 117th Cong. (2022).
[205] Steigelman, *supra* note 93, at 15–16 (noting "prize law remains good law, albeit rare in practice" and "prize law and related concepts, like privateering, might be employed to combat future threats that are not yet fully addressed in the law of armed conflict").
[206] 10 U.S.C. §§ 8851–8881; *see also* 28 U.S.C. § 1333.
[207] 28 U.S.C. § 1333 ("The district courts shall have original jurisdiction, exclusive of the courts of the States, of: (1) Any civil case of admiralty or maritime jurisdiction, saving to suitors in all cases all other remedies to which they are otherwise entitled. (2) Any prize brought into the United States and all proceedings for the condemnation of property taken as prize."); *see also* 10 U.S.C. § 8852 (granting original jurisdiction to the United States district courts for prize proceedings).

United States or adopted and ratified by the President."[208] Jurisdiction is also predicated on which U.S. port a captured vessel is brought into.[209]

This existing statutory structure of prize courts presents three main challenges for a proposed application to assets seized by malicious cyber actors. The first issue is whether a prize court could obtain jurisdiction over seized assets absent a declaration of war. The second is determining how financial assets such as cryptocurrency could fall under prize court jurisdiction. The third issue is how to determine which district court would have jurisdiction over assets seized in cyberspace that are never "brought into a port of the United States." All of these issues can be resolved by reconditioning prize law as an effective tool against malicious cyber actors.

1. Prize Court Jurisdiction Absent a Declaration of War

There is considerable precedent in the international community that a formal declaration of war is required to initiate prize proceedings.[210] This presents a challenge for cyber prize courts, as cyber operations are generally conducted absent a declared war and below the level of armed conflict.[211] However, if prize-taking is seen as a tool to maintain peace, as originally intended by the Framers of the Constitution, then such cases could be initiated without a declaration of war.[212] Additionally, treating malicious cyber actors as *hostis humani generis* could establish that a state

[208] 10 U.S.C. § 8851. "Enemy property" and "neutral property used or transported in violation of the obligations of neutrals under international law," captured by the Army, Air Force, or Space Force while "engaged in hostilities," is exempt from prize procedures. *Id.*
[209] 10 U.S.C. § 8853(a) ("If a prize is brought into a port of the United States, or the Commonwealths or possessions, proceedings for the adjudication of the prize cause shall be brought in the district in which the port is located.").
[210] Clapham, *supra* note 163, at 1233 (citing scholars who hold the belief that prize law only applies during an armed conflict and that "some national legal orders probably require a Declaration of War before a prize court can sit").
[211] Priyanka R. Dev, *"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, 50 TEX. INT'L L.J. 381, 388 (2015) ("relatively few cyber acts result in the type of physical harm or damage that States traditionally accept as unlawful").
[212] Lobel, *supra* note 186, at 1060 (The Framers believed "any possible narrowness implied by the authority to 'declare war' made it necessary to include the use of force in time of peace among the enumerated congressional powers.").

of conflict exists without the need to declare war.[213] Recent international trends in prize law also suggest alignment with this view.

a. International Views

Several decades after the Paris Declaration, England passed the Prize Courts Act of 1894, which required a formal declaration of war to exist for a prize court to exercise jurisdiction.[214] In 1939, when King George issued an order establishing prize court jurisdiction to seize the property of the German Reich or private German citizens, the existence of a state of war was cited as justification.[215] In 1965, India presented an argument that prize courts could only be established during war and were, therefore, illegal under the United Nations Charter since no country could now declare war.[216] India would later pass the Indian Naval and Aircraft Prize Act of 1971, which established prize court jurisdiction over vessels, aircraft, and cargo seized during war, armed conflict, or in exercise of the right of self-defense.[217] During its 1971 war with Pakistan, India utilized prize law to adjudicate the capture of Pakistani naval vessels, merchant ships, and cargo taken from Danish vessels.[218] The Islamic Republic of Iran introduced legislation in 1988 to establish a War Prizes Tribunal, also founded on the existence of a state of war, with jurisdiction over seizures of enemy and neutral vessels and goods.[219]

Israel recently broke from the view that prize court jurisdiction is dependent on a declaration of war.[220] In 2012 and 2016, the Israeli military seized two civilian vessels for violating the blockade of Gaza and

---

[213] Andrew Demaio, *Upping the Stakes to Win the War Against Somali Piracy: Justifications for a New Strategy Based on International Humanitarian Law*, 22 GEO. MASON L. REV. 387, 393 (2015) (*Hostis humani generis* "meant enemy in the sense of a wartime foe who could be attacked and killed without a declaration of war or formal hostilities.").
[214] Clapham, *supra* note 163, at 1201 (citing Prize Courts Act 1894, 57 & 58 Vict. c. 39, § 2(1)–(3)).
[215] *Id.* at 1201–02.
[216] *Id.* at 1228–29.
[217] Naval and Aircraft Prize Act, 1971, §§ 4(1)-4(3), No. 59, Acts of Parliament, 1971 (India).
[218] Clapham, *supra* note 163, at 1230.
[219] *Id.* at 1230–31.
[220] *Id.* at 1247.

condemned them under prize court proceedings.[221] The first vessel, the Finnish-flagged *Estelle*, was released due to Israel's delay in initiating prize proceedings. However, the Haifa District Court and the Israeli Supreme Court both held that a formal declaration of war is not required to initiate prize court proceedings as long as a state of armed conflict exists.[222] The seizure of the second vessel, the Dutch-flagged *Zaytouna-Olivia*, was affirmed by the Haifa District Court.[223] Israel's successful condemnation of a neutrally-flagged civilian vessel through prize proceedings, absent a declaration of war, could bolster the legitimacy of a U.S. prize court taking action against assets seized in cyberspace.

b. Domestic Views

Prize law in the United States was never originally intended to be strictly a tool of war.[224] The Framers of the Constitution viewed prize-taking as a potential tool of peace that could be utilized in lieu of resorting to war.[225] The Articles of Confederation even contained a provision that authorized letters of marque and reprisal to be issued during peacetime.[226] Prize taking occurred in the Quasi War without a formal declaration of war.[227] The view that prize law was separate from the law of war was upheld by the U.S. Supreme Court during the War of 1812, where the taking of prizes was "an independent substantive power, not included in that of declaring war."[228] As U.S. prize law continued to develop, prize taking absent a declaration of war was deemed permissible if it occurred under circumstances suggesting war, such as during a blockade.[229] As demonstrated recently, the proposed congressional bill authorizing letters

---

[221] *Id.* at 1245–47; *see also* Steigelman, *supra* note 93, at 15–16.
[222] Clapham, *supra* note 163, at 1246–47.
[223] Steigelman, *supra* note 93, at 16.
[224] *See* ARTICLES OF CONFEDERATION of 1781, art. IX, para. 1 (granting Congress the authority to issue "letters of marque and reprisal in times of peace").
[225] Lobel *supra* note 186, at 1059 ("The Continental Congress recognized that letters of marque and reprisal issued 'in times of peace' could constitute state-authorized private warfare short of declared war.").
[226] ARTICLES OF CONFEDERATION of 1781, art. IX, para. 1.
[227] Sidak, *supra* note 166, at 481.
[228] Brown v. U.S., 12 U.S. 110, 126 (1814).
[229] Clapham, *supra* note 163, at 1237–38 (referencing Authority of the President to Blockade Cuba, *supra* note 202).

of marque and reprisal against certain Russian nationals is not predicated on a state of war existing between the United States and Russia.[230]

Accepting that the U.S. practice of prize law does not require a declared war, the argument to apply prize law against malicious cyber actors is further strengthened by applying the customary international law traditions of *hostis humani generis*. If malicious cyber actors are treated as *hostis humani generis*, then all states may exercise jurisdiction over them, as all states are at war with them.[231] Applying these principles of universal jurisdiction would extend to the ability of prize courts to adjudicate proceedings concerning assets seized by malicious cyber actors.[232] A declaration of war would not be needed.[233] Adopting this view is also significant as it avoids the problem faced by attribution in cyberspace. As *hostis humani generis*, it would no longer matter where a malicious cyber actor was located, or under what authority or direction they were operating, so long as their assets could be seized and brought to a prize court.

2. Cryptocurrency as Prize

Current statutory law looks at vessels and aircraft as potential prizes.[234] While this appears to preclude cryptocurrency, or other financial assets contained in a digital wallet, as prize, there is growing evidence suggesting Congress has the authority to draft legislation that could authorize the seizure of assets other than vessels or aircraft.[235] The War Powers Clause of the Constitution empowers Congress to grant letters of marque and reprisal, as well as to "make Rules concerning Captures on

---

[230] *See supra* note 204 and accompanying text.
[231] Helfman, *supra* note 168, at 809–10.
[232] Daniel A. Lavrisha, *Pirates, Ye Be Warned: A Comparative Analysis of National Piracy Laws*, 42 U. TOL. L. REV. 255, 259 (2010) (The doctrine of *hostis humani generis* "allowed English courts to adjudicate property issues . . . without any formal declarations of war." Lavrisha later adds that these common law principles of the English courts concerning universal jurisdiction over *hostis humani generis* were inherited and adopted by the United States.).
[233] *Id.*
[234] 10 U.S.C. § 8851.
[235] *See* H.R 6869, 117th Cong. (2022) (authorizing letters of marque and reprisal to seize "any yacht, plane, or *other asset*") (emphasis added); *see also* H.R. 3216, 110th Cong. (2007) (authorizing letters of marque and reprisal to seize "the person and property of Osama Bin Laden" and other conspirators behind the 9/11 attacks).

Land and Water."[236] The term "Captures on Land and Water" refers to the rules governing the transfer of ownership of property captured during war.[237] While the cyberspace domain did not exist during the drafting of the Constitution, this express power of Congress to legislate on the transfer of ownership rights should extend to governing the rules of capture in cyberspace. By extending prize law to encompass assets taken in cyberspace and instituting prize court proceedings to obtain ownership, Congress would add more legitimacy to U.S. government seizures of cyber assets without having to demonstrate that a particular cyber group was acting as an enemy.[238] This legitimacy would primarily be derived by providing the opportunity for any claimed owners of the cyber assets to raise their arguments in prize court against its condemnation by the U.S. government.

3. Determining Cyber Prize Court Jurisdiction

One of the historical aspects of prize taking was selecting a prize crew to sail the captured vessel into a friendly port to be condemned at prize court.[239] However, cryptocurrency contained in a digital wallet cannot be physically brought into a U.S. port.[240] While this may appear to present a serious challenge, the U.S. Code does allow the Secretary of the Navy to designate a district to administer prize proceedings if "no part of [the prize property] has been or can be sent in for adjudication."[241] If intangible assets such as cryptocurrency could be interpreted as prize property that cannot be sent in for adjudication, then under existing statutory authority, the Secretary of the Navy could designate a district court to serve as the

---

[236] U.S. CONST. art. I, § 8, cl. 11.
[237] Sidak, *supra* note 166, at 468.
[238] An argument could also be made that seized cyber assets of cybercriminals deemed *hostis humani generis* are "enemy property" exempt from the need for prize procedures under 10 U.S.C. § 8851.
[239] Steigelman, *supra* note 93, at 2.
[240] David V. Croft, *Cryptocurrency in Estate Planning*, 33 OHIO PROB. L.J. NL 8 (2023) ("Unlike traditional assets, cryptocurrencies are not tied to a physical location or institution. They are geographically agnostic. They exist solely in the digital realm, protected by complex cryptographic algorithms, and stored in digital wallets.").
[241] 10 U.S.C. § 8853(c) ("If the prize property is lost or entirely destroyed or if, because of its condition, no part of it has been or can be sent in for adjudication, proceedings for adjudication of the cause may be brought in any district designated by the Secretary of the Navy.").

prize court. Under this statute, proceeds from the sale of these assets would be deposited with the U.S. Treasurer.[242]

B. The Function of a Cyber Prize Court

If the hurdles facing a cyber prize court could be resolved as demonstrated, then such a court would be a very efficient tool to combat and deter malicious cyber activity. Its greatest strength would be its avoidance of the issues surrounding cyber attribution.

1. The Vision of a Cyber Prize Court

Rather than target traceable cryptocurrency paid as ransom, as it is currently able to do, the U.S. government could, under this interpretation of prize law, target and seize the financial assets of malicious cyber actors wherever they were found.[243] The seizure of such assets could be done without attribution to a particular malicious cyber activity, and the prize court process would provide an avenue for the claimed owner of the cyber assets to raise protest.[244] Rather than having to trace the digital path of a specific ransom, any digital currency or asset associated with a malicious cyber actor could be seized.[245]

In a nod towards the maritime tradition of prize law and in alignment with current statutory authority, the Secretary of the Navy could designate a particular district court to adjudicate the prize proceedings and thereby

---

[242] *Id.* ("In such cases the proceeds of anything sold shall be deposited with the Treasurer of the United States or public depositary in or nearest the district designated by the Secretary, subject to the orders of the court for that district.").

[243] *See* Romo, *supra* note 37 (detailing how the FBI was able to recover a portion of paid ransom money using the associated encryption key).

[244] Since the malicious cyber actor or criminal is being treated as *hostis humani generis*, there would be no need to definitively associate them with a particular state or deal with jurisdictional issues in cyberspace. Historically, vessel or cargo owners in prizes cases could argue the innocence of their vessel or cargo, such as claiming the vessel was not flying an enemy flag, or that the cargo on a neutral vessel was not destined for an enemy port. *See* Steigelman, *supra* note 87, at 3.

[245] When treating cyberspace as the ocean, then digital currency passing through the internet would be like pirated goods being transported across the sea, and universal jurisdiction could be enforced. *See* Parker, *supra* note 3, at 596-97.

transfer ownership of the seized assets to the U.S. government.[246] This would also allow the original owner of the property to raise arguments against condemning the seized assets as prize. Governments and non-state actors could raise protests in prize court, but such occurrences would likely be rare. As governments that utilize malicious cyber actors do so to maintain plausible deniability, it is unlikely that many foreign countries would bring forth opposition to a claim brought forth for adjudication in a cyber prize court. Cybercriminal groups, who also rely on anonymity, would also be unlikely to assert opposition to claims made in cyber court.[247] For such a claim against condemnation to be successful, the party would have to prove that the seized financial assets were not the product of malicious cyber activity or that prize proceedings were not initiated within a reasonable amount of time.[248] Once ownership of the seized assets was transferred to the U.S. government and deposited into the Treasury, the government could utilize the funds as preferred or required.

2. The Impact of a Cyber Prize Court

As the financial benefits of cyber-attacks, such as ransomware attacks, are a significant motivator for cybercriminals, hitting malicious cyber

---

[246] 10 U.S.C. § 8853 (authorizing the Secretary of the Navy to designate a district to administer prize proceedings if "no part of [the prize property] has been or can be sent in for adjudication").

[247] *See* Bagdasarova, *supra* note 8, at 1013-14 (discussing how anonymity aids cybercriminals in carrying out attacks); *See also* Amina Allison, *The Psychology of Cybercrime: Understanding Motivations to Craft Effective Prevention Strategies*, CYBERSECURITY EDUC. INITIATIVE (May 12, 2025), https://cysed.org/the-psychology-of-cybercrime-understanding-motivations-to-craft-effective-prevention-strategies/ [https://perma.cc/9AD7-BPRE] (discussing the psychological buffer the anonymity of the internet provides criminals, detaching them from the consequences of their actions and encourages them to operate without fearing repercussions).

[248] 10 U.S.C. § 8854 (detailing why prize proceedings should begin within a "reasonable time" because otherwise "any party claiming the captured property may, in any district court as a court of prize (1) move for a monition to show cause why such proceedings shall not be started; or (2) bring an original suit for restitution."); *see also* Steigelman, *supra* note 93, at 3 (discussing the vessel owner's opportunity in prize proceedings to "predictably [argue] the innocence of their ship or cargo," which in the cyber context would mean presenting a claim that the seized assets were not associated with malicious cyber activity or a malicious cyber actor).

actors in their pockets would be an effective counter to their activities.[249] By imposing a high financial cost on cybercriminals, governments that utilize cybercriminals will be challenged to find actors willing to accept contracts.[250] Seizing the financial assets of government-backed malicious cyber actors, like those in North Korea, will also degrade their ability to fund weapons projects.[251]

While seizing the financial assets of cybercriminals and terrorist organizations may deter future cyber attacks against the U.S. government and private sector, utilizing prize courts to convert those assets would have additional financial benefits. Seized assets could be used to fund U.S. cyber operations and reimburse entities affected by cyber and ransomware attacks. This two-pronged effect will see the U.S. cybersecurity forces increase in strength as funds flow in, while the power of malicious cyber groups is diminished.[252]

C. Final Thoughts on Cyber and Prize

Scholars like B. Nathaniel Garrett suggest private citizens should be authorized as cyber privateers due to the United States' lack of supremacy in cyberspace.[253] However, the shift away from privateering in both the international community and by practice in the United States since the Paris Declaration would make widespread acceptance of this proposal challenging. There are also questions concerning regulating the behavior of private parties conducting government-sanctioned activities.[254] While

---

[249] Riedy et al., *supra* note 29 (the majority of cybercriminals are motivated by "direct or indirect financial gain").

[250] Since state actors have a strong financial incentive to engage in cybercriminal activity due to the "low cost and high yield" of such tactics, imposing costs on conducting malicious cyber activity will remove those incentives. *See* Manshu, *supra* note 48.

[251] Lyngaas, *supra* note 49 (detailing that a large amount of funding that goes into North Korea's missile program comes from malicious cyber activity).

[252] The FBI's Internet Crime Complaint Center reported losses of $16.6 billion to cybercrime in the United States in 2024. Approximately $12.5 billion of this total was a result of ransomware, though the FBI's report suggests the actual amount may be much higher. *See* INTERNET CRIME COMPLAINT CTR., FEDERAL BUREAU OF INVESTIGATION INTERNET CRIME REPORT 2024 (2024).

[253] Garrett, *supra* note 17, at 697.

[254] Ryan R. Migeed, *Avast, Ye Botnets!: Applying Lessons from the Law of Piracy to the Problem of Botnets*, 54 GEO. WASH. INT'L L. REV. 375, 393-98 (2023) (One concern is what would prevent a "cyber privateer" from going rogue and targeting the financial assets

utilizing cyber privateers with specifically tailored letters of marque and reprisal may be effective, acceptance by the international community is unlikely. [255] Even the United States has largely shifted away from government-sanctioned personal enrichment, making such a proposal unpopular.[256] Cyber prize courts would appear most legitimate if claims of cyber prize were brought only by the U.S. government.

VI. Conclusion

The threat of cyber-attacks from both state and non-state actors continues to grow, and forward-thinking approaches are needed to address them. As our current body of laws are insufficient to address cybercriminal activity, reapplying the historic Law of Prizes to this modern problem can become a viable tool for countering, deterring, and neutralizing cybercriminals' ability to threaten the U.S. government, private institutions, and the public. The parallels between the ocean and cyberspace make prize law an applicable tool to use against malicious cyber actors. These cybercriminals, due to their behavior in violation of international norms, should be treated as *hostis humani generis* and their assets seized wherever they can be found. With some involvement from Congress, prize law can be an effective and legal way to dispose of seized assets in a manner that financially benefits the United States and funds future U.S. cyber operations against malicious cyber actors. This process will also lend legitimacy to U.S. cyber operations against malicious cyber actors and may encourage allies to adopt similar approaches to cyber and prize law.

---

of entities that are not malicious cyber actors, as privateers are profit-motivated and "inherently unreliable" Migeed's article further explores some of the issues with utilizing "cyber privateers").

[255] Garrett, *supra* note 17, at 702 (arguing that specially tailored letters of marque could prevent vigilantism, but even so, the international community has moved away from privateering since the Paris Declaration, and the United States since the War of 1812.).

[256] Steigelman, *supra* note 93, at 14.