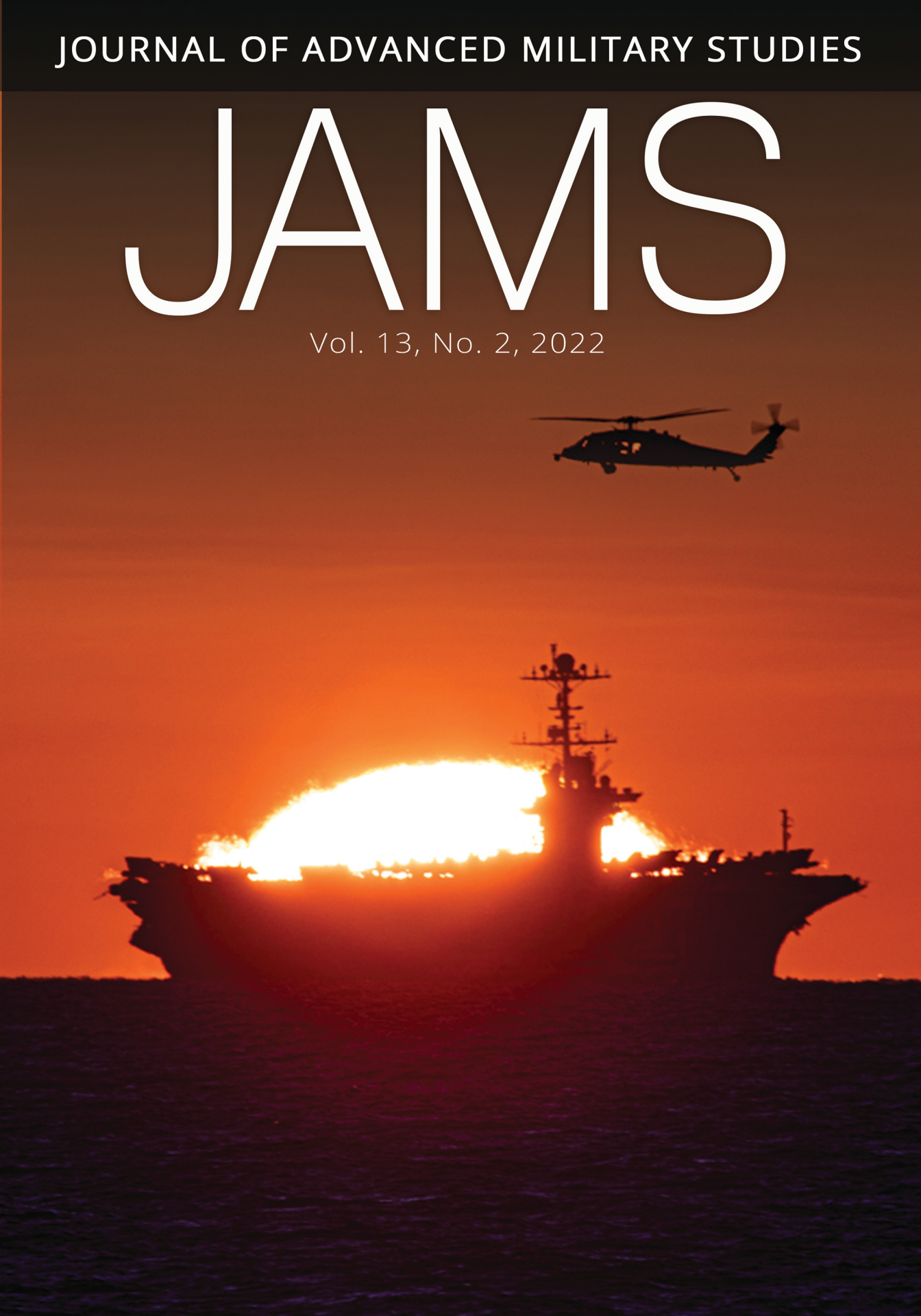
JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

Vol. 13, No. 2, 2022



JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

MCUP

Published by Marine Corps University Press
2044 Broadway Street | Quantico, VA 22134

Journal of Advanced Military Studies
(Print) ISSN 2770-2596
(Online) ISSN 2770-260X

Established in 2008, MCU Press is an open access publisher that recognizes the importance of an open dialogue between scholars, policy makers, analysts, and military leaders and of crossing civilian-military boundaries to advance knowledge and solve problems. To that end, MCUP launched the *Journal of Advanced Military Studies* (JAMS) to provide a forum for interdisciplinary discussion of national security and international relations issues and how they have an impact on the Department of Defense, the Department of the Navy, and the U.S. Marine Corps directly and indirectly. JAMS is published biannually, with occasional special issues that highlight key topics of interest.

ARTICLE SUBMISSIONS
The editors are looking for academic articles in the areas of international relations, geopolitical issues, national security and policy, and cybersecurity. To submit an article or to learn more about our submission guidelines, please email MCU_Press@usmcu.edu.

BOOK REVIEWS
Send an email with a brief description of your interests to MCU_Press@usmcu.edu.

SUBSCRIPTIONS
Subscriptions to JAMS are free. To join our subscription list or to obtain back issues of the journal, send your mailing address to MCU_Press@usmcu.edu.

ADDRESS CHANGE
Send address updates to MCU_Press@usmcu.edu to maintain uninterrupted delivery.

INDEXING
The journal is indexed by ProjectMUSE, Scopus, EBSCO, ProQuest, OCLC ArticleFirst, Defense Technical Information Center, Journal Seek, IBZ Online, British Library System, Lancaster Index to Defense and International Security Literature, and AU Library Index to Military Periodicals.

The production of this journal and other MCUP products is graciously supported by the Marine Corps University Foundation.

Contents

Vol. 13, No. 2

Like the Sea, So Cyberspace
A Brief Exploration of Establishing Cyberspace Norms through a Maritime Lens

Lieutenant Commander Travis D. Howard, USN (Ret); and Jose de Arimateia da Cruz, PhD/MPH

Abstract: This article compares the history of establishing maritime laws, norms, customs, and standards of conduct with the rise of cyberspace as an artificial domain akin to a digital sea. A brief history of how humanity established enduring norms and standards at sea is described, followed by a comparative analysis of the world's physical maritime domain to digital cyberspace. Recommendations are made for contextualizing cyber threats and policy issues within a naval framework. Finally, the authors offer some brief conclusions.

Keywords: cyberspace, international norms, maritime, piracy, ransomware, cyberwar

Humanity has always held an innate attraction to the maritime domain.[1] It is as familiar and fundamental to us as anything on this Earth, and we have been drawn to it for trade, war, transportation, and nourishment. It has been here for eons in all its splendor and was not made by humankind. Nations have claimed it, but no one can control the sea: one can only hold portions of it at a time—meager territorial claims over a vast ocean scape—a tenuous grasp at best. Over centuries, humanity has learned to coexist with the world's oceans and establish international standards of conduct to share this common good.

LtCdr Travis Howard, USN (Ret), CISSP-ISSMP, is a senior information security professional with more than 20 years in the field focusing on cybersecurity policy, strategy, and risk management in the national defense sector and is a PhD candidate at Capitol Technology University studying cybersecurity leadership. He is a retired U.S. naval officer with advanced qualifications in information warfare and surface warfare and taught global cybersecurity at Georgia Southern University, Savannah, GA, as an adjunct. Dr. Jose de Arimateia da Cruz is a professor of international relations and comparative politics at Georgia Southern University and a research professor at the U.S. Army War College Center for Strategic Leadership Homeland Defense and Security Issues, Carlisle, PA.

Journal of Advanced Military Studies vol. 13, no. 2
Fall 2022
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20221302007

The internet, on the other hand, was created by humankind. Born from the Advanced Research Projects Agency Network (a.k.a. ARPANET) in the 1960s, this small network of academic and research institutions has grown from four sites to hundreds of thousands worldwide.[2] Today (as of this draft), the internet contains 4.36 billion pages of information, with the estimated size of Google's total index in the tens of trillions.[3] More broadly, the internet is an environment within the more extensive *cyberspace*: a complex mesh of networks, devices, and elastic nodes by which humankind's information is communicated globally. It is the sum of human knowledge given a matrixed, semicorporeal form of data centers, gateways, and cables—a vast, digital sea of information and organizations. The term *cyberspace*, coined by science fiction writer Ford Gibson in his 1984 novel *Neuromancer*, has since captured the world's imagination and has been used in academic, policy, and media circles for decades. Recent scholars have argued that cyberspace, as a general medium of communication and information sharing, has been around since the discovery of the telegraph.[4] Terms like *netizen*, denoting an active participant of the internet, have made their way into dictionaries like Merriam-Webster (the irony of quoting an online dictionary, once widely available in print, is not lost on the authors).[5]

Much of society's activities involve cyberspace these days: trade, war, transportation (of information), and nourishment (of the mind and soul). It has been described as "a new existential dimension of man," a "non-space place" that humans depend on for speed of communication, constructing and sharing visions and ideas, and performing new forms of commercial enterprises.[6] Nevertheless, our norms for dealing with this digital frontier are mainly nonexistent. Nation-states and nonstate actors exploit it, legitimate businesses anchor their livelihood within it, we entertain ourselves with it, and a grandmother talks to her grandkids via video chat halfway around the world using it.

Perhaps the reader can already see the parallels between the world's physical oceans and the artificial digital ones. Without knowing what it would become, we have created something that resembles that which we are connected to so strongly for life and livelihood: the sea. Much can be learned from the history of establishing maritime laws, norms, and standards of conduct that can be applied to cyberspace. With the world's governments and policy makers grasping at attempts to quiet the cyber threat landscape and enable economic prosperity, drawing an analogy to familiar territory is helpful.

This article seeks to inform, persuade, and encourage the public policy space and interested readers that follow defense and national security matters. The authors start with a view of vulnerabilities and threats that intrinsically tie the physical (maritime) and digital (cyberspace) to create an imperative for establishing norms. A literature review examines the current state of establishing norms. We discuss what was learned from a case study of maritime warfare—the 1980–88 "Tanker War" between Iran and Iraq—and apply those lessons to the cyber domain. Finally, we acknowledge limitations and provide recommendations to policy makers, practitioners, and researchers.

The Imperative: Cyber Threats Targeting the Maritime Domain

The International Maritime Organization's (IMO) Maritime Security and Piracy arm tracks and reports on threats to international shipping, including piracy and armed robbery against ships, and maintains a publicly available database.[7] Furthermore, history has shown that maritime warfare and actions taken by warships on the high seas threaten shipping.[8] Understanding these threats in the maritime domain is an important parallel to understanding the cyberspace domain and the dangers that hold assets at risk within both nation-states and non-nation-states.

Nation-state threats can involve warfare or law enforcement actions. Military actions within or near them can easily threaten international and commercial shipping lanes. From 1981 to 1988, military actions between Iran and Iraq affected merchant shipping in the Arabian Gulf and the Strait of Hormuz, a period known to many as the "Tanker War." The conflict eventually invoked the United Nations Security Council Resolution 598, calling for the immediate end of hostilities and the start of UN peacekeeping operations on the Iran-Iraq border until 1991.[9] Political positioning, control of oil investments, and even geography played a role in shaping this threat event as a critical example of how nation-state hostilities affect maritime shipping. George K. Walker, in his thorough review of the Tanker War in *The Tanker War, 1980–1988: Law and Policy*, noted that the conflict between the Arabian Gulf nations, which embroiled the rest of the world, resulted in the most significant loss of merchant ships and mariners' lives since World War II; more than 400 commercial ships were attacked, 200 merchant seamen were killed, and the attacks resulted in the loss of more than 40 million tons of shipped goods.[10]

Non-nation-state threats, and often the focus of much of the literature on maritime threats to commercial shipping, include piracy and terrorism. It might surprise those unfamiliar with the maritime domain to learn that piracy on the high seas continues even today, despite enjoying a 27-year low in 2021, with only 132 piracy and armed robbery incidents reported worldwide by the International Maritime Bureau (IMB).[11] A publication sponsored by the North Atlantic Treaty Organization's (NATO) Science for Peace and Security Programme describe pirate attacks on shipping that have affected maritime, transport, and insurance companies through profit loss and rising costs to transport goods and personnel safety since the turn of the twenty-first century.[12] It is worth noting that, in many cases, maritime shipping continues to face armed piracy without armaments or armed escorts, and few companies can afford (or are legally allowed) to employ private security teams.

During the last decade or more, concern has continued to mount in the maritime sector about the threats posed by cyberspace.[13] Integrated harbor systems and seagoing vessels of all sizes are increasingly reliant, perhaps now entirely dependent, on information technology and communications networks.[14] Newsworthy cyberattacks by cyber threat actors, influenced by or directly af-

filiated with nation-states, have constantly demonstrated a capability to affect operational technology (OT) and industrial control systems (ICS) through cyberspace effects.[15] Adverse cyber effects comprise a genuine threat to maritime systems and nautical operations. Recent research argued for "maritime cyber resilience," where a system can anticipate, withstand, and recover from a cyber threat with minimum downtime.[16] The convergence of OT/ICS, IT, and always-connected communications technology in the maritime domain means maritime domain leaders cannot ignore cyber threats.

Literature Review of Cyberspace Norms

Current literature on cyberspace norm development is nascent at best, owing to the emerging nature of the topic and the complex, adaptive problem it presents. Cyberspace continues to be a new and challenging domain for policy makers and diplomats and is often ill-understood.[17] The core of helpful literature on the subject comes from international relations, law, cybersecurity journals, periodicals, or government reports (most of them U.S. based). A scholarly search using EBSCO returned only 46 "cyberspace norms" results as an exact match. Much of the literature reviewed discusses nations establishing credible deterrence and cementing national sovereignty over technology infrastructure within a nation's boundaries.

Harvard International Review writer Olga Kiyan described the U.S. and Russian interests in cyberspace as fundamentally different, causing differing approaches to norm development within the United Nations. The two nations lead vastly different working groups with different conclusions.[18] She observes that this fundamental difference occurs due to how the United States and other liberal democracies view cybersecurity as a sociotechnical issue. In contrast, Russia, China, and other like-minded governments view "information security" as "consolidating state cyber sovereignty."[19] This notion is agreed on by noted international policy researcher and advisor Alexander Klimburg in his book *The Darkening Web: The War for Cyberspace*, in which he describes significant disagreement of values and definitions between liberal democracies and states that prioritize power projection, sovereignty, and control.[20]

In a 2014 analysis of "state-centric cyber peace," Dr. Scott Shackelford and Andraz Kastelic analyzed 34 national cybersecurity strategies to note governance trends that could inform international law and norms development.[21] The authors described the imperative for norm development given the difficulties in building multilateral treaties on international behavior in cyberspace and little agreement in the existing literature at the time on best practices that would inform such actions.[22] Shackelford and Kastelic concluded that, for norms to be successful, they must be "clear, useful, and do-able," and the most significant potential for agreement between disparate nations seems to be in protecting critical international infrastructure on which they all depend, such as international trade, commerce, and financial systems.[23] The authors also noted a significant lack of strategic and policy commitment among nations in prose-

cuting international cybercrime, suggesting difficulty in norm consensus for international law enforcement; the highest convergence existed in those nations with sophisticated cybercrime treatments, such as the United States and United Kingdom.[24]

Government and diplomatic reports on cyberspace norms comprise an essential part of the existing literature on the topic. Two primary groups within the United Nations continue to advocate for cyberspace norm development: The Group of Governmental Experts (GGE), comprising 25 member nations established in 2004, and the Open-Ended Working Group (OEWG), including more than 150 participating countries that formed in 2019. It is important to note that the United States, Russia, and China are active participants in both groups. However, the literature states that the GGE is dominated by U.S. and European Union thought leadership, while the Russian Federation advocates for the OEWG as the preferred method of consensus on the issue.[25]

The GGE met for almost a decade and produced numerous reports in 2010, 2013, 2015, and 2019.[26] The United Nations (UN) General Assembly adopted the 2015 GGE report as Resolution A/RES/70/237, within which states agreed to 11 nonbinding norms to promote stability, free expression, and a disavowal of malicious use of connected technology.[27] In 2017, the United States proposed criteria through the laws of war, requesting endorsement of how they applied in a cyber conflict, but it was struck down by Russia, China, Cuba, and other nations that refused to do so.[28]

In 2021, the third and final session of the OEWG in information and telecommunications resulted in the unanimous endorsement of 150 participating countries for the group's final report to the General Assembly. The report lays out recommendations for voluntary behavior norms, international law, and future dialogue for global cybersecurity. Although consensus was reached, not all countries agreed, disassociating from the final report so as not to be bound by its recommendations.[29]

Finally, it is interesting to note that existing literature has already begun to draw parallels between the maritime domain and cyberspace. Indeed, Evans Horsley's comparison of state-sponsored ransomware through a maritime piracy lens inspired this article.[30] Horsley's analysis of existing international law enforcement against piracy contained within the UN Convention on the Law of the Sea (UNCLOS) and how it could be accepted or refuted to apply to state-sponsored ransomware groups is a prime example of the ambiguous nature of existing law and the need for establishing stronger norms.[31] In the next section, we explore this further by applying a maritime lens to cyberspace norms and offer a comparison between a historical maritime conflict—the Iraq/Iran Tanker War—and how lessons learned by the international community in that conflict can be applied to cyberspace before a similar conflict erupts in the digital domain.

Applying a Maritime Lens to Cyberspace Norms

As the literature shows, state and nonstate-sponsored influences affect cyberspace just as they do in the physical realm, such as the maritime domain. Both state and nonstate cyber threats can hold public and private organizations at risk, including those that provide critical services to the public, such as power, water, and sewage infrastructure.[32] Russia, China, Iran, and North Korea have all been associated with malign cyber activity targeting U.S. critical infrastructure.[33] Of particular interest is the threat of *ransomware*, which targets government and businesses alike, and has become a money-making scheme of criminal enterprises who "focus on victims whose business operations lack resilience or whose consumer base cannot sustain service disruptions, driving ransomware payouts up."[34] Such actions invoke maritime piracy in a new domain, operating from safe-harbor nations to prey on others in an environment lacking norms and enforcement.[35]

Defining cyberspace itself has been fraught with challenges. Often described as a collection of gateways, routing, switching technology, and independent and interdependent networks, many people see cyberspace as the "worldwide web" or the internet. The reality is far more complex, blending physical and digital environments, machine-code data sets, and human-readable information; only portions of cyberspace are accessible to those with commercially available tools (such as a web browser) to view it. Gálik and Tolnaiová describe cyberspace as a hierarchy with physical, logical, information, and human layers linked and dependent on the other, with information as the basic unit or building block.[36]

As the sea contains an entire ecosystem of life and activity belonging to no single human organization, so too does cyberspace process, store, and transmit data beyond a single organization's control or even understanding, save perhaps one: the Internet Corporation for Assigned Names and Numbers (ICANN). As a multinational stakeholder governance group based in the United States but established as a nonpolitical nonprofit organization, ICANN is probably as close as we can get to an international governance group for cyberspace, compared perhaps to the IMO with significant differences in authority and political power. ICANN is not associated with an international political governing body like the United Nations and is limited in scope to the searchable internet through regulating internet protocol (IP) addresses and domain naming services (DNS).[37]

Before the IMO established the International Regulations for Preventing Collisions at Sea (agreed on in 1972 and adopted in 1977), giving way to the UNCLOS signed in 1982 by 117 states, norms within the maritime domain were regional at best.[38] Technology moved faster in the nineteenth century following the industrial revolution, sailing gave way to steam, ships moved faster, and more traffic plied the open oceans. As the premier sea power, England became the standard-bearer for international norms at sea, enforcing Admiralty Law.[39] Such early efforts to organize around international norms gave way to

the first global maritime conference in 1889, hosted by the United States, where rules were codified and agreed on, paving the way for IMO's creation.[40]

Today, 99 percent of the world's merchant tonnage has agreed to at least some IMO regulations, such as pollution prevention.[41] Such essential cooperative efforts led to other treaties, conferences, and international agreements to combat maritime threats such as piracy, thus increasing the international norms and cooperation that the domain enjoys today. The IMO supports all UN Sustainable Development Goals (SDGs) across environmental, economic, and social lines of effort.[42] Could a similar path be followed to establish standards in cyberspace for all nations?

Applying Observations and Lessons from the Tanker War to Cyberspace

Norms in cyberspace are challenging to establish because of code-based cyber weapons, the adaptive and complex nature of cyberspace itself, and the internationally universal belief in not tying one's intelligence apparatus through agreed-on rule sets. The proposed criteria, led by working groups formed through the United Nations and assisted by international think tanks, have resulted in proposed standards that range from target limitations (preventing damage to civilian infrastructure or incident response teams) to outright prohibition of certain types of malicious code.[43] Following the 2015 GGE report and subsequent resolution, in which Russia was a member and a key proponent, Russia conducted a successful cyberattack on Ukraine's electrical grid—a clear example of how a nation can refuse to be limited by norms they agreed to without a straightforward means of imposing cost by the international community. Nevertheless, Nye also posits that countries still have four core reasons to agree on standards to constrain behavior in cyberspace: coordination, prudence, reputational costs, and domestic pressures; establishing this behavior can take time, perhaps decades, to cement as norms.[44]

The law and policy ramifications surrounding the Tanker War compare how warfare improved norms in the maritime domain and how cyberspace norms could similarly be enhanced. There are several lessons about the global social process and international norms. When reviewing the effects of the Tanker War on law and policy, George Walker describes that civic order claims in international law significantly impact public order norms and claims.[45] For instance, the Tanker War caused widespread oil price hikes and supply chain shortages, forcing the international community to side with civic order claims that would ultimately restore the public order norms.[46] In cyberspace, widespread attacks and malfeasance by threat actors, both state and nonstate, affect the international marketplace. In the future, such attacks may force a preference for claims favoring public order norms and establishing transnational cyberspace law, along with governing bodies to administer it.

In the case of the Tanker War, the United Nations, specifically the Security Council, was instrumental in serving as the international body for adjudicat-

ing disputes and, ultimately, bringing about an end to the conflict through mediation and resolution of international peacekeeping once it was made clear that the public order was threatened.[47] International norms are not a perfect or immediate solution, and the Tanker War is one such example: the conflict continued for eight years, intensifying in 1988 before finally reaching a cease-fire by Iran and Iraq accepting UN Resolution 598, a resolution that took years of negotiation while the destruction and bloodshed in the Arabian Gulf continued.[48]

What can be learned about establishing public order norms in cyberspace from a maritime conflict like the Tanker War? Several themes contributed to a final resolution:

- International *commitment* to a governing body and, through the UN Charter, a consensus that resolutions by that body are binding for member states,
- International *resolve* to continue using the UN as a vehicle to seek diplomatic resolution, and
- International *pressure*, through military, economic, and diplomatic channels, to end the belligerents' behavior for the good of the public order and deter future aggression.

A disruptive conflict in cyberspace, with threat actors causing widespread and internationally felt effects, has no established diplomatic channel like the UN Security Council with binding powers to impose costs on belligerents. Walker notes that the United Nations resolutions affirming freedom of navigation in the Arabian Gulf and surrounding regions played a significant role in the Tanker War. The Gulf Cooperation Council emerged as a critical diplomatic pressure point by the end of the conflict.[49] It seems clear that, if viewed from a historical maritime perspective, cyberspace norms can enjoy some measure of success as a deterrent and that the UN can and should be the body to establish those norms and enforce them.

While international cybersecurity norms are taking shape at the United Nations, individual states must still protect their interests by shaping those norms. The United States, for its part, has a strategic imperative to be a key player in the formation of cyberspace norms, similar to how it was instrumental in hosting the international maritime conference in 1889. The U.S. Cyberspace Solarium Commission's (CSC) final report, released in 2020, describes shaping cyberspace norms and behavior as a central strategic pillar, going so far as to say that standards will not take shape without America's help.[50] Such a statement may serve as a call to action for American policy makers, particularly as the United States and like-minded democracies prefer a free and open internet for communication and commerce. Still, adversarial nations will undoubtedly see it as a U.S. attempt to take control of international rulemaking. It could set back negotiations in bodies like the United Nations.

The CSC recommendation to establish a Bureau of Cyberspace Security and Emerging Technology, at the assistant secretary level, within the U.S. De-

partment of State to engage in international diplomacy about cyberspace norms and behavior shaping could perhaps be the most impactful recommendation to further international cyberspace norms.[51] Policy makers with cyber policy and law expertise must engage in higher-level, informed discussions. Looking back to that first international maritime conference in 1889, the president of that conference was Navy rear admiral Samuel Rhoads Franklin—clearly a subject matter expert in maritime security, seamanship, and navigation by title and profession.[52]

Establishing international cybersecurity norms is just one arrow in a quiver of solutions to deal with cyber conflict below the level of what might be considered traditional warfare. While piracy on the high seas was severely curtailed at several historical points, it was never fully extinguished. Shipping organizations must still protect themselves by enacting antipiracy security measures for ships underway in dangerous areas. So too must cyberspace-connected information systems enable a solid cybersecurity program with the right people, processes, and technology.

Increasing cyber resiliency and cybersecurity of critical infrastructure—for example, maritime navigation and port control systems—is a means to reduce the risk of system failure, impose costs on cyberattackers, and support international cyberspace norms by removing easy targets from potential attackers. Regulatory compliance with verification processes such as audits is essential to ensuring standards are met, and these resiliency measures can realistically reinforce norms to deter aggressors.[53] Agencies such as the Coast Guard are vital to ensuring that these critical systems maintain cybersecurity standards.[54] They require clear policies to take enforcement actions if deficiencies are found.[55] An intergovernmental feedback channel that can reaffirm protective and resiliency measures can serve as part of "layered cyber deterrence" and reinforces international cybersecurity norms, particularly for critical international systems such as commerce and finance, of which the maritime domain fits centrally.[56]

As a component of infrastructure under threat from cyberattacks, the use case of cyber-connected maritime systems helps illustrate the need for international cybersecurity norms when viewed from maritime safety of navigation and reinforcement of naval examples. These international standards and practices reinforce good behavior while deterring negative behavior that can cause disastrous effects. Just as the International Convention for the Safety of Life at Sea provides norms and standards for designs like the pilothouse and navigation systems, so, too, must an international standard exist for cyberspace to prevent a threat actor from usurping those systems and causing conditions detrimental to maritime operations and safe navigation.[57]

Conclusions

There are clear parallels between international norms and standards established in the maritime domain that can be likewise applied to cyberspace. Just as the sea serves as a transportation and commerce medium, cyberspace functions as

the twenty-first century "digital sea" for information transportation, thought-sharing, and high-speed commerce that cross national borders in ways never before. Cyberspace knows no absolute sovereignty (although several nations would prefer otherwise), and the netizens of the internet are genuinely an international collective engaged in a global community. Threats in the maritime domain, such as piracy, have loose approximations in cyberspace with ransomware and profit-seeking cyber gangs, just as nation-states hold increasing national interests and develop digital weapons of war.

It is necessary to understand the limitations of this article and the literature reviewed herein. Much of the existing works serve as literature reviews or commentary (expert or otherwise) that seeks to inform or persuade, including this article. The work of Shackelford and Kastelic, published nearly a decade ago, perhaps provides the most comprehensive analysis of national cybersecurity strategies with an eye toward international law and norms development in current searchable literature. Policy makers and informed audiences alike would be well served with up-to-date academic scholarship on this topic, examining trends in strategy development, international agreements, multilateral treaty negotiations, and policy diffusion. Additionally, public-private partnerships and nongovernment organizations should continue to publicly publish thought leadership on the subject outside of paywall limitations that can be leveraged and built on by other analysts, advisors, and scholars for the benefit of all nations seeking consensus in cyberspace norms.

There are real benefits in establishing international cybersecurity norms and standards that can reduce the risk for all cyber-connected systems and organizations. While the United Nations and international think tanks have made significant progress, much more work remains to be done, particularly with attributing cyber actions and holding nations accountable for those actions and the actions of their citizens. It is hard work, but so were those first few international maritime conferences establishing the law of the sea, seeking consensus, and holding nations accountable.

The United States will undoubtedly continue to be viewed as the standard-bearer in establishing international cyberspace norms, but it will take the entire international community to ensure success. Time is needed to grow and refine models, but time is in short supply. Cyberspace moves at machine speed—the United States must continue to exert diplomatic pressure within the United Nations and other alliances, such as NATO, to accomplish the strategic recommendations of the U.S. Cyberspace Solarium Commission: promote responsible behavior in cyberspace, deny benefits of damaging exploitation, and impose costs to threat actors.[58] Establishing norms in the cyber domain, with the history of maritime norms to offer context and lessons, will benefit all nations.

Endnotes

1. Allen Parachini, "Aquatic Attraction: Poets, Pragmatists, and Scholars Ponder the Inexplicable Appeal of Being Near Water," *Los Angeles (CA) Times*, 7 April 1989, l.

2. Stephen Bates, "The Ancient History of the Internet," *American Heritage* 46, no. 6 (October 1995): 34.
3. "Daily Estimated Size of the World Wide Web," WorldWideWebSize.com, accessed 3 November 2021.
4. Slavomír Gálik and Sabína Tolnaiová, "Cyberspace as a New Existential Dimension of Man," in *Cyberspace*, ed. Evon Abu-Taieh, Abdelkrim Mouatasim, and Issam Hadid (London: IntechOpen, 2019), https://doi.org/10.5772/intechopen.88156.
5. "Netizen," Merriam-Webster, accessed 27 July 2022.
6. Gálik and Tolnaiová, "Cyberspace as a New Existential Dimension of Man," 6.
7. "Maritime Security," International Maritime Organization (IMO), accessed 27 July 2022.
8. George K. Walker, *The Tanker War, 1980–88: Law and Policy*, International Law Studies (Newport, RI: U.S. Naval War College, 2000).
9. Security Council Resolution 598: Iraq-Islamic Republic of Iran, United Nations Peacemaker.
10. Walker, *The Tanker War, 1980–88*, 74
11. "IMB: Piracy and Armed Robbery at 27 Year Low in 2021," *Maritime Executive*, 12 July 2021.
12. Silvia Ciotti Galletti. *Piracy and Maritime Terrorism: Logistics, Strategies, Scenarios* (Amsterdam, The Netherlands: IOS Press, 2012).
13. Galletti, *Piracy and Maritime Terrorism*, 79–80; and Christian Bueger, "What Is Maritime Security?," *Marine Policy*, no. 53 (2015): 159–64, https://doi.org/10.1016/j.marpol.2014.12.005.
14. Galletti, *Piracy and Maritime Terrorism*, 79.
15. Tashreef Shareef, "9 Times Hackers Targeted Cyberattacks on Industrial Facilities," Makeuseof.com, 15 January 2022.
16. E. Erstad, R. Ostnes, and M. S. Lund, "An Operational Approach to Maritime Cyber Resilience," *TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation* 15, no. 1 (March 2021): 27–34, https://doi.org/10.12716/1001.15.01.01.
17. Olga Kiyan, "The Role of US-Russia Divergence: Establishing Cybersecurity Norms in the United Nations," *Harvard International Review* 42, no. 4 (2021): 24–27.
18. Kiyan, "The Role of US-Russia Divergence," 25.
19. Kiyan, "The Role of US-Russia Divergence," 26.
20. Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin Press, 2017).
21. Scott Shackelford and Andraz Kastelic, "Toward a State-Centric Cyber Peace: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity," *New York University Journal of Legislation and Public Policy* 18, no. 4 (2015): 895–984.
22. Shackelford and Kastelic, *The Darkening Web*, 926.
23. Shackelford and Kastelic, *The Darkening Web*, 927.
24. Shackelford and Kastelic, *The Darkening Web*, 928.
25. Kiyan, "The Role of US-Russia Divergence," 26; and Joseph S. Nye Jr., "The End of Cyber-Anarchy?," *Foreign Affairs* 101, no. 1 (January/February 2022): 7–8.
26. *Regional Consultations Series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (New York: United Nations, 2019).
27. Kiyan, "The Role of US-Russia Divergence," 27; *2015 UN GGE—Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)* (New York: United Nations, 2015); and *Regional Consultations Series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, 3.
28. Alex Grigsby. "The End of Cyber Norms," *Survival* 59, no. 6 (2017): 109–22, https://doi.org/10.1080/00396338.2017.1399730.

29. Josh Gold. "Unexpectedly, All U.N. Countries Agreed on a Cybersecurity Report. So What?," *Council on Foreign Relations* (blog), 18 March 2021.
30. E. F. Horsley, "State-Sponsored Ransomware through the Lens of Maritime Piracy," *Georgia Journal of International & Comparative Law* 47, no. 3 (2019): 669–81.
31. Horsley, "State-Sponsored Ransomware Through the Lens of Maritime Piracy," 677–81.
32. *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: U.S. Office of the Director of National Intelligence, 2022).
33. *Annual Threat Assessment of the U.S. Intelligence Community*, 8–17.
34. *Annual Threat Assessment of the U.S. Intelligence Community*, 24.
35. Horsley, "State-Sponsored Ransomware through the Lens of Maritime Piracy."
36. Gálik and Tolnaiová, "Cyberspace as a New Existential Dimension of Man," 3–4.
37. "What Does ICANN Do?," Internet Corporation for Assigned Names and Numbers (ICANN), accessed 8 August 2022.
38. "Maritime Law," ScienceDirect.com, 9 July 2022.
39. "The U.S. Understanding of the Laws of Naval Warfare in the 18th and 19th Centuries," Naval History and Heritage Command, 10 September 2019.
40. "Brief History of IMO," International Maritime Organization, accessed 29 July 2022.
41. "Pollution Prevention," International Maritime Organization, accessed 29 July 2022.
42. "IMO and the Sustainable Development Goals," International Maritime Organization, accessed 29 July 2022.
43. Nye, "The End of Cyber-Anarchy?," 32–42.
44. Nye, "The End of Cyber-Anarchy?," 9.
45. Walker, *The Tanker War, 1980–88*.
46. Walker, *The Tanker War, 1980–88*.
47. Walker, *The Tanker War, 1980–88*, 77–78.
48. Security Council Resolution 598: Iraq-Islamic Republic of Iran; and Walker, *The Tanker War, 1980–88*, 74–76.
49. Secretariat General of the Gulf Cooperation Council; and Walker, *The Tanker War, 1980–88*, 77–78.
50. *Cyberspace Solarium Commission Final Report* (Arlington, VA: Cyberspace Solarium Commission, 2020), 3.
51. *Cyberspace Solarium Commission Final Report*, 3.
52. "Final Act of the International Marine Conference Held at Washington, October 16 to December 31, 1889," *American Journal of International Law* 5, no. 1 (1911): 42–73, https://doi.org/10.2307/2212463.
53. Lt Rachel Ault, USN, "The Coast Guard Needs Stronger Policy to Prevent Maritime Cyber-Attacks," U.S. Naval Institute *Proceedings* 148, no. 2 (2022): 27–31.
54. Ault, "The Coast Guard Needs Stronger Policy to Prevent Maritime Cyber-Attacks," 27–29.
55. Ault, "The Coast Guard Needs Stronger Policy to Prevent Maritime Cyber-Attacks," 30–71.
56. *Cyberspace Solarium Commission Final Report*, 29–30; and Shackelford and Kastelic, *The Darkening Web*, 929–30.
57. Erstad, Ostnes, and Lund, "An Operational Approach to Maritime Cyber Resilience," 29–31.
58. *Cyberspace Solarium Commission Final Report*, 1–2.