

CYBER LETTERS OF MARQUE: ADDRESSING THE GEOPOLITICAL RISKS OF PRIVATE CYBER WARFARE: LESSONS FROM HISTORY AND INTERNATIONAL LAW

GLENYS P. SPENCE*

ABSTRACT

This Article examines H.R. 4988, the “Cybercrime Marque and Reprisal Authorization Act of 2025,” which seeks to revive the historical practice of letters of marque by authorizing cyber letters of marque against state-linked cybercrime. It argues that, although escalating state-sponsored cyberattacks and attribution difficulties have prompted calls for novel defensive tools, this proposal represents an anachronistic and dangerous use of constitutional authority. By delegating coercive power to private actors operating extraterritorially, the bill threatens to recreate in cyberspace the blurred lines between public and private violence that characterized mercenary practices during the Thirty Years’ War and the activities of chartered trading companies in the imperial era.

The Article compares the historical abuses of maritime privateering, which ultimately led to its international abolition, to the foreseeable excesses and accountability gaps that would accompany privately contracted cyber operators. It contends that such delegation conflicts with foundational principles of international law, including state sovereignty, non-intervention, and the prohibition on the use of force under the United Nations Charter, and would exacerbate the attribution and enforcement problems already evident with private military companies. Finally, the Article evaluates how existing instruments, such as the Montreux Document and the International Code of Conduct for Private Security Service Providers, could be adapted to regulate private cyber operators within an established international legal framework. It concludes that meaningful governance of cyber defense requires building on these contemporary regimes rather than resurrecting a discredited constitutional relic.

I. INTRODUCTION

As of late 2025 and early 2026, there has been a significant legislative push to revive the constitutional power to grant Letters of Marque and Reprisal.¹ In

* Professor Glenys Spence is an Assistant Professor of Law at the University of Toledo College of Law. She earned her LL.M. in Admiralty and Maritime Law from Tulane University Law School in 2016. She holds a J.D. from the University of Pittsburgh School of Law (2003), where she received a Certificate of Advanced Studies in International and Comparative Law. Thanks to research assistant, Haley Livingstone, and the Library Staff at the University of Toledo College of Law for their tireless efforts in assisting with this research.

1. See Cartel Marque and Reprisal Authorization Act of 2025, S. 367, 119th Cong. (2025) (demonstrating proposed legislation in the U.S. Congress which seeks to authorize the President to commission private individuals to seize vessels and assets belonging to transnational criminal organizations and drug cartels).

2026, the Scam Farms Marque and Reprisal Authorization Act (H.R. 4988), the proposed “Cyberbill,” seeks to empower the U.S. executive with the authority to issue “cyber letters of marque” to private operators for combating foreign-backed cybercrime and recovering digital assets.² The proposed bill seeks to modernize a dormant constitutional authority by applying centuries-old maritime concepts to the abstract complexities of cyberspace.³ This legislation would empower the President to issue “cyber letters of marque” to private operators, authorizing them to seize the persons or property of individuals or foreign governments involved in broadly defined cybercrime enterprises. Mirroring historical privateers who profited from captured vessels, these digital actors would be incentivized through the recovery of stolen digital assets or financial awards, effectively harnessing private-sector technical expertise to achieve national security objectives.⁴

There is no doubt that cyber-attacks and cybercrimes have become more sophisticated by both state and non-state actors.⁵ Given the recent spate of these attacks on the American government, businesses and consumers, the proposed bill, in theory, is not alarmist. Some solution clearly is needed to combat these issues which have the potential to evolve into full scale cyber-warfare.⁶

Contrary to popular academic writings and the swash-buckling movies of Hollywood, letters of marque were not always confined to state-sponsored naval warfare.⁷ Originally, letters of marque had two functions.⁸ In the early medieval period, letters of marque were employed as a “rights-based” conflict-resolution tool.⁹ It was not until the late medieval and early modern age of sail that letters

2. Scam Farms Marque and Reprisal Authorization Act of 2025, H.R. 4988, 119th Cong. (2025).

3. *See id.*

4. *See id.* § 3.

5. *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 822 (2012) (describing major state-linked cyber operations and large-scale cyberattacks demonstrating the growing sophistication of cyber warfare and cybercrime).

6. *See id.* (noting uncertainty over whether cyber operations qualify as armed conflict under the law of war); *see also* Stephen Weigand, *Critical infrastructure facing cyber surge in OT and supply chains in 2026*, SC WORLD (Jan. 8, 2026), <https://www.scworld.com/feature/critical-infrastructure-facing-cyber-surge-in-ot-and-supply-chains-in-2026> [<https://perma.cc/8F9K-G3A9>].

7. *See generally* Christopher D. Beck, *Seizing Liberties: Private Rights, Public Good, and Letter of Marque in Medieval Marseille* pp. 10-19 (Aug. 2012) (Ph.D. dissertation, Fordham University) (ProQuest) (explaining the distinction between privateers in a trade war (called *droit de course*) and letters of marque to resolve individualized judicial conflict. . . . “The use of marque in the Middle Ages represents an instance when the interaction between rulers and citizens became an institutionalized method both to end regional conflicts and to return legal advantage to dispossessed individuals”).

8. *See id.*

9. *See generally id.* (Positing that “while Marseille’s use of marque is not conclusive evidence for the existence of Weber’s modern bureaucracy in the Middle Ages, the use of marque as a tool for conflict resolution suggests the beginnings of a formulaic and institutionalized form of conflict resolution used within the western Mediterranean trade network.” *Citing to*

of marque took on a more sinister cloak of state-sponsored coercion.¹⁰ Nevertheless, the concept of letters of marque, as conceptualized in the modern age to authorize privateers in naval warfare, presents a controversial yet compelling framework for addressing modern cybercrimes.¹¹

The application to cyberspace requires navigating complex legal, ethical, and practical challenges to prevent uncontrolled escalation in the global commons and ensure accountability in the digital domain. While framed as a modern application of constitutional authority, this paper argues the legislation is an anachronistic and dangerous solution. It risks creating a “Wild West” in cyberspace by blending 19th-century legal concepts with 21st-century technological realities, leading to a host of geopolitical and legal conflicts. The paper employs a multidisciplinary qualitative methodology integrating historical legal analysis with comparative international law and doctrinal research. This approach combines historical context, legal conflicts, and potential governance models for private cyber operators.

This analysis examines the historical evolution, legal friction, and governance models surrounding private cyber operators, ultimately arguing that the United States must reject the revival of archaic maritime tools in favor of a framework rooted in established international law. The inquiry begins in Part II by deconstructing the definitions of cybercrime, cyber-attack, and cyber warfare. By adopting Professor Oona Hathaway’s legal framework, the paper identifies the precise responses required to address modern American vulnerabilities. Part III then bridges theory with reality, presenting tech industry forecasts of emerging digital threats and highlighting the alarming lack of U.S. preparedness to meet them.

The study shifts to a historical perspective in Part IV, examining why the “letter of marque,” a tool of imperfect warfare, retains a lingering presence in U.S. jurisprudence. However, Part V demonstrates the danger of this legacy, exploring how applying maritime concepts to a domain without physical borders triggers profound conflicts within the international legal order. Drawing on the precedent of private military companies in anti-piracy operations, Part VI illustrates how deploying privateers to seize digital assets could expose the United States to severe legal consequences and claims of international law violations.

Rather than pursuing unilateral “cyber-privateering,” Part VII advocates for a diplomatic pivot toward strengthening existing multilateral standards, such as the Montreux Document and the International Code of Conduct (“ICoC”).

GIANFRANCO POGGI, *THE DEVELOPMENT OF THE MODERN STATE: A SOCIOLOGICAL INTRODUCTION* 30-32 (Stanford Univ. Press 1978); RICHARD SWEDBERG, *THE MAX WEBER DICTIONARY: KEY WORDS AND CENTRAL CONCEPTS* (Stanford Univ. Press, 2005)).

10. *See id.*

11. *See, e.g.,* Jules Lobel, *Covert War and Congressional Authority: Hidden War and Forgotten Power*, 134 U. PA. L. REV. 1035 (1986) (explaining that the use of private actors to carry out military or foreign policy objectives has deep historical roots and is reflected in Congress’s constitutional authority to authorize such force).

Ultimately, Part VIII concludes that the complexities of the digital age demand a sophisticated, modern governance model, one that prioritizes accountability and international stability over an obsolete 18th-century relic.

II. CYBERCRIME OR CYBERWAR? RESOLVING TERMINOLOGICAL AMBIGUITY IN POLICY

A pivotal issue in the debate over cyber letters of marque is the legal classification of digital threats. While our vernacular use often conflates all nefarious cyber activities, a strict legal distinction between cybercrime and cyber-warfare is necessary to authorize privateers without inadvertently triggering an “act of war.” A major obstacle to reform is the lack of terminological clarity.¹² The proposed bill lists definitions that do not contain the language of war, which is required to trigger the Marques and Reprisals Clause of the Constitution.¹³ The inclusion of the offense under section 1030 of title 18 of the U.S. Code may suffice as that section pertains to offenses committed with the intent to injure the United States.¹⁴

In a 2012 Article, Professor Oona Hathaway, along with other international law experts, explored the legal uncertainty surrounding digital strikes, questioning whether the traditional law of war can or should govern what many call “cyber-warfare.” Hathaway argues in “The Law of Cyber-Attack” that current legal frameworks are inadequate to address modern cyber threats and proposes a new approach grounded in international cooperation. A precise definition of “cyber-attack” is central to this framework, distinguishing it from cybercrime and cyber warfare to highlight specific national security threats. A central concern is the risk of escalation.¹⁵ If cyber-attacks are legally classified as warfare, victims like Iran might claim a right to respond to digital incursions, such as *Stuxnet*, with conventional physical force in self-defense.¹⁶ The authors provided the following table to illustrate the distinctions among the various terms.

12. See Hathaway et al., *supra* note 5, at 823.

13. See Scam Farms Marque and Reprisal Authorization Act of 2025, H.R. 4988, 119th Cong. (2025).

14. See 18 U.S.C. § 1030 (2020).

15. See Hathaway et al., *supra* note 5, at 832 (proposing a purpose-based definition of cyberattacks to distinguish them from ordinary cybercrime for legal and policy purposes).

16. See *id.* at 819.

Table 1: Essential characteristics of different cyber-actions¹⁷

	Type of cyber-action		
	Cyber-attack	Cyber-crime	Cyber-warfare
Involves only non-state actors		✓	
Must be violation of criminal law, committed by means of a computer system		✓	
Objective must be to undermine the function of a computer network	✓		✓
Must have a political or national security purpose	✓		✓
Effects must be equivalent to an “armed attack,” or activity must occur in the context of armed conflict			✓

To address these issues, the Article clarifies how cyber-attacks relate to existing legal structures, including international humanitarian law, emerging international regulations, and domestic criminal law. However, the authors demonstrate that these current frameworks are fundamentally deficient.¹⁸ The law of war only applies to the narrow subset of attacks that occur during an ongoing conflict or rise to the level of an “armed attack,” while other legal systems offer only fragmentary solutions. Because existing tools are inadequate, the authors conclude that a new, comprehensive legal framework is essential.¹⁹ However, as this paper discusses, are letters of marque the answer?

III. THE INVISIBLE FRONTLINE: STRATEGIC PRE-POSITIONING AS MODERN WARFARE

In 2026, the landscape of threats to critical infrastructure has shifted from simple data theft to a sophisticated era of strategic pre-positioning and autonomous disruption.²⁰ The most pervasive evolution is the rise of agentic AI, where malicious actors deploy self-governing software agents that can independently conduct reconnaissance, adapt to defensive countermeasures, and execute multi-stage attacks on power grids and water systems without human intervention. This automation allows for “vibe hacking,” AI-driven social engineering so precise in its mimicry of human behavior and corporate tone that

17. *Id.* at 833.

18. *Id.* at 821.

19. *Id.*

20. Weigand, *supra* note 6.

traditional employee training often fails to stop it.²¹

Simultaneously, the geopolitical climate has birthed a doctrine of "living off the land," exemplified by state-sponsored groups like *Volt Typhoon* and *Salt Typhoon*.²² Rather than using identifiable malware, these actors hijack a system's own legitimate administrative tools to remain undetected within the networks of telecommunications and transportation hubs. Their goal is rarely immediate theft. Instead, they are "pre-positioning," embedding themselves deep within the architecture of essential services to ensure they can trigger physical, kinetic failures during a future conflict.²³

The vulnerability of these systems is further exacerbated by the accelerated convergence of IT and Operational Technology ("OT"). As aging industrial sensors and legacy control systems are brought online to leverage cloud efficiencies, they expose previously air-gapped infrastructure to modern ransomware. This creates a dangerous "interdependency risk," where a single vulnerability in a third-party software library can cascade through the entire supply chain, crippling logistics, food distribution, and energy sectors simultaneously.²⁴ Tech experts have signaled the "parade of "horribles" expected from the nefarious uses of technology in cyber-space. According to these experts, "critical infrastructure targeting will expand into sectors supporting logistics and manufacturing."²⁵

Finally, a more patient but equally existential threat looms in the form of "Harvest Now, Decrypt Later" strategies.²⁶ Adversaries are currently intercepting and storing massive volumes of encrypted critical infrastructure data, betting on the near-term arrival of quantum computing to eventually break today's cryptographic standards.²⁷ This ensures that even if a network is secured today, the secrets of its structural weaknesses and strategic communications remain at risk for the decade to come.²⁸

IV. HISTORICAL ANACHRONISM AND THE "WILD WEST" OF CYBERSPACE

A letter of marque was historically defined as a government license issued to an individual, known as a "privateer," authorizing them to attack and

21. *See id.*

22. CHRIS JAIKARAN, CONG. RSCH. SERV., IF12798, SALT TYPHOON HACKS OF TELECOMMUNICATIONS COMPANIES AND FEDERAL RESPONSE IMPLICATIONS (2025).

23. *See generally id.* (describing adversary pre-positioning within critical infrastructure to enable later physical or kinetic disruption); *see also* David DiMolfetta, *Cyber experts pinpoint what to look out for in 2026*, NEXTGOV (Dec. 30, 2025), <https://www.nextgov.com/cybersecurity/2025/12/cyber-experts-pinpoint-what-look-out-2026/410306/> [<https://perma.cc/DP8L-XFVP>] (As Beijing continues to pre-position and embed access across U.S. critical infrastructure, questions of preparedness, deterrence, and response will increasingly shape how cyber policy is integrated into broader national security planning).

24. *See* JAIKARAN, *supra* note 22; Weigand, *supra* note 6.

25. Weigand, *supra* note 6.

26. *See* DiMolfetta, *supra* note 23.

27. *See id.*

28. *See id.*

capture the vessels and property of a foreign state.²⁹ The term “reprisal” specifically referred to a state-sanctioned act aimed at seeking redress for an injury committed by a foreign entity through the seizure of their property.³⁰ This mechanism served as a vital tool of economic statecraft, allowing nations with limited naval resources, such as the nascent United States during the Revolutionary War and the War of 1812, to supplement their military forces cost-effectively.³¹ Privateers operated at their own expense and were highly motivated by the profits generated from the sale of captured “prizes,” with these seizures being adjudicated in specialized admiralty courts.³²

The Framers of the U.S. Constitution recognized the gravity of this power, placing the authority to issue letters of marque solely with Congress, not individual states, because granting such letters was inherently viewed as an action that could directly lead to a state of war.³³ Thus, in *Barron v. City of Baltimore*, Chief Justice Marshall stated that the Constitution’s total prohibition on states issuing letters of marque was a necessary safeguard for national peace. He cautioned that allowing individual states to authorize privateers would “lead directly to war,” as such actions are inherently hostile. By stripping states of this power, the Framers ensured that a single state could not unilaterally provoke a foreign conflict and embroil the entire Union in a war that only Congress has the authority to declare.³⁴

The privateering practice eventually declined in the 19th century and was formally abolished among many nations by the 1856 Declaration of Paris respecting Maritime Law.³⁵ While the United States was not a formal signatory to this agreement, it has largely adhered to the principles set forth.³⁶ Consequently, Congress has not authorized the use of letters of marque since the Civil War era, leaving the constitutional authority dormant for well over a century.³⁷

The post-medieval historical use of letters of marque involved

29. Allen Loayza, *Cyber Privateers: Protecting American Intellectual Property from Cyber Theft*, 12 LANDSLIDE 27, 29 (2020).

30. See William Young, *A Check on Faint-Hearted Presidents: Letters of Marque and Reprisal*, 66 WASH. & LEE L. REV. 895, 900 (2009); see also Theodore M. Cooperstein, *Letters of Marque and Reprisal: The Constitutional Law and Practice of Privateering*, 40 J. MAR. L. & COM. 221, 222 (2009).

31. See, e.g., Cooperstein, *supra* note 30, at 221; see also Young, *supra* note 30, at 902.

32. John M. Golden, *Patent Privateers: Private Enforcement’s Historical Survivors*, 26 HARV. J.L. & TECH. 545, 563 (2013).

33. See generally *id.* at 564 (Privateering could complicate the work of diplomats by stoking conflict with foreign powers).

34. See STEVE P. MULLIGAN, CONG. RSCH. SERV., LSB11272, LETTERS OF MARQUE AND REPRISAL (PART 1): INTRODUCTION AND HISTORICAL CONTEXT 2 (2025); see also *Barron v. City of Baltimore*, 32 U.S. 243, 249 (1833) (Marshall, C.J.) (“To grant letters of marque and reprisal would lead directly to war; the power of declaring which is expressly given to Congress.”).

35. *Id.* at 245; see also Declaration Respecting Maritime Law, Apr. 16, 1856, 46 Brit. & Foreign State Papers 26 (1856) [hereinafter Declaration of Paris].

36. See *id.* at 245-46.

37. Robert P. DeWitte, *Let Privateers Marque Terrorism: A Proposal for a Reawakening*, 82 IND. L.J. 131, 134 (2007).

commissioning private vessels, or privateers, to seize enemy merchant ships during wartime.³⁸ The major maritime powers at the time dispersed mercenaries called privateers by the British Crown, to wage war on the high seas against each other to conquer ocean spaces.³⁹ This practice, while effective in its time, was fraught with abuse, leading to its eventual abolition by the 1856 Declaration of Paris.⁴⁰ The primary concerns with privateering were the lack of consistent state control over these private actors and the difficulty in distinguishing between legitimate privateers and pirates.⁴¹ This historical context offers a cautionary tale for modern cyber-privateering.

Privateers operated with broad discretion as long as they remained loyal to their commissioning nation, a dynamic best exemplified by Sir Francis Drake during the reign of Queen Elizabeth I.⁴² Acting essentially as a contracted private military force for the English crown, Drake was instrumental in numerous naval engagements against the Spanish Armada.⁴³ However, his career illustrates the often-indistinguishable line between privateering and piracy.⁴⁴ While he fought official battles on behalf of the sovereign, his reputation was equally defined by his seizure of immense wealth.⁴⁵ Because of these predatory raids for gold and silver, many historians conclude that Drake and his fellow privateers were frequently no different from the pirates they were legally distinguished from.⁴⁶

The United States declined to sign the 1856 Paris Declaration Respecting Maritime Law, primarily because the treaty's prohibition on privateering favored established naval powers like Great Britain and France.⁴⁷ By maintaining the right to commission privateers, the U.S. preserved a cost-effective method for a smaller navy to challenge dominant maritime forces.⁴⁸

As a matter of constitutional hierarchy, the Paris Declaration cannot be construed as superseding the U.S. Constitution, nor does it diminish the plenary authority granted to Congress under Article I, Section 8 to authorize Letters of

38. MULLIGAN, *supra* note 34, at 1.

39. See generally Glenys P. Spence, *Combating Maritime Perils in the Global Supply Chain: An Analysis of Force Majeure Clauses and the Doctrine of Commercial Impracticability in The Wake of "State-Sponsored Piracy"*, 15 J. NAT'L SEC. L. & POL'Y 267, 286-87 (2025) (describing how major maritime powers commissioned privateers—state-sanctioned mercenaries—to attack enemy shipping and seize oceanic territory, noting legal and commercial impacts).

40. See Declaration of Paris, *supra* note 35; see also Cooperstein *supra* note 30, at 245.

41. See Golden, *supra* note 32, at 566.

42. Spence, *supra* note 39, at 289.

43. See *id.* (There may be no better example of early privateers and the purpose that they served than Sir Francis Drake. Francis Drake was a commissioned privateer during Queen Elizabeth's reign. Drake was instrumental in fighting the Spanish Armada on behalf of Great Britain.)

44. Cooperstein, *supra* note 30, at 224.

45. See Golden, *supra* note 32, at 563.

46. Cale Gressman, *A Brief History of English Privateers*, COLLECTOR (May 9, 2023), <https://www.thecollector.com/english-privateers/> [https://perma.cc/J757-5LL8].

47. See Cooperstein, *supra* note 30, at 245-46.

48. *Id.*

Marque and Reprisal.⁴⁹ While much of the Declaration is now viewed as customary international law, which the U.S. generally respects, such customs do not hold authority when they conflict with the U.S. Constitution or federal statutes.⁵⁰ In the event of a direct conflict between international custom and a Congressional mandate, U.S. courts and the executive branch are bound to prioritize domestic constitutional authority.⁵¹

Applying this 19th-century legal concept to 21st-century cyberspace is deeply problematic. The digital domain lacks clear physical borders, and actions taken by private operators can have unintended, widespread geopolitical consequences.⁵² Delegating sovereign power to private companies operating extraterritorially threatens to create a “Wild West” in cyberspace, where accountability is elusive and attribution remains a complex challenge.⁵³ The rapid, often anonymous nature of cyber operations makes direct state control and immediate de-escalation nearly impossible to manage under a privateering framework.⁵⁴

The central tension surrounding cyber letters of marque lies in whether a 19th-century naval power can be safely repurposed for a 21st-century digital landscape that lacks clear borders or established international norms. Proponents, including the Digital Chamber and Representative David Schweikert, argue that traditional law enforcement tools are fundamentally

49. See e.g., DeWitte, *supra* note 37, at 132.

50. See JAN MARTIN LEMNITZER, POWER, LAW AND THE END OF PRIVATEERING 3 (2014) (describing the Declaration as “almost instantaneous customary law”); *but see* Curtis A. Bradley & Jack L. Goldsmith, Customary International Law as Federal Common Law: A Critique of the Modern Position, 110 HARV. L. REV. 815, 857 (1997) (arguing that customary norms remain subordinate to the federal separation of powers and the Constitution) (“Nor does Article VI list CIL as a source of supreme federal law. Article I does authorize Congress to define and punish offenses against the law of nations, and Congress has exercised this and related powers to incorporate select CIL principles into federal statutes. But Congress has never purported to incorporate all of CIL into federal law. And Congress’s selective incorporation would be largely superfluous if CIL were already incorporated wholesale into federal common law, as advocates of the modern position suggest.”).

51. LEMNITZER, *supra* note 50.

52. See generally Molly Picard, *Cyberspace: The 21st-Century Battlefield Exposing Soldiers, Sailors, Airmen, and Marines to Potential Civil Liabilities*, 4 NAT’L SEC. L.J. 125, 141 (2015) (asserting that “[T]he law regulating cyberspace is neither clear nor precise”).

53. See Ben Haklai, *Cybersecurity Private-Public Partnerships: A Bridge to Advance Global Cybersecurity*, 56 TEX. TECH L. REV. 627, 683 (2024) (attribution is the ability to determine the source, origin, or identity of cyberattackers, by collecting and analyzing evidence, such as technical, operational, or contextual indicators).

54. See e.g., Nicholas Tsagourias & Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31 EUR. J. INT’L L. 941, 944 (2020) (attribution in cyberspace has traditionally been presented as a challenge because of anonymization, the falsification of identities, the multi-stage nature of cyber operations, the dynamic landscape of cyber threats, the undifferentiated nature of cyber tools, the human and technical resources required in performing attribution and the lengthy timescales involved. State attribution has been even more challenging for the same reasons but also because of the serious political and legal consequences that attribution or misattribution may trigger).

insufficient against the rapid scale of state-linked cybercrime.⁵⁵ They contend that this constitutional “mechanism provides a legitimate, controlled way to leverage private-sector expertise to hack back,” thereby providing a necessary layer of accountability and a means for restitution.⁵⁶

Conversely, critics view the concept as a dangerous anachronism that threatens to turn cyberspace into a lawless “Wild West.”⁵⁷ One primary concern is the difficulty in maintaining real-time control over private actors, which creates significant risks regarding accountability for unintended collateral damage in the digital realm.⁵⁸ Furthermore, actions taken by private operators could be interpreted as violations of state sovereignty under international law, potentially triggering geopolitical escalation or leaving the operators themselves vulnerable to prosecution in foreign jurisdictions.⁵⁹ There are also grave due process concerns, as authorizing asset seizures without traditional judicial oversight could lead to legal liability and the wrongful targeting of individuals or entities.⁶⁰

Ultimately, the limitations of current proposals like H.R. 4988 suggest that stability in the digital domain is better served by building upon established international law rather than reviving a discredited maritime concept. A modern approach must prioritize robust oversight, clear chains of command, and strict adherence to the principles of state sovereignty and the responsible use of force in cyberspace.

V. FROM MARITIME MARQUE TO CYBER BILL: THE 2026 FRAMEWORK FOR PRIVATE DIGITAL REPRISAL

America is locked in an ongoing “cyber war,” with critical federal networks and private infrastructure under continuous automated attack from nation-state actors and criminal syndicates.⁶¹ Ransomware has evolved into a pervasive and incessant threat, subjecting U.S. consumers and commercial entities to a near-constant state of digital siege. The threat landscape requires focusing on both systemic infrastructure risk and targeted corporate attacks.⁶² In 2026, cyber warfare has evolved into a permanent background risk where automated AI-driven tools launch sophisticated attacks at a scale and speed previously unseen.

55. See Scam Farms Marque and Reprisal Authorization Act of 2025, H.R. 4988, 119th Cong. § 2(2) (2025).

56. See *id.*; see also Loayza, *supra* note 29.

57. See Christopher M. Kessinger, *Hitting the Cyber Marque: Issuing a Cyber Letter of Marque to Combat Digital Threats*, ARMY L. 4, 5 (2013).

58. See Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L L. 103, 115 (2014).

59. *Id.*

60. *Id.*

61. Michael J. Lebowitz, *The Cyberenemy: Using the Military Justice System to Prosecute Organized Computer Attackers*, J.L. TECH. & POL'Y 83, 84 (2013) (“The United States is literally under cyberassault on a second-by-second basis”).

62. *Id.*

Unlike traditional warfare, these attacks lack the audible cues of explosions or gunfire; however, their silent and unassuming nature is precisely what makes them so dangerous.⁶³

Motivations for these incursions vary widely, ranging from recreational hacking and corporate espionage to financial theft and more sinister geopolitical sabotage.⁶⁴ While the United States maintains a perpetual defensive posture to safeguard its digital infrastructure, scholars and security analysts warn that a sufficiently sophisticated offensive operation could precipitate a systemic collapse. Such a high-impact strike poses an existential threat to the national power grid and the integrity of Department of Defense (“DoD”) communication networks, potentially resulting in catastrophic socioeconomic and national security consequences.⁶⁵ The primary obstacle to accountability is the attribution problem.⁶⁶ Attackers employ anonymization protocols to redirect traffic through multiple intermediary nodes, creating a layered circuit that prevents the attribution of malicious activity to a specific source.⁶⁷

The application of letters of marque to cyberspace has ignited a significant debate over whether a power designed for 19th-century naval warfare can be safely repurposed for 21st-century digital conflicts, which lack clear battlefields, borders, and established international norms. Proponents of the shift, including the Digital Chamber and Representative David Schweikert, argue that traditional law enforcement tools are fundamentally insufficient against the speed and scale of modern, state-linked cybercrime. They contend that this constitutional mechanism offers a legitimate and controlled means of leveraging private-sector talent, enabling “hack-back” operations that provide both accountability and restitution for victims.⁶⁸

Conversely, critics view the concept as an anachronistic and dangerous solution that risks transforming cyberspace into a lawless “Wild West.” A primary concern is the difficulty of maintaining real-time control over private actors, raising critical questions about accountability for unintended

63. *Id.*

64. See Lebowitz, *supra* note 61, at 86.

65. See Scott J. Shackelford & Amanda N. Craig, *Beyond the New “Digital Divide”: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT’L L. 119, 149 (2014); see also Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing A “Cyber-Pearl Harbor”*, 18 VA. J.L. & TECH. 289, 290 (2014); Kessinger, *supra* note 57, at 4.

66. See TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 80 (Michael N. Schmitt ed., 2017) (noting that the “technical difficulty of tracing a cyber operation to its source” remains a primary barrier to establishing state responsibility); see also Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SEC. L. 229, 233 (2012) (discussing how attackers utilize intermediate “zombie” computers to mask their true geographical origin).

67. Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 528 (2020).

68. See e.g. Kessinger, *supra* note 57, at 218.

consequences or collateral damage in the digital realm.⁶⁹ Furthermore, opponents warn that actions taken by private operators could be interpreted as violations of state sovereignty and international law, potentially triggering geopolitical escalation or leaving operators vulnerable to prosecution in foreign jurisdictions. There are also significant due process concerns, as authorizing asset seizures without traditional judicial oversight could lead to potential liability for wrongfully targeted individuals or entities.⁷⁰

To prevent these authorizations from devolving into unchecked digital vigilantism, the regulatory framework should be envisioned as a highly structured, layered oversight model.⁷¹ This model begins with the President issuing specific “suitable instructions” to ensure that every private offensive action aligns with clear national interests.⁷² Accountability can be further reinforced by a mandatory requirement for privateers to post substantial security bonds; these financial guarantees would serve as a deterrent against misconduct and can be forfeited if an operator violates the terms of their commission or causes unauthorized collateral damage.⁷³

Operationally, digital privateers would be governed by strict guardrails designed to limit their reach and prevent domestic overreach.⁷⁴ Commissions would be restricted to actions against specific foreign criminal syndicates or state-backed enterprises, with operations generally mandated to occur outside U.S. geographic boundaries. Eligibility for such a commission would be predicated on passing rigorous federal vetting and background checks, and authorized entities would be required to adhere to stringent data governance protocols, including maintaining auditable logs of all activities.⁷⁵

Finally, the framework would incorporate essential checks and balances through both the legislative and judicial branches. The executive branch will be required to submit periodic reports to Congress detailing all privateer activities, while the judiciary will remain a critical venue for reviewing the legality of specific seizures.⁷⁶ To mitigate the risk of escalating geopolitical tensions, the model emphasizes diplomatic coordination and deconfliction efforts with

69. Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors As Proportionate Countermeasures to Transboundary Cyberharm* Shearman & Sterling Student Writing Prize in Comparative and International Law, 52 COLUM. J. TRANSNAT'L L. 275, 294-95 (2013).

70. See *id.*

71. See e.g. Kessinger, *supra* note 57, at 4, 19.

72. See Scam Farms Marque and Reprisal Authorization Act of 2025, H.R. 4988, 119th Cong. § 3 (2025).

73. See Kessinger, *supra* note 57.

74. See Allen Loayza, *Cyber Privateers Protecting American Intellectual Property from Cyber Theft*, 12 LANDSLIDE 27, 30 (2020) (Cyber privateers would be required to post a bond and abide by highly detailed operational rules to receive a letter of marque. The letter of marque would also include adequate controls to limit the actions a privateer could take, as well as the duties owed to the people whose systems they infiltrate and any uninvolved third parties.)

75. *Id.*

76. See Kessinger, *supra* note 57, at 4.

international partners.⁷⁷ Many proposed versions of this authority also include time-bound commissions, ensuring that the power to disrupt an adversary is temporary and expires once a specific infrastructure threat has been neutralized.⁷⁸

*A. The Letters of Marque and Reprisal Clause: Historical Basis
and Modern Debate*

The “Letters of Marque and Reprisal” clause, enshrined in Article I, Section 8, Clause 11 of the U.S. Constitution, is a historical artifact that grants Congress the power to authorize private citizens to use force on behalf of the government.⁷⁹ This power was a vital tool for the early United States, which lacked a large, standing navy to protect its maritime interests.⁸⁰ During the 1787 Philadelphia Convention, the Framers vested the federal legislature with exclusive, absolute authority to issue letters of marque and reprisal, expressly prohibiting states from doing so.⁸¹ This decision drew little controversy, likely due to the successful use of privateers during the Revolution and the precedent established by the Articles of Confederation.⁸² The practice declined in the 19th century and was formally abolished among many nations by the 1856 Declaration of Paris respecting Maritime Law, which the U.S. has since adhered to in principle, though it is not a formal signatory. Congress has not authorized the use of letters of marque since the War of 1812.⁸³

Just as the young American Republic once relied on private fighting forces to compensate for a lacking navy, modern lawmakers are looking to private cyber operators to bolster national security.⁸⁴ During the American Civil War, the Confederacy utilized letters of marque to commission privateers against the North, an act that defined the era’s maritime struggle.⁸⁵

Today, cyberspace has become the new “high seas”, a vast, lawless frontier where the U.S. government struggles to keep pace with foreign criminal

77. *Id.*

78. *Id.*

79. U.S. CONST. art. 1, § 8, cl. 11.

80. See Lobel, *supra* note 11, at 1035.

81. U.S. CONST. art. 1, § 10, cl. 1.

82. See Mulligan, *supra* note 38.

83. Young, *supra* note 30, at 8907 (Congress issued no more letters of marque and reprisal after the War of 1812, and the few privateers unwilling to give up the lifestyle and potential rewards of privateering began to offer their service as pirates to other nations, especially in Latin America).

84. See Todd Emerson Hutchins, *Structuring A Sustainable Letters of Marque Regime: How Commissioning Privateers Can Defeat the Somali Pirates*, 99 CAL. L. REV. 819, 847 (2011).

85. See *id.* at 856 (During the American Civil War, the Union government declared that it would abide by the principles of the Paris Declaration during hostilities; the South did not and sought to hire British and French privateers.)

syndicates.⁸⁶ In response, proposed legislation, such as the Scam Farms Marquee and Reprisal Authorization Act, seeks to revive this historical tool, granting the President authority to license private entities to disrupt and seize assets from cyber-adversaries. Much like the Civil War-era privateers, these modern “cyber-privateers” would bridge the gap between limited government resources and the rising tide of foreign threats.⁸⁷

Since the 1970’s Cold War rivalries and in the post-cold-war times, governments have turned more and more to covert paramilitary operations to conduct foreign policy.”⁸⁸ Particularly during the Reagan Administration, the use of these operations to overthrow or coerce foreign governments to work towards the U.S. interest doubled.⁸⁹ In the present political climate under President Trump, these covert operations are poised to re-emerge re-energize to assure that countries perceived to be acting against U.S. interests are brought to heel.⁹⁰ Only this time, the activities will be also carried out in cyberspace, terra nullius, no-man’s land.⁹¹

It remains unclear under both United States and international law whether responding to cyberattacks with letters of marque is legally proper. Furthermore, any such response risks triggering significant separation of powers issues concerning the War Powers, the Letter of Marque and Reprisals, and the Foreign Affairs Clauses of the Constitution.⁹²

The enduring debate over the Framers’ original intent, specifically the requirement for a shared war-making authority, has become increasingly salient as the line between Executive prerogative and Legislative mandate blurs.⁹³ While the post-WWII era and the prolonged conflicts in Iraq and Afghanistan highlight an expansion of Executive unilateralism, the recent military intervention in Venezuela and the apprehension of Nicolás Maduro have

86. See e.g. Jesse Jacob McMurdo, *Cybersecurity Firms-Cyber Mercenaries?*, 4 HOMELAND & NAT’L SECURITY L. REV. 35 (2016) (As the threat of conventional World War II-style war continues to diminish, the emergence of a new battlefield-cyberspace-has taken a position equal to that of land, sea, air, and space); see Rosenzweig, *supra* note 58.

87. See generally, Kessinger, *supra* note 57, at 5 (“A cyber letter of marque would enable a privateer to seize digital assets, disrupt fiscal and communication networks, destroy attacking networks, and act as a cyber bounty hunter”).

88. See Lobel, *supra* note 11, at 1037-39.

89. See *id.*

90. See e.g. Exec. Order No. 14,390, 91 Fed. Reg. 18, 271 (Mar. 6, 2026) (establishes a specialized operational cell within the National Coordination Center to dismantle transnational criminal organizations, prioritizes the repatriation of seized assets to fraud victims, and integrates private-sector capabilities to disrupt foreign cyber-enabled criminal syndicates and “scam farms”).

91. Lobel, *supra* note 11, at 1037-39; see Jesse Jacob McMurdo, *Cybersecurity Firms—Cyber Mercenaries?*, 4 Homeland & Nat’l Sec. L. Rev. 35, 38, 40 (2016).

92. See Lobel, *supra* note 11, at 1036-39.

93. See e.g. John C. Dehn, *War Is More Than A Political Question: Reestablishing Original Constitutional Norms*, 51 LOY. U. CHI. L.J. 485, 486 (2019).

reignited questions regarding the limits of Article II power.⁹⁴

In contrast, the proposed use of letters of marque in cyberspace represents a pivotal reassertion of Article I authority.⁹⁵ By utilizing a specific congressional decree rather than relying on inherent Executive clandestine powers, this framework positions the United States to uniquely revive the Marque and Reprisal Clause.⁹⁶ Proponents argue that the characterization of cyberspace as *terra nullius*, a digital “high seas,” legitimizes this legislative delegation to private actors, offering a constitutional mechanism to project power into jurisdictional voids that traditional state-led enforcement cannot reach.

Originating in 1295 under Henry II and formalized through fifteenth-century Admiralty courts, letters of marque became a vital instrument of maritime jurisdiction. In the United States, this authority was incorporated into the Articles of Confederation and, subsequently, the Constitution, where federalists and non-federalists alike viewed it as an essential component of national war power.⁹⁷

The intersection of maritime conflict and international law significantly shaped American governance, beginning with President Washington’s 1793 Proclamation of Neutrality.⁹⁸ This legal evolution eventually produced the “Charming Betsy” canon, which stands for the proposition that an act of Congress should not be construed to violate international law unless there is no other interpretation.⁹⁹ While Congress authorized letters of marque during the War of 1812, the global tide shifted with the Declaration of Paris during the Crimean War.¹⁰⁰ Notwithstanding, the United States initially declined to sign the Declaration to preserve its right to augment a small navy.¹⁰¹ Memories from

94. Marc Weller, *The U.S. Capture of President Nicolás Maduro—and attacks on Venezuela—Have no Justification in International Law*, CHATHAM HOUSE (Jan. 6, 2026), <https://www.chathamhouse.org/2026/01/us-capture-president-nicolas-maduro-and-attacks-venezuela-have-no-justification> [https://perma.cc/5ZRG-8YVD]; 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, 954-55 (1997).

95. Jonathan L. Still, *Resurrecting Letters of Marque and Reprisal to Address Modern Threats*, (Strategy Research Project, U.S. Navy).

96. See Lucian Rombado, *Grant Cyber Letters of Marque to Manage “Hack Backs”*, U.S. NAVAL INST. PROC., at pp. 1400 (2019); Robert P. DeWitte, *Let Privateers Marque Terrorism: A Proposal for a Reawakening*, 82 IND. L.J. 131, 133-34 (2007).

97. See generally Young, *supra* note 30, at 905 (Given the prominence of privateers in the Revolutionary War, it is not surprising that the Framers included a provision for letters of marque and reprisal in both the Articles of Confederation and the Constitution).

98. See e.g., Saikrishna B. Prakash & Michael D. Ramsey, *The Executive Power over Foreign Affairs*, 111 YALE L.J. 231, 329 (2001).

99. See *Murray v. Schooner Charming Betsy*, 6 U.S. 64, 118 (1804).

100. Zac Morgan & Ian A. Merritt, *Reviving Letters of Marque*, CTR. FOR MAR. STRATEGY (Oct. 29, 2024), <https://centerformaritimestrategy.org/publications/reviving-letters-of-marque/> [https://perma.cc/8JDQ-HB33].

101. See John M. Golden, *Patent Privateers: Private Enforcement’s Historical Survivors*, 26 HARV. J.L. & TECH. 545, 562 (2013).

both the Revolutionary War and the Civil War complicated this stance.¹⁰² When the Confederacy issued its own letters of marque, President Lincoln famously refused to retaliate in kind, despite British recognition of the South as a belligerent.¹⁰³ This refusal led to complex litigation over whether Confederate seizures constituted acts of war or simple piracy, raising the theoretical question of whether the U.S. had informally adopted the Paris Declaration as customary international law.¹⁰⁴

This trend of restraint continued through the Spanish-American War, during which Congress again declined to commission privateers. This period also saw the landmark *Paquete Habana* decision,¹⁰⁵ which affirmed that international law is an integral part of the American legal system and that courts must adhere to the customs of the law of nations in the absence of conflicting domestic legislation.¹⁰⁶ Despite this long period of dormancy, the letter of marque clause remains a functional part of the Constitution.¹⁰⁷ Recent legislative interest suggests that the clause may be repurposed for the digital age, as Congress contemplates using letters of marque to combat cyber-terrorism and rogue states in the realm of information warfare.¹⁰⁸

Furthermore, the paper draws a crucial comparison between the historical abuses of maritime privateering that prompted its international abolition and the potential for similar excesses by private cyber mercenaries. The legal status of these “cyber privateers” would be ambiguous under international humanitarian law. Unlike state agents operating under a clear chain of command, private operators present unique challenges regarding the laws of armed conflict, non-combatant immunity, and accountability for collateral damage.¹⁰⁹ Private cyber-attacks against state-linked actors or infrastructure could be interpreted as coercive interference in another state’s internal affairs, violating the principle of

102. See Young, *supra* note 30 at 900 (in the early years of the United States, the President, constrained by limited military size, manpower, and technology, may have been unable to achieve many commercial and military objectives without relying on privateers).

103. STEVE P. MULLIGAN, CONG. RSCH. SERV., LSB11273, LETTERS OF MARQUE AND REPRISAL (PART 2): DRAFTING HISTORY AND U.S. PRACTICE 3 (2025).

104. See Kessinger, *supra* note 57, at 9.

105. *The Paquete Habana*, 175 U.S. 677, 700 (1900).

106. See *id.* (“[W]here there is no treaty, and no controlling executive or legislative act or judicial decision, resort must be had to the customs and usages of civilized nations; and, as evidence of these, to the works of jurists and commentators who by years of labor, research, and experience, have made themselves particularly well acquainted with the subjects of which they treat.”).

107. See Cooperstein, *supra* note 30, at 253; Anthony J. Bellia Jr. & Bradford R. Clark, *The Law of Nations As Constitutional Law*, 98 VA. L. REV. 729, 729-30 (2012).

108. Press Release, Rep. David Schweikert, *Schweikert Introduces Cybercrime Marque and Reprisal Authorization Act to Combat Foreign Scam Syndicates* (Aug. 20, 2025), <https://schweikert.house.gov/2025/08/20/schweikert-introduces-cybercrime-marque-and-reprisal-authorization-act-to-combat-foreign-scam-syndicates/> [<https://perma.cc/2PVT-UGNQ>].

109. See generally Rosenzweig, *supra* note 58, at 110 (If piracy is the right analogy, then private sector aggressive cyber defense may well be unlawful, and even aggressive countermeasures by nation-states might have to respect the sovereignty of other countries).

non-intervention.¹¹⁰

In both U.S. and international law, a cyberattack is considered an act of war requiring congressional approval when its scale and effects mirror a traditional kinetic strike, resulting in death, injury, or significant physical destruction.¹¹¹ Because there are no universally binding international criteria, these determinations are made on a case-by-case basis using a “consequence-based” approach.¹¹² Under this standard, digital operations that cause catastrophic outcomes, such as destroying a dam to displace populations, inducing a nuclear meltdown, or hijacking air traffic control systems to cause crashes, are viewed as equivalent to kinetic military strikes.¹¹³ Factors such as the intent to cause grave harm, the immediacy of the threat, and the overall severity of the disruption are the primary metrics for identifying an act of war.¹¹⁴

Under the U.S. Constitution, only Congress has the power to declare war, and the War Powers Resolution generally requires the President to seek authorization for introducing armed forces into hostilities.¹¹⁵ While presidential authority as Commander-in-Chief allows self-defense actions, recent legislation still notes that the War Powers Resolution¹¹⁶ may apply to certain military cyber operations. The proposed Cybercrime Marque and Reprisal Authorization Act of 2025 attempts to bypass some of these ambiguities by authorizing private actors,¹¹⁷ but if such a private operation were to result in mass casualties, it would likely fall under existing war powers scrutiny, creating potential legal conflicts.¹¹⁸ The consensus remains that the physical effects of an attack are the decisive factor.

110. *See id.* at 112 (Letters of marque and reprisal are, essentially, “a license authorizing a private citizen to engage in reprisals against citizens or vessels of another nation”).

111. Greg Mgrditchian & Ernest A. Yazzetti, Jr., *2013 National Lawyers Convention International: Cybersecurity-the Policy and Politics of A Leading National Security Threat*, 41 RUTGERS COMPUTER & TECH. L.J. 194, 212 (2015).

112. *Id.*

113. *See* Hathaway et al., *supra* note 5 at 847 (a cyber-attack need only penetrate a critical system to justify a conventional military response that could start a physical, kinetic war—this approach could undermine the security of the international community by making war much more likely).

114. *See id.* at 848 (The key criterion determining when a cyber-attack constitutes an armed attack is the severity of the harm caused. A cyber-attack justifies self-defense “only if its foreseeable consequence is to cause physical injury or property damage and, even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion.”).

115. U.S. CONST. art. I, § 8, cl. 11.

116. 50 U.S.C. §§ 1541–48.

117. Cybercrime Marque and Reprisal Authorization Act of 2025, H.R. 4988, 119th Cong. (2025).

118. *See* Hathaway et al., *supra* note 5, at 848 (Under this test, a cyber-attack on the air traffic control system causing planes to crash would be regarded as an armed attack because it is foreseeable that such an attack would cause loss of life and substantial property damage.).

B. Constitutional Authority in the Cyber Domain

The Letters of Marque and Reprisals Clause is a frequently overlooked component of the U.S. Constitution that grants Congress the power to authorize private actors to engage in retaliatory actions.¹¹⁹ In the digital age, this clause faces new scrutiny as a potential tool for “hacking back” against foreign threats.¹²⁰ The primary tension lies in the Separation of Powers: while Congress has the authority to issue these letters, the President, as Commander in Chief, oversees the execution of national defense.¹²¹ This jurisdictional overlap becomes particularly complex when digital attacks originate from state-sponsored actors, triggering the President’s foreign affairs powers.

While Article I gives Congress the power to “define and punish Piracies and Felonies committed on the high seas,” modern digital incursions, such as ransomware or state-led sabotage, often fall outside traditional legal definitions of piracy.¹²² However, historical precedent suggests a shared responsibility. Just as President Jefferson navigated maritime warfare against the Barbary States by merging his Commander-in-Chief authority with Congressional intent, a modern administration might argue that thwarting threats to national digital infrastructure and commerce justifies the use of private cyber-operatives.¹²³

Historical crises, from the use of privateers in the Revolutionary War to the response to Confederate commerce raiding, demonstrate that presidential power is at its peak when facing “quasi-sovereign” threats that endanger the nation’s economic lifeblood. In cyberspace, the Commander-in-Chief clause can be construed not as a declaration of war but as a defensive mandate to neutralize threats to national security and global trade.¹²⁴ By marrying executive action with the spirit of the Letters of Marque, the government could theoretically authorize private “cyber-privateers” to protect the digital commons.¹²⁵

Historically, a Letter of Marque served as the line of demarcation between illegal piracy and legitimate state-sanctioned defense. Although the 1856 Paris Declaration Respecting Maritime Law abolished privateering, the United States never formally acceded to it, leaving a theoretical opening for the use of private vessels, or in this case, private security firms, to respond to violence.¹²⁶

In the current landscape, the absence of a clear government framework

119. See generally JAY WEXLER, *THE ODD CLAUSES: UNDERSTANDING THE CONSTITUTION THROUGH TEN OF ITS MOST CURIOUS PROVISIONS* (2011) (“[t]he United States hasn’t issued a letter of marque or reprisal in almost two hundred years.”); accord Spence, *supra* note 39, at 286.

120. See Rosenzweig, *supra* note 58, at 105 (defining “hack back” as “[T]he synchronized, real-time capability to discover, detect, analyze, and mitigate threats.”).

121. See U.S. CONST. art. I, § 8, cl. 11; U.S. CONST. art. II, § 2, cl. 1.

122. U.S. CONST. art. I, § 8, cl. 10.

123. See Robert F. Turner, *State Responsibility and the War on Terror: The Legacy of Thomas Jefferson and the Barbary Pirates*, 4 CHI. J. INT’L L. 121, 128-29 (2003).

124. U.S. CONST. art. II, § 2, cl. 1.

125. See generally Rosenzweig, *supra* note 58, at 113 (discussing piracy as not prohibited by the Paris Declaration and analogizing to cyber privateering).

126. *Id.* (discussing the legality of cyber privateers).

leaves private corporations in a legal gray area, unsure if hiring Private Cyber Security Contractors (“PCSCs”) to “hack back” or neutralize threats is lawful. Given the scale of modern digital crises and the legal hurdles of direct military intervention, authorizing private entities through a modernized “Digital Letter of Marque” may offer a temporary solution to secure the global digital economy.¹²⁷

C. The Paris Declaration: Has it Ripened into Customary International Law?

In 2026, the question of whether the 1856 Paris Declaration has “ripened” into binding customary international law has moved from academic debate to an urgent matter of national policy.¹²⁸ This legal evolution is unfolding against a backdrop of persistent gray-zone conflicts and strained national budgets, where the centuries-old concept of privateering found fertile ground for revival. Practical necessity drives this movement. Nations are eager to exert global influence without the staggering financial and political costs of traditional military engagement.

The central argument for this new age of “state-sponsored sea dogs” rests on sheer cost-effectiveness.¹²⁹ As modern defense budgets struggle to fund the construction of long-lead warships, private military companies have stepped forward to offer ready-made capacity.¹³⁰ By authorizing private firms to bear the costs of vessels, crews, and equipment, governments can project power through privateers rather than expensive, state-maintained cruisers.¹³¹ This strategy has proven particularly relevant in theaters of economic warfare, such as the Strait of Hormuz, where alliances of nations have employed commissioned privateers to target “ghost fleets” of sanctioned oil tankers.¹³² Operating under strict but opaque letters of marque, these actors inflict steep economic costs on adversaries while maintaining a low-footprint form of deterrence.¹³³

This utility has extended beyond the physical waves into the digital realm, where legislative proposals in the United States have sought to adapt “letters of marque and reprisal” for cyberspace.¹³⁴ This framework allows vetted “white

127. Joshua Parisi, “*WWW*” *Marques the Spot: Privateering as a Solution to Cryptocurrency Theft*, 72 S. METHODIST U.L. REV. 895, 912 (2019).

128. See Rosenzweig, *supra* note 58, at 112-13.

129. John M. Golden, *Patent Privateers: Private Enforcement’s Historical Survivors*, 26 HARV. J.L. & TECH. 545, 560 (2013).

130. Montgomery Sapone, *Have Rifle with Scope, Will Travel: The Global Economy of Mercenary Violence*, 30 CAL. W. INT’L L.J. 1, 17 (1999).

131. *Id.*

132. See Stop Harboring Iranian Petroleum Act, Pub. L. No. 118-50, div. J, 138 Stat. 915, 966 (2024) (codified at 22 U.S.C. § 10101 note) [hereinafter SHIP Act]; Exec. Order No. 14,390, 91 Fed. Reg. 18,271 (Mar. 6, 2026).

133. See Sapone, *supra* note 130, at 134.

134. See Scam Farms Marque and Reprisal Authorization Act of 2025, H.R. 4988, 119th Congress (2025).

hat” hackers to execute government-authorized “hack-backs” against foreign threats and sophisticated criminal cartels. For the government, the allure of this approach lies in plausible deniability. Operations conducted by private actors offer a degree of separation, allowing states to disrupt enemy operations without triggering the full diplomatic fallout or the rigid rules of engagement associated with official military action.

However, the question remains whether the Paris Declaration, which the United States never signed, now carries the weight of customary international law that forbids such practices. Critics argue that the benefits of privateering are outweighed by the risk of dismantling the international rules-based order and blurring the lines between legitimate combatants and opportunistic mercenaries.¹³⁵ While the return of the privateer offers a pragmatic solution to modern capability gaps in the maritime and cyber domains, it reintroduces a chaotic element into global conflict, challenging the fragile 170-year consensus that sought to keep private warfare abolished.¹³⁶

In 2026, the global landscape is increasingly defined by gray-zone conflicts, a strategic space that exists in the volatile middle ground between peaceful diplomacy and all-out conventional war. These conflicts are characterized by an intentional ambiguity. Actors seek to achieve major geopolitical goals through aggression that is calibrated to remain just below the “red lines” or legal thresholds that would trigger a decisive military response. By operating in this shadow area, nations can challenge the international order while maintaining a degree of plausible deniability.

The hallmark of a gray-zone campaign is the use of non-traditional tools to exert pressure. This includes the deployment of “maritime militias,” civilian-appearing vessels used to harass commercial shipping or probe undersea infrastructure, and the execution of sophisticated cyberattacks designed to degrade a nation’s economy without firing a single shot. In 2026, these tactics are often supported by AI-driven disinformation campaigns intended to destabilize a target’s domestic politics and social cohesion from within.¹³⁷

Strategic experts often describe this as a “salami-slicing” strategy, where a series of small, incremental provocations, none of which alone justify a declaration of war, cumulatively result in a significant strategic shift.¹³⁸ By the time a defender realizes the extent of the damage, the aggressor has already established a new “normal” on the ground or in cyberspace. Consequently, the

135. See Rosenzweig, *supra* note 58, at 117.

136. See *id.*

137. Ben Crowell & Wade Turvold, *Illegal, Unreported, and Unregulated Fishing, and the Impacts on Maritime Security*, in HINDSIGHT, INSIGHT, FORESIGHT: THINKING ABOUT SECURITY IN THE INDO-PACIFIC 209, 214–15 (Alexander L. Vuving ed., 2020).

138. See Richard W. Maass, *Salami Tactics: Faits Accomplis and International Expansion in the Shadow of Major War*, 5 TEX. NAT’L SEC. REV. 33, 33 (2021); see also Lorenz Langer, *The South China Sea As A Challenge to International Law and to International Legal Scholarship*, 36 BERKELEY J. INT’L L. 362 (2018) (citing Robert Haddick, *Salami Slicing in the South China Sea*, FOREIGN POL’Y (Aug. 3, 2012) (describing “salami slicing” as the accumulation of small actions that, over time, add up to a major strategic shift)).

gray zone has become the primary arena for modern power competition, forcing governments to develop new legal and military frameworks to counter threats that are too aggressive to ignore but too subtle to meet with traditional force.

VI. THE THRESHOLD OF CONFLICT: WAR POWERS, ACCOUNTABILITY, AND THE EXTRATERRITORIAL CHALLENGE IN CYBERSPACE

In both U.S. and international law, a cyberattack rises to the level of an act of war requiring congressional approval when its scale and effects mirror those of a traditional kinetic armed attack, resulting in death, injury, or significant physical destruction. Under the prevailing “consequence-based” approach endorsed by the Tallinn Manual and the U.S. State Department, digital operations are viewed as equivalent to military strikes if they cause catastrophic outcomes such as nuclear meltdowns, the destruction of dams, or the hijacking of air traffic control systems.¹³⁹ Beyond physical damage, the determination depends on the severity, immediacy, and scale of the disruption, as well as the clear intent to cause grave harm or destabilization.¹⁴⁰

This legal threshold directly impacts U.S. domestic law, where the Constitution vests the power to declare war solely in Congress.¹⁴¹ While the War Powers Resolution requires the President to seek authorization for hostilities, modern executive authority often relies on the Commander-in-Chief’s power to act in self-defense. Recent laws, such as Public Law 117-263, authorize the Defense Secretary to conduct military cyber operations to defend critical infrastructure, often framing these as actions “short of hostilities.”¹⁴² However, the proposed Act seeks to bypass traditional war power ambiguities by authorizing private actors. If a private operation under a letter of marque were to trigger mass casualties, it would likely fall under existing war powers scrutiny and conflict with the U.N. Charter’s restrictions on the use of force.

A major legal hurdle for such legislation is the presumption against extraterritoriality, a principle holding that U.S. laws apply only within the United States unless Congress explicitly states otherwise.¹⁴³ This principle is justified by the need for international comity, respect for congressional intent regarding domestic matters, and the maintenance of checks and balances. To determine if a law applies abroad, the Supreme Court utilizes a two-step analysis: first, looking for a clear indication of congressional intent, and second, determining if the “focus” of the conduct occurred within the U.S.¹⁴⁴ Because the decentralized nature of cyberspace makes it difficult to pinpoint the location

139. Harold Hongju Koh, Remarks at USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012) (transcript archived at the U.S. Department of State) (explaining what constitutes the use of force in cyberspace).

140. See Hathaway et al., *supra* note 5, at 847.

141. U.S. CONST. art. I, cl. 2.

142. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, 136 Stat. 2395 (2022).

143. Hathaway et al., *supra* note 5, at 877.

144. Nestle USA, Inc. v. Doe, 593 U.S. 628, 632-33 (2021).

of activity, any legislation like H.R. 4988 must contain explicit language to overcome this presumption and provide legal clarity for authorized actions against foreign threats.

VII. CONFLICTS WITH INTERNATIONAL LAW

International law principles applicable to cyber conflict in 2026 are primarily anchored in the U.N. Charter and international humanitarian law.¹⁴⁵ At the core of peacetime regulations is the principle of state sovereignty, which requires nations to respect the territorial and internal independence of others, meaning unauthorized network penetrations are generally considered legal violations. This is closely linked to the prohibition of the use of force under Article 2(4) of the U.N. Charter, where cyber operations are categorized as a use of force if their scale and effects mimic kinetic attacks, such as those causing physical destruction or loss of life.¹⁴⁶ Correspondingly, Article 51 preserves a state's inherent right to self-defense if a cyber operation reaches the threshold of an armed attack.¹⁴⁷

Beyond these prohibitions, the principle of due diligence dictates that states must ensure their territory is not knowingly used for malicious activities that harm the rights of other nations. This is complemented by the principle of non-intervention, which forbids coercive interference in the internal affairs of a state, particularly regarding electoral integrity or essential government functions.¹⁴⁸

When cyber operations occur within the context of an armed conflict, the framework shifts to international humanitarian law, often referred to as *jus in bello*.¹⁴⁹ The principle of distinction is paramount, requiring that attackers differentiate between civilian objects and military objects to ensure that digital strikes are never directed at the public. This is balanced by the principle of proportionality, which prohibits any attack where the anticipated civilian harm, including indirect effects like the collapse of a power grid, is excessive compared to the direct military advantage gained.¹⁵⁰ Furthermore, the principles of military necessity and precautions in attack require states to limit their operations to legitimate goals and take all feasible measures to minimize incidental civilian damage. By 2026, these frameworks will have evolved through the U.N.'s Global Mechanism, which increasingly treats civilian data

145. U.N. Charter art. 2, para. 4; see generally FRANÇOIS DELERUE, THE THRESHOLD OF CYBER WARFARE: FROM USE OF CYBER FORCE TO CYBER ARMED ATTACK, in THE LAWFULNESS OF CYBER OPERATIONS 273-342 (Cambridge Univ. Press 2020) (recognizing that the UN Charter's drafters in 1945 could not have anticipated military cyber operations, but its deliberately flexible language allows it to adapt and apply to such modern developments).

146. See generally *id.* (summarizing that under the UN Charter, cyber warfare begins at the Article 2(4) threshold for the threat or use of force; only cyber operations that rise to that level can qualify as cyber warfare under *jus contra bellum*).

147. U.N. Charter, para. 51.

148. See Hathaway et al., *supra* note 5, at 848.

149. See Delerue, *supra* note 145.

150. See Koh, *supra* note 138.

as a protected object under humanitarian law, reflecting a strategic shift in how international law governs the digital domain.¹⁵¹

The delegation of sovereign power to private companies operating extraterritorially directly conflicts with foundational principles of state sovereignty under international law, which grants a state exclusive authority over its territory. The U.N. Charter generally prohibits the unilateral use of force and emphasizes state sovereignty and non-intervention in the affairs of other nations.¹⁵² While cyber operations exist in a legal “grey zone,” state-sanctioned “hack-backs” could violate the U.N. Charter’s prohibition on the use of force or, at the very least, escalate cyber conflicts. Actions by private U.S. cyber operators against foreign entities, even if authorized by the U.S. government, could be construed as violations of these principles, potentially triggering international disputes or retaliatory actions.

In 2026, the international legal community largely adheres to the “scale and effects” test to determine if a cyber operation constitutes a use of force under Article 2(4) of the UN Charter.¹⁵³ A cyber operation is considered a use of force when its consequences are comparable to those of a traditional kinetic or armed attack.¹⁵⁴ The most prominent examples include operations that directly cause physical injury or death to humans, such as the remote manipulation of a regional air traffic control system to cause a mid-air collision or the hijacking of medical device networks to disrupt life-saving treatments.¹⁵⁵

Beyond direct casualties, operations that cause significant physical destruction of property are also classified as a use of force.¹⁵⁶ This includes the use of malware to override safety protocols at an industrial facility, such as a chemical plant or a nuclear power station, leading to a catastrophic explosion or toxic leak.¹⁵⁷ Similarly, a cyberattack on a national power grid that results in a prolonged, widespread blackout causing secondary deaths and massive infrastructure failure would meet this threshold. In the maritime and logistics sectors, the remote sinking of a commercial or military vessel by manipulating its ballast or navigation systems is considered a clear act of force.¹⁵⁸

Legal interpretations have also expanded to include “functional equivalents” of physical damage. For instance, a cyber operation that permanently disables a nation’s primary financial exchange or its telecommunications backbone, effectively “bricking” the hardware so it is no

151. United Nations Convention Against Cybercrime, *opened for signature* Oct. 25, 2025, G.A. Res. 79/243, U.N. Doc. A/RES/79/243 (Dec. 24, 2024).

152. *See* Koh, *supra* note 138 (cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law).

153. *Id.*

154. *See id.*; *see also* Hathaway, *supra* note 5, at 826.

155. *Id.* at 817 (Cyber-attacks have become increasingly common in recent years. Capable of shutting down nuclear centrifuges, air defense systems, and electrical grids, cyber-attacks pose a serious threat to national security.).

156. *Id.*

157. *Id.*

158. *Id.*

longer usable, is increasingly treated as a use of force due to the severity of the societal and economic devastation. While mere espionage or temporary website defacement generally falls below this threshold, any digital act that results in a “kinetic-like” impact is categorized as a use of force, potentially triggering a state’s right to respond in self-defense.¹⁵⁹

The transition from maritime security to digital defense reveals significant challenges and gaps in the legal landscape. Jurisdictional complexity serves as a primary hurdle. Whereas terrestrial law relies on territory and maritime law relies on the “flag state,” cyberspace mirrors the non-territorial nature of international waters. This creates a jurisdictional maze where actors can bypass stringent national regulations, much like ships using flags of convenience, making attribution and legal recourse exceptionally difficult.¹⁶⁰

The use of force and the establishment of clear rules of engagement present another central conflict. While states typically maintain a monopoly on the use of force, private entities operate within a persistent grey area. In maritime contexts, private guards are generally limited to self-defense against criminal acts of piracy, yet the line between protection and excessive force frequently blurs, leading to diplomatic incidents.¹⁶¹ This ambiguity is amplified in the abstract realm of cyberspace, where defining what constitutes a proportional response versus an act of aggression remains intensely debated.

Furthermore, the structure of corporate vs. individual accountability complicates the enforcement of international standards. Because private military and security companies are corporate bodies, they cannot be tried in international criminal courts; only individual employees face such charges. This reality makes it nearly impossible to trigger state responsibility for wrongful conduct, especially as companies can dissolve and reform under new identities to evade financial liability. Despite these hurdles, the persistent presence of these private actors has begun to play a normative role, subtly pushing states to formalize and regulate the involvement of non-state actors in national and international security frameworks.

This entire debate is framed by the presumption against extraterritoriality, a core principle of U.S. statutory interpretation that assumes U.S. laws apply only domestically to respect the sovereignty of other nations and ensure Congress makes key foreign policy decisions.¹⁶² Courts use a two-step test to determine if a statute applies abroad: first, looking for a clear indication from Congress, and

159. See Koh, *supra* note 138 (A State’s national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof. As the United States affirmed in its 2011 International Strategy for Cyberspace, “when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country.”).

160. See generally Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction’s Hollow Foundation*, 45 Harv. Int’l L.J. 183, 184 (2004) (recognizing that an assertion of universal jurisdiction may cause conflict and hostilities among countries if it is seen as an encroachment on the sovereign authority of the country with traditional jurisdiction).

161. See *id.* at 185.

162. *Kiobel v. Royal Dutch Petroleum*, 569 U.S. 108 (2013).

second, determining if the focus of the conduct occurred within the U.S.¹⁶³ This presumption creates a challenge for cyber legislation, as the decentralized nature of cyberspace makes it difficult to pinpoint the location of activity. To provide clarity for authorized actions against foreign threats, legislation must explicitly state its intent for extraterritorial application to overcome this presumption.¹⁶⁴

Reviving privateering in either the maritime or cyber domain would likely prompt significant negative international reactions, legal challenges, and potential escalation of conflicts, potentially casting the United States as an outlaw nation and increasing global instability. Reactions from other countries would likely focus on diplomatic condemnation and legal challenges. The international community has widely considered privateering, abolished under the 1856 Paris Declaration, which has ripened into customary international law.¹⁶⁵ A U.S. revival would therefore be seen as a blatant disregard for established international norms.

Using private actors also blurs the crucial legal distinctions between state agents, combatants, and civilians, creating complex issues regarding accountability under international humanitarian law.¹⁶⁶ Other nations would raise concerns about controlling these private entities, especially if they operate outside strict governmental command structures or commit abuses. Furthermore, in the cyber domain, private actors conducting “hack-backs,” or disruptive operations, could easily affect networks and infrastructure in third-party countries. These nations would likely view such actions as violations of their sovereignty, leading to strong political pushbacks and diplomatic friction.

The move would also likely trigger escalation and reciprocal actions. Adversaries such as China, Russia, and Iran, which already use state-sponsored cyber tactics, would likely use the U.S. move as a justification for escalating their own actions and potentially authorizing their own privateers, conceivably leading to a global free-for-all in both the maritime and cyber domains. Increased tensions would also result from using privateers to target commercial shipping, which would directly impact global trade and create security dilemmas for all nations. The use of private actors, a key element of hybrid warfare, is designed to offer plausible deniability, but this also makes official de-escalation mechanisms more difficult, as the U.S. government would struggle to manage the actions of personnel not integrated into a normal chain of command.

Finally, reviving privateering would likely damage alliances. Many U.S. allies, who strongly support a rules-based international order, would be uncomfortable with the practice. This could jeopardize international cooperation on maritime security and the development of much-needed cyber norms. The “piracy” narrative would become a powerful tool for U.S. adversaries in information warfare, further damaging public support for U.S.

163. *See Nestle USA, Inc. v. Doe*, 593 U.S. 628 (2021).

164. *Id.*

165. *See LEMNITZER, supra* note 50.

166. *See e.g. Collin S. Allan, Attribution Issues in Cyberspace*, 13 CHI.-KENT J. INT’L & COMP. L. 55, 64 (2013).

actions both domestically and internationally. In essence, reviving privateering would likely be perceived as a dangerous regression to a more chaotic form of conflict, leading to damaged U.S. diplomatic standing and increased global instability.

VIII. THE ACCOUNTABILITY PARALLEL: LAND VS. MARITIME PRIVATE SECURITY COMPANIES

The concerns surrounding H.R. 4988 are not theoretical; they echo the real-world challenges governments face using private military and security companies (“PMSCs”), both on land and at sea. The growth of the PMSC industry, following military downsizing after the Cold War, created a robust global market, often filled with ex-military personnel. This “privatization of security” introduces significant accountability gaps and legal ambiguities that serve as a crucial cautionary tale for the proposed cyber marque system.¹⁶⁷

H.R. 4988 mirrors existing accountability issues with Private Military Companies (“PMCs”). PMSCs share many similarities with historical privateers, despite being primarily employed by private entities. Today, these contractors provide clients with essential services such as intelligence, infrastructure security, and risk analysis. While not a permanent solution to maritime insecurity, they serve as a necessary temporary measure to mitigate rising shipping costs and the loss of life at sea.¹⁶⁸ The unique difficulty of attributing cyberattacks adds a layer of complexity. Inaccurate targeting by a cyber privateer could trigger unintended cyber conflicts with potentially severe consequences.¹⁶⁹

In the realm of piracy, relying solely on national navies is increasingly impractical. In recent years, global maritime forces have become severely overstretched.¹⁷⁰ Beyond persistent piratical attacks, the international community is managing multiple major crises, including the ongoing Russia-Ukraine war and escalated conflicts in Gaza, fueled by threats from Iran and Hezbollah. These concurrent flashpoints have forced regular militaries to prioritize high-stakes regional stability over routine merchant vessel protection, leaving a security gap that PMSCs now fill.¹⁷¹

However, the practice comes with perils for states in the same way that the use of privateers historically pushed their governments into full-scale wars. When privateers violated the laws and customs of war, their home governments often lacked the means to enforce accountability, leading to abuses against

167. *Id.* at 64.

168. Spence, *supra* note 39, at 290-91.

169. *See generally* Allan, *supra* note 166, at 64-65 (under international law, state-authorized conduct is attributable to the authorizing state—even when carried out by private individuals—because authorization effectively makes such actors de facto state organs, most commonly when states recruit private groups for cross-border missions).

170. Spence, *supra* note 39, at 290-91.

171. *Id.*

foreign ships and their crews. Monitoring the actions of privateers/PSCs operating far from governmental authority was nearly impossible.¹⁷²

These uncontrolled and potentially criminal actions created diplomatic incidents and risked escalating conflicts.¹⁷³ The use of PMCs has highlighted significant accountability gaps, often involving debates over jurisdiction and oversight in conflict zones.¹⁷⁴ The unique complexities of attribution in cyberspace exacerbate these issues. A cyberattack launched by a private entity could be easily misattributed or designed to appear as the work of another actor, further complicating international relations and the application of legal standards. The lack of transparent, verifiable operational control makes the PMSC model in cyberspace particularly risky. The central tension is whether a power designed for 19th-century naval warfare can be safely and effectively repurposed for 21st-century digital conflicts, which lack clear battlefields, borders, and established international norms for private-actor engagement.

IX. ALTERNATIVES FOR GOVERNANCE: ADAPTING EXISTING FRAMEWORKS

To address the persistent legal gaps surrounding private security actors, the international community has developed “soft law” frameworks designed to provide guidance where binding treaties are absent. Rather than reviving an outdated and discredited concept, this paper evaluates how existing regulatory frameworks could be adapted to provide a more robust and legally sound mechanism for governing private cyber operators. The Montreux Document, which clarifies international legal obligations related to PMSCs in armed conflict, offers a foundational structure for ensuring compliance with international law.¹⁷⁵

The Montreux Document serves as a primary example, clarifying the existing legal obligations of states regarding private military and security companies during armed conflicts. Although originally intended for land-based operations, its principles have been extended to maritime security, emphasizing that private personnel remain civilians protected from attack unless they directly participate in hostilities.¹⁷⁶ This nonbinding document clarifies the international legal obligations of states concerning PMSCs in armed conflict. It could be a model for applying existing international law to govern private actors in cyberspace.

Complementing this is the International Code of Conduct for Private Security Service Providers (“ICoCPSS”), a voluntary, principles-based

172. Grace Rodden & James Walsh III, *The Legal Issues of Private Armed Security on Commercial Ships*, 58 *FED. LAW.* 30, 32 (2011).

173. *See id.* at 33-34.

174. *Id.* at 32.

175. Permanent Rep. of Switzerland to the U.N., Letter dated Oct. 2, 2008 from the Permanent Rep. of Switzerland to the United Nations addressed to the Secretary-General, U.N. Doc. A/63/467-S/2008/636 (Oct. 6, 2008).

176. *Id.* at ¶ 26.

framework that encourages these companies to respect human rights and humanitarian law in their global operations.¹⁷⁷ Adapting principles from the Montreux Document and the ICoCPSS could lead to a more stable environment.

However, these frameworks also highlight the ongoing struggle to ensure true compliance and accountability. Because they are not legally binding and rely heavily on national enforcement, significant regulatory gaps remain. Applying these lessons to the digital domain suggests that simply authorizing cyber letters of marque without a robust, internationally agreed-upon governance structure would likely replicate the existing challenges seen with private military companies. Without such a foundation, the use of private actors in cyberspace risks exacerbating oversight issues and potentially leading to the same lack of accountability found in traditional private security sectors.

X. CONCLUSION

Ultimately, H.R. 4988 falters by attempting to revive the “letter of marque,” an outdated and discredited concept, ill-suited for modern conflict. By prioritizing a framework rooted in established international law over state-sponsored privateering, policymakers can better promote stability and prevent unintended escalation in the digital domain.¹⁷⁸ The history of PMSCs warns that without a binding international treaty, national enforcement alone leaves dangerous gaps in accountability. Tech leaders, including those at Armis, have already demonstrated that state-level threats are best combated through proactive, data-driven defense and collective technological preparation rather than unregulated offensive proxies.¹⁷⁹ To ensure a secure digital future, modern governance must move beyond the limitations of H.R. 4988, prioritizing robust oversight, clear chains of command, a steadfast commitment to state sovereignty, and the responsible use of force in cyberspace.

177. See *Int'l Code of Conduct for Priv. Sec. Serv. Providers*, ¶¶ 30-31 (as amended Dec. 10, 2021).

178. See generally Allan, *supra* note 166, at 72 (noting that scholars are mixed regarding whether Article 2(4) of the UN Charter should be concretely interpreted to cyber-attacks or if specific treaties on cyber-attacks would prove more useful).

179. See Weigand, *supra* note 6.