

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

MARINE CORPS UNIVERSITY
BGen Maura M. Hennigan, USMC
President

Col Paul M. Melchior, USMC
Chief of Staff

SgtMaj Aaron G. McDonald, USMC
Sergeant Major of MCU

EDITORIAL STAFF

Ms. Angela J. Anderson
Director, MCU Press

Mr. Jason Gosnell
Managing Editor/Deputy Director

Ms. Stephani L. Miller
Manuscript Editor

Mr. Christopher N. Blaker
Manuscript Editor

Dr. Michael Burns
Manuscript Editor

ADVISORY BOARD

Dr. Rebecca J. Johnson
Provost
Marine Corps University

Col Mary H. Reinwald, USMC (Ret)
Editor, *Leatherneck Magazine*

Col Christopher Woodbridge, USMC
(Ret)
Editor, *Marine Corps Gazette*

Col Jon Sachrison, USMC (Ret)
COO, MCU Foundation

SCHOOLHOUSE DIRECTORS

Colonel Greg Poland, USMC
School of Advanced Warfare

Colonel Todd P. Simmons, USMC
Expeditionary Warfare School

Colonel Brian Sharp, USMC
Marine Corps War College

Colonel Brad Tippet, USMC
Command and Staff College

Journal of Advanced Military Studies

(Print) ISSN 2770-2596

(Online) ISSN 2770-260X

DISCLAIMER

The views expressed in the articles and reviews in this journal are solely those of the authors. They do not necessarily reflect the opinions of the organizations for which they work, Marine Corps University, the U.S. Marine Corps, the Department of the Navy, or the U.S. government. When necessary, errata will be published immediately following the book reviews.

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.

FREELY AVAILABLE AT WWW.USMCU.EDU/MCUPRESS

Contents

Vol. 13, No. 2

From the Editor	7
CONFLICT ON THE SEAS	
Zumwalt, Holloway, and the Soviet Navy Threat: Leadership in a Time of Strategic, Social, and Cultural Change <i>John T. Kuehn, PhD</i>	19
Allies through Thick and Thin: U.S. Navy Strategic Communication, 1986–1994, in Transatlantic Context <i>Jon-Wyatt Matlack</i>	33
Neglected Maritime Terrain in the Bay of Bengal: An Examination of the Future of the Andaman and Nicobar Islands <i>Major Evan Phillips, USMC</i>	56
The Port-Hopping War: Littoral and Amphibious Operations in the War of the Pacific, 1879–1884 <i>Tommy Jamison, PhD</i>	79
The Maritime Silk Road: Concerns for U.S. National Security <i>Major Lindsey Madero, USA</i>	99
The Black Sea Thread in Russian Foreign Policy and How the United States Can Respond <i>Adam Christopher Nettles</i>	119
Like the Sea, So Cyberspace: A Brief Exploration of Establishing Cyberspace Norms through a Maritime Lens <i>Lieutenant Commander Travis D. Howard, USN (Ret); and Jose de Arimateia da Cruz, PhD/MPH</i>	142

The Cyber Sea: Conflict and Security 154
Major Kevin Doherty, USA

Cyberspace and Naval Power 167
Matthew J. Flynn, PhD

The Army and Sea Control: Reconsidering Maritime Strategy 182
in the Twenty-first Century
Nathan A. Jennings, PhD

REVIEW ESSAY

Reformists Posing as Revolutionaries: The Penchant 197
for the Endless Repetition of Past Mistakes
Faoud Mami, PhD

BOOK REVIEWS

Bridging the Theory-Practice Divide in International Relations 209
edited by Daniel Maliniak, Susan Peterson, Ryan Powers, and
Michael J. Tierney
Reviewed by Evren Altinkas, PhD

The Global Village Myth: Distance, War, and the Limits of Power 213
by Patrick Porter
Reviewed by Lieutenant Colonel Alexandra Gerbracht, USMC

The Command of the Air by Giulio Douhet 216
Reviewed by Master Sergeant Bonnie L. Rushing, USAF

The Other Face of Battle: America's Forgotten Wars and 218
the Experience of Combat by Wayne E. Lee, Anthony E. Carlson,
David L. Preston, and David Silbey
Reviewed by Daniel Ward

Grey Wars: A Contemporary History of U.S. Special Operations 221
by N. W. Collins
Reviewed by Christopher D. Booth, JD/MA

On Contested Shores: The Evolving Role of Amphibious 223
Operations in the History of Warfare edited by Timothy Heck
and B. A. Friedman
Reviewed by Samantha Boelter, MAH

<i>Strategy Shelved: The Collapse of Cold War Naval Strategic Planning</i> by Steven T. Wills Reviewed by Daniel Ward	225
<i>Spymaster's Prism: The Fight against Russian Aggression</i> by Jack Devine Reviewed by Sara Ferragamo	227
<i>Meeting China Halfway: How to Defuse the Emerging US-China Rivalry</i> by Lyle J. Goldstein Reviewed by Eric Shibuya, PhD	234
<i>Immortal: A Military History of Iran and Its Armed Forces</i> by Steven R. Ward Reviewed by Thomas Zacharis	235
<i>Between Desert Storm and Iraqi Freedom: U.S. Army Operations in the Middle East, 1991–2001</i> by Jourden T. Moger Reviewed by James Bowden, MA	237
<i>Shocks and Rivalries in the Middle East and North Africa</i> edited by Imad Mansour and William R. Thompson Reviewed by Satgin Hamrah, MA/MPA	238

Cyberspace and Naval Power

Matthew J. Flynn, PhD

Abstract: Seapower has come to cyberspace as a measure of the so-called greatest transfer of wealth in history given the efforts of China and other states to steal intellectual property online. But the first greatest transfer of wealth comprised Europe's rise to prominence post-1500 ACE. What historians call the "rise of the West" came to fruition with a forfeiture of the ideological promise of sharing the benefits of Western civilization worldwide. Cyberspace promises to align both threads of the new naval power, economic gain, and ideological conviction, a novel change in the history of conflict at sea all made possible by the technical marvel of cyberspace.

Keywords: greatest transfer of wealth, naval power, openness, rise of the West, cyber sovereignty, conflict at sea

One main purpose of naval power is attaining resources to drive the economic enrichment of a nation. That push naturally breeds conflict at sea among nation-states seeking the same end. The foremost success in this competition is what scholars call the "rise of the West" and refers to Europe's ability to gain prominence post-1500 ACE, as a realignment of resources went decidedly in favor of the emerging Western nation-states. A series of modest naval expeditions led to a concerted effort to gain riches abroad and bring them to Europe. Military coercion first interdicted and then redirected

Dr. Matthew J. Flynn serves as professor of war studies at Marine Corps University, Quantico, VA. He specializes in the evolution of warfare and has written on topics such as preemptive war, revolutionary war and insurgency, borders and frontiers, and militarization in the cyber domain. His publications include *Settle and Conquer: Militarism on the Frontier of North America, 1607–1890* (2016), examining American westward expansion as a successful counterinsurgency. He also coauthored a study analyzing revolution and civil liberties, titled *Washington & Napoleon: Leadership in the Age of Revolution* (2012). Books such as *First Strike: Preemptive War in Modern History and Contesting History: The Bush Counterinsurgency Legacy in Iraq* (2008) look at preemptive warfare as national policy and counterinsurgency's impact on national power, respectively.

Journal of Advanced Military Studies vol. 13, no. 2

Fall 2022

www.usmcu.edu/mcupress

<https://doi.org/10.21140/mcu.j.20221302009>

trading networks in the Americas and Asia to such an extent as to revive Europe as a power center that relied on sea lines of communication to accomplish what became the greatest transfer of wealth in history.

Today, a similar change unfolds in cyberspace, but in the other direction. The new greatest transfer of wealth arises from non-Western states acting in cyberspace to steal technology from Western states to then seek advancement on the world stage. To address this reality, those considering conflict at sea must weigh how cyberspace has assumed the mantle of naval power to feed a globalization movement driving regional inequalities. However, smoothing over difference, rather than creating imbalance, appears to be the new mandate of casting cyber power alongside naval power.

The ensuing “sea” conflict in cyberspace struggles to apply geographic dimensions when using the labels West and non-West nomenclature that makes sense only when referring to European countries and the United States as Western. That division falters today since Japan, for example, can be considered Western, not because of its geographic location but because it marries an international trade imperative with some form of democracy. A better focus dismisses geography. A more inclusive means of government contrasts with dictators imposing authoritarian rule while pursuing global trade opportunities as well. The resultant political tension inherent in this contrasting dynamic draws naval power into the cyber realm where geographic boundaries are even harder to attain or maintain than at sea.

The struggle to realign state power continues online as more open states confront governments hoping to limit access in this new space. The issue here is controlling content coupled with the urge to communicate among a population subsuming the mere desire to conduct an economic transaction. That key distinction means a cyber conflict over resources demands an ideological showdown in that domain, as was the case with the rise of the West. It is less things coming full circle than it is naval power as cyber power forcing the rise of the West paradigm to fulfill its lofty ideal of sharing resources globally in the hopes of forestalling conflict. The alternative leaves trade benefiting one region more than others and functioning as a means of imbalance on the world stage. The thesis of this article is that the ideological goal of promoting democracy with trade is a needed choice given that the extension of that ideal to cyberspace via openness can check China’s growing power.

The Greatest Transfer of Wealth

In recent times, cyber vulnerabilities have eroded state sovereignty to the point where China, in particular, has plundered intellectual capital from the United States via online theft and espionage. Critics of an open internet lament this “greatest transfer of wealth in human history.”¹ Thanks to cyberspace, global interaction now works against Western interests, making that exchange felt in a remarkably short period of time of some 40 years. Stealing Western secrets via cyber access has identified a startling shift of riches among nations that com-

menced in short order, threatening the Western advantage in global trade and perhaps imposing a position of disadvantage.

This fear of economic parity or even inferiority contained a noticeable declaration of hypocrisy given Europe's, then America's, rise to power via a similar exchange, amounting to the first greatest transfer of wealth in human history. Scholar William H. McNeill described this process as the "rise of the West." He stressed the ability of a European power center after the year 1500 to exploit the wealth of existing trading networks in the Americas and Asia during some 400 years.² Poverty-stricken Europe then remade itself into the most powerful region of the world.

While McNeill recognized some benevolence in this process, others called out Western expansion as no more than imperialism. This practice allowed a European primacy in world affairs that rested on a social system embracing universalism; only one "modern world" existed, albeit after 1500 one tilted toward European ascendancy.³ That line of analysis spurred additional research to address why an impoverished Europe rose to dominate more prosperous regions of the globe. If biological factors could help explain the European conquest in the Americas, as Alfred S. Crosby showed in *The Columbian Exchange*, and Jared Diamond stressed in *Guns, Germs, and Steel*, that development did not explain what occurred in Asia where uncontrolled illness did not decimate the population there but Europeans still came to dominate the region.⁴ Some based this outcome on internal, European factors. In *The Wealth and Poverty of Nations*, David Landes wrote that a superior work ethic explained the results and that key mentality sprung from geographic conditions; Western Europe simply enjoyed a better climate than other regions, the ensuing salubrious living facilitating a drive toward "industrial innovation."⁵ More insight in this respect led to intellectual inclusion. Europeans borrowed ideas from outside their region when they needed to, and, even if in a halting fashion, embraced the best ideas internal to Europe. Less restriction due to shedding prejudice invited an open-mindedness that meant a distinct advantage.

McNeill's book *The Rise of the West* set the parameters of this line of historical inquiry: a dominant China and Middle East giving way to a rising Europe after 1500. Those scholars focused on Asia conceded the main cause of eclipse was a lack of intellectual prowess. For this reason, Asia abdicated a leading role in world affairs, a withdrawal centered on China. For instance, China had initiated a movement in intellectual discovery before seeing Europe birth a "modern science" that eclipsed Chinese efforts.⁶ Others championed Asia as too great a region to be pushed to the side even if faltering in the face of modernity. As Eric L. Jones writes in *Growth Recurring: Economic Change in World History*, "economic growth would have been possible in any society had impediments, especially political ones, been removed."⁷ Yet, to examine circumstance, whether producing internal weakness or foolishly yielding to it, overlooked the main driver of this evolution. This was the inequality of competition turned into

conflict, although not always a clash predicated on violence and therefore not one of war.

Cyberspace captures that very framework of structure mattering more than geography—when that template is affirmed, the world becomes flat indeed. Joseph Needham called this possibility a “regionless” competition and an inevitable and needed synthesis between East and West.⁸ Such a broad action led to a universalism speaking to a unity inherent in science—a global reality surpassing earthly difference and featuring a “cultural essentialist” thinking.⁹ For Needham, openness referred to a joint venture in science that had always been humanity’s intent. That goal awaited a grand technological accomplishment—such as global connectivity.

Up to this point, human intellectual capital spelled the currency for either taking a region forward or seeing it bypassed. A stagnate or even retrograde movement stemmed from an obtuseness that generated physical realities from intellectual rigidity; a fear of global interaction followed, slowing development within a state and inviting a decline in national power. This reaction crippled the Ottoman Empire’s ability to sustain its power when religious dogma crowded out the reforms needed to counter European advances.¹⁰ Addressing barriers to exchange among diverse peoples interacting in a borderland more often than not signified the future prospects of a regional power. Those engaged beyond borders looked forward with confidence to future days; those erecting barriers expressed trepidation about the same end. Those seeking engagement, or Landes’s drive to an intellectual openness, encounter McNeill’s prophecy of a “world-wide cosmopolitanism” and a world visited by a “vastly greater stability” arising from a “Western imprint.” To see such a future meant a stilling of violence as a means of settling disputes due to a “growingly effective international bureaucracy.”¹¹

For a time, it appeared that a Western-dictated globalization had indeed subsumed the world. Western culture reached the far corners of the Earth largely on the back of the economic success of capitalism. When Europe forfeited its dominant position after the World Wars of the mid-twentieth century, it fell to the United States to deliver this outcome. The fall of the Union of Soviet Socialist Republics (USSR) heralded this achievement. With the collapse of that state, a long-standing opponent of American-defined democracy, the norm of government empowering as many people as possible moved unimpeded about the world.¹² The pushback was immediate, some decrying the new faith in democracy as no more than a capitalist-based “world war,” others denouncing the immorality of Western influence as “neoliberal” and as a means to allow the strong to dictate to the weak, thereby expanding social inequality. Consumerism also surfaced as a global norm and as a less flattering reflection of Western culture.¹³ In short, if most nations acted along Western norms of commerce, too many states had found ways to blunt the push for democracy associated with capitalism and did so with U.S. complicity, all in the name of making money.¹⁴ These critics could not stop the movement, however. If not an “end of

history,” civilization had achieved a threshold, a single system elevated to appear the banner of modernity, at the least a needed benchmark to reach in order to flourish in a new world.¹⁵

As governments willingly sought out financial advantage, humanity glimpsed a borderless world as multinational corporations pushed for monetary exchange that relegated demarcation lines to potentially ceremonial markers.¹⁶ In this process of globalization, the nation-state system took a hit as well, and international boundaries appeared to wane in the face of economic advancement.¹⁷

Content to watch a natural evolution in globalization, the United States prepared to reap the benefits of a world now shaped according to its norms. This change would be a slow process, but one clearly bowing before U.S. interests. One must appreciate the calm and almost welcoming disposition of the United States toward this development. Its vision of world affairs was coming true, and its belief in its *exceptionalism* was reaching fulfillment. Simply motivated by ideas of communion aided by governmental blessings of the effort, humanity had reached for a meeting of the minds, a shared endeavor of making prosperity and hope a global mission.

This self-actualization of the human race fit American lofty sensibilities. When the internet surfaced, this thinking gained further traction, generating a moment when technology had delivered the means of implementing globalization.¹⁸ A missed opportunity had been made good since connectivity meant something more than merely economic advancement. The new age reached past the rise of the West as cyberspace delivered a noble and rightful payoff, one benefiting all and doing so by smashing borders and doing this not by authoring a land invasion propagated by armies answering to a single state or alliance, but doing so by the sheer force of ideas. The international exchange should be one of discourse, of people reaching out to one another, of learning about each other in ways never before possible—instantaneously and without the oversight by either elected or self-appointed authorities.

Cyber Sovereignty

Borders appeared to be dead at this point since one people inhabited the Earth, not citizens of differing states, but those online or “netizens.”¹⁹ And then adversaries of globalization spreading via cyberspace declared that openness does not serve as an expression on behalf of humanity; rather, it marks the cultural threats lurking in the new domain. One must be on guard against these insidious, intellectual dangers, and attempting to mount that defense means curtailing an open internet. Championing cyber sovereignty represents a start, not so much a genuine means of curbing connectivity since logical (physical) connection remains, but more of a willingness to stop unfettered human interaction via openness that would result in so much more than seeking online access to turn a profit. One had to dominate the monetary proceeds of cyberspace and control, even stop, the social interaction that accompanies such trade. The rise

of the West mentality had come to cyberspace: profit via a bounty allowing one region to attempt to exploit another but stymie societal connection that might drive parity among competitors.

When it comes to cyberspace, territorial sovereignty enjoys an uneasy transition to the domain. A state exercises control over the physical infrastructure located on its soil providing connectivity to the internet. One expert describes this mandate as authorizing governments to “regulate activities occurring within their territories and to enforce their domestic law.”²⁰ This stand appears straightforward enough and therefore valid. A state would naturally govern online use within its borders. Yet, a government will enable information online to flow onto another country. In this light, cyberspace does not fall under one nation’s sovereignty. Rather, countries have an obligation to promote and ensure connectivity. Clearly, nations function as parts to a whole even as those parts may well answer to state sovereignty.²¹ *The Tallinn Manual on International Law Applicable to Cyber Warfare*, the West’s quintessential answer to placing cyber realities firmly on a legal footing, captures this ambiguity perfectly. “Rule 1” defines “sovereignty” as allowing a state to “exercise control over cyber infrastructure and activities within its sovereign territory,” “although no state may claim sovereignty over cyberspace *per se*.”²²

In this confusion regarding what constitutes shared cyberspace lies a growing uncertainty regarding what guarantees openness within a state. No matter a declared respect for territorial sovereignty, Western actions advancing openness transgress on the very idea of sovereignty as a means of connectivity ensuring best business practices. For the West, the *de facto* norm allows openness to function as an outgrowth of that connectivity. To states fearing openness, new international agreements must make plain the violation of a free exchange of ideas.²³ Given this divergence, territorial sovereignty has not been sufficient to make clear what must happen in cyberspace. Somehow, despite an alignment of cyber sovereignty with the concept of the nation, a clear understanding of openness has fallen outside that norm.

Those supporting cyber sovereignty base their views on the Westphalian state system of 1648. This logic flows from the assumption that agreeing to territorial borders granted Western European nations a reprieve from endless conflict. Once ending the Thirty Years’ War with this agreement, prosperity rose and helped Europe attain a dominant position in the world.²⁴ This characterization of the nation-state system overstates Western achievement. In Europe, defining borders did not always equate to a national identity. That step evolved much more slowly and perhaps arrived only with the French Revolution in 1789. Still, after 1648, Europe did take another big step forward in terms of regional identity and exerting global power, and the fact that conflict among these emerging states assumed more predictable and acceptable forms no doubt played a role in this development.

Bringing to bear some old thinking about nationalism on the new reality of cyber yields a familiar outcome, as nation-state norms become a mechanism for

authoritarian regimes to control the interface. What eventually became a key part of Western expansion—state sovereignty fostering centralized rule—now enables many nations to deny their citizens unfettered access to the internet by implementing government regulations that maintain a watchful eye over all internet traffic.²⁵ Nations attempting to erect borders in cyberspace to keep out undesirable contacts try to restrict openness as they deem appropriate.

The Reach of Naval Power

To exert naval power generated interaction as much as confrontation among nations. The same applies to cyberspace and that mixing worries countries vulnerable to that exchange. As connectivity continues to grow in cyberspace, those governments fearing openness as the free exchange of information and ideas online offer increased resistance. That opposition stems from leaders of autocratic nations worried about the cultural impact of connectivity, and, surprisingly, from many voices in democratic states responsible for protecting their networks. Altogether, cyber sovereignty becomes a means of trying to thwart openness by retaining state borders in a cyber world.

Those propagating fears of connectivity to enforce cyber sovereignty appeal to Western norms of government-imposed boundaries, law, and possession. To make state sovereignty work in the cyber age, one has to give up on the idea of one world. All people are not the same. Rather, different parts of the world enjoy different rules and norms. Cultural specificities mean a rationale for separation and maintaining an international state system featuring different nations. That goal betrays the most effective use of naval power in history: the rise of the West. The question becomes, can Western powers arrest this process in the cyber age, and to what end? Perhaps shoring up network security can stop a loss of intellectual capital. But to do so cripples the other arm attending economic expansion, a quality resting on American sensibilities. The world could be united by overcoming difference, and the United States had set out to do this from its inception. That conceit did not require all people to be American. Rather, all people clearly should be American because the pursuit of freedom knew no boundaries when considered a universal attribute.²⁶ With this reference, cyber sovereignty presented a technically savvy body politic with a visceral contradiction: technology speaking to global outreach and a movement endorsing that very connection, but also a cry from within the United States for cyber sovereignty in order to protect the American public from that very outcome.

To dispel such a gross contradiction, the emerging global interchange in cyberspace met with recrimination among U.S. state authorities as a reaction to fears of a borderless world. Fancy defined those past movements where mere cyber connectivity had helped mobilize whole populations to act against their oppressive governments. The Middle East arose as a striking example in this regard, an early success story being the Arab Spring. Then came an unspoken global repudiation of the movement. Populations had acted, to be sure, but the outgrowth had produced dislocation and destabilized the region. Dicta-

tors have weathered that movement to this point, but technology could still usher in a sea change.²⁷ The United States suffered the most regress in terms of what might come next. Americans had believed a government holding people in check stood for oppression. Now, populations in other parts of the world can agitate for freedom, but have to face an American litmus test demanding an unclear standard.

Other states noticed the hesitation and strove to recover their own sense of purpose. States like Russia and China justified cyber sovereignty as online control that quelled their society of users from thinking that fostered social largesse. In the case of China, big data offers enticement to that very end: increased business activity from better processing power coupled with an upgrade to state surveillance.²⁸ Thoughts that looked to humanity as one entity, and not many competing groups, suffered in the face of that oppression. Any aspirations of a global, American-led online world faltered as a result as governmental authorities looked to arrest this process of online interaction by enacting controls over the very means of exchange that defined openness.

Embracing control meant that all nations could point to war as the outgrowth of cyber realities. Threats dominate the platform, not promise. Fear should guide the online experience, not trust. What had been an arbitrary experience enjoined with the excitement of connecting with everyone anywhere now has to have intrusive limits and safeguards. People cannot be trusted, the technology cannot be trusted, and the world remains a warzone first and foremost. Cyber merely advances a pending doom, a means to accentuate a familiar path of conflict.²⁹

Western governments could no longer be certain of the outcome of such a struggle should unfettered online access be the norm. These power centers hoped to hold onto power by controlling private business. The idea of corporations, the monied interests in the hands of those less willing to obey state boundaries, setting governance, or merely undermining government by doing nothing to rein in the presumed chaos, appeared a real possibility in a cyber age where that sector had in fact created so much of the platform and did so to serve a humanity hungering for connectivity.³⁰ Profit followed, and nation-states allowed corporations to exist with continued financial gain so long as the corporate entity towed the line of state sovereignty in pursuit of a world resting on devices to make connections in all walks of life, and so arrives the internet of things.

So far, the idea of naval power remained intact and familiar, if one accepted cyber sovereignty. But realigning sovereignty has always been the foremost outcome of naval power gaining resources and has always fueled conflict at sea. Now, U.S. decision makers had to contend with that reality in cyberspace. The connection is that interaction at sea or across cyberspace means redefining sovereignty, or trying to keep it as it always is no matter that impossibility. Resources were certainly one aspect of this struggle, but there remained the ideological imperative accompanying such thinking. After the rise of the West,

Americans defended the best of this European expansion, a hope that enrichment of one region would cause the emulation of that success in other less fortunate regions of the globe. A shared prosperity would emerge and with that change a more peaceful accord among like-minded nations.

Today, the ability to steal ideas online meant non-Western states acted to make this very prophecy come true. But defending cyber sovereignty meant Western states opposed that attempt. While protecting and defending intellectual property made sense, the larger issue of invalidating the ideological premise Americans safeguarded in the rise of the West meant a defeat of casting the American ideal globally.

Naval power was supposed to make good this vision when in American hands. American naval power made sea lanes accessible across the world, a common access to international waters. This guarantee appeared self-serving in the extreme as those norms fueled the American trade juggernaut. Equal access benefits Americans most. But American altruism stresses a universalism in the intent; free trade could benefit everyone. The new greatest transfer of wealth disputes this optimism both in effect and purpose. First, other nations such as China trade across the globe. Second, the ideological need to share ideas as a means to economic empowerment had come to pass, but in an illegal manner according to Western observers. No matter, the obvious contradiction had been exposed: a desire for material resources justified by a promise of parity someday, but a promise that was never honored. Cyber realities had tested the ideological conviction behind Western naval power and found it wanting.

Seeing difference across the globe underscored how democratic (Western) states feared the very connectivity they did so much to foster. Cyber had not brought humanity to a point of bliss, but instead brought crisis. Technology could not save someone; it could only foment a dark reckoning. Human ingenuity could not get one past these inflexible moments. With each advance in cyberspace, humanity faced limitation, not largesse. Such doom spawned only one form of government—one purporting control. Projections of wise leaders in government doing unpleasant tasks for a greater good, albeit a localized good as per any understanding of sovereignty, encouraged obedience among state populations. States did not proctor community, only self-preservation of a lone actor. The internet served both aims, a nurturing of individualism in search of a community but also a fear of overextending one's private reach. Identifying that contradiction as misfortune meant that the outcome mattered more than the process. Those shaping the online world embraced this deliberate emphasis, a by-product of stressing cyber sovereignty. Just as 1648 marked a great abuse of power in the name of sovereignty, so too did a cyber world limited in recollection of democratic activism online.³¹ The push online to break the grip of state sovereignty became a forgotten story, and so too did the push of humanity aspiring for change by accepting a clash over thinking, less a war over territory.

Future of Naval Power as Cyber Power

The vilification of cyber as a nemesis to a universalism inherent in the medium made it easy to spurn a sharing of long-held power; rather, a sad reactionaryism took hold. This thinking reversed what the founders of American republican government expected and undermined the advent of democracy already surfacing online.³² That result means Americans face a crisis when contemplating naval power and a conflict at sea. To deny a realignment of riches as was unfolding in the cyber domain appears an obvious mandate, until the intellectual cost of that act comes to the surface. The ideological baggage of any naval presence came to roost in cyberspace like never before as the online quality of humanness reaching across the globe threatens sovereignty. Most tolerated the business end of connectivity, even encouraged it, for obvious reasons: financial gain. Too many could not condone the output behind a shared human activity of simply sharing ideas, especially not if the world must remain as it was before online realities took hold.

A final contrast remains, set by those proclaiming the virtue of cyber sovereignty. They maintain that the threats online are so great and pervasive that one cannot but conclude that severe restrictions of online use would be the logical extension of cyber sovereignty. At the very least, controls could reduce online use to mere polite conversations, all approved by the state. Moreover, public information could be approved by state authorities, and only sanctioned users could post or access such material. However, such controls would discourage use altogether, a near impossibility not due to financial loss but more due to the absurdity of returning to a life before internet use. The gains are clear from ease of access to information, from financial transactions saving time and money, from the ability to talk to more people more often for more time and at affordable cost. Those seeking retrenchment fail to consider the impossibility of setting the clock back. An appeal to a better existence in the past is easy to sell and nearly impossible to enact.

The demonization of the new continues, however. Governments promise the impossible of controlling online use and hold out the fear of not being able to do that very thing. Assurance and despair seek user obligation to cyber sovereignty. That surrender accepts a status quo that no longer exists, a status quo grossly imperfect in its outgrowth delivering strife and conflict, and a status quo that merely sought self-preservation of an old order that hardly spoke to universal functionality, the very premise of online existence. One could not hold back time, denounce the future, and seek to control the onrush of modernity, even when appealing to cyber sovereignty.

A future defying cyber sovereignty is here, for now. Clearly in the ether of cyberspace stands stateless terrain, a cognitive terrain, an area completely free of state sovereignty. That standing parallels sea power and suggests the rise of the West remains in play as an ideological imperative at long last redressing the regional inequalities that came from that development. More of a sharing of intellectual capital as a means of economic enrichment must come into play,

or the United States must give up on its push for an ideologically shared vision of trade fostering better relations in order to find similarity and accord among peoples. Cyber vulnerabilities have allowed parts of the world to catch up to the West, but that development means the West can right a long-standing ill inflicted on less powerful states that were to meet the promise of advancement someday, but something held as too far off to be actionable, until now. One need only accept this fact of openness and protect it. This feat arrived from an ability to tap a space that had awaited human discovery. Somewhere between Earth and space in the electromagnetic sphere, cyberspace lurked and delivered a universal existence speaking to the best of humanity. That truth is self-evident, best testified to in the efforts of states to redact the existence of openness followed by the state drive for cyber sovereignty to quash the society of users that functions online and produces a community that is bigger than government.

In place of that supposed utopia comes the dystopia of returning the world to what it was before cyberspace. Authoritarian states like Russia and China recoil before this medium.³³ Putin attempts to cast a narrative that abounds in cyberspace and has enjoyed some success in capturing a nostalgic Russian history embracing territorial expansion even if facing connectivity with great trepidation.³⁴ China's great fire wall stands to keep its citizens apart from online realities, all the while that nation engages in global commerce designed to foster exchange beyond its borders.³⁵ Smaller states fear the impact of these "cyber rebellions" too.³⁶ North Korea, for example, remains a reclusive state but one forced to engage in cyber ransom attacks to prop up their cash-starved edifice. Looking beyond its borders is a great imperative to enrich the nation and keeps alive the possibility of internal upheaval from public discontent stemming from web access.³⁷ Even the United States weighs concerns about online, citizen activism as radicalism at home roils its body politic. To look backward suggests a return to a unifying American identity as divorced from the world, an end tacitly admitting an inability of a democracy to weather a free exchange of information.³⁸

Again, such retrograde thinking clashes with online realities that may well be effaced or diminished as a consequence, but not before the folly of such an outcome reveals itself. That struggle, so parochial in the past, now assumes much larger parameters. Openness replaces that narrow ideological construct with a declaration of human access to ideas.³⁹ This universalism defines a frontier as it should be, the validation of the human need for discovery. To this end, those attempting to defend cyberspace as a positive strive to place cyberspace on a level defying sovereignty. This effort has yet to achieve its full measure, one that accepts globalization as a process reshaping the power structure enacted with the rise of the West.

Cyberspace has closed the gap of riches, but now comes the ideological measure. The online world means Western states must live up to the ideological conviction inherent in the rise of the West as that of sharing resources to create more like-minded peoples who then shun the propensity to turn toward war. In

turn, China will have to do the same. With this recognition comes a vision of cyberspace declaring human interchange as the prized commodity arising from trading goods. Naval power as cyber power forces the acceptance of this other arm of Western expansion, as shared material gain means ideology can at last help defend an open trading system given the altruistic motive behind online existence. This presents another opportunity to foster an exchange across the globe and on a more equitable basis given the difficulty in setting standards of sovereignty in cyberspace. In that dynamic stands a counter to Chinese hopes of expansion via online subterfuge to commandeer the intellectualism defining a so-called Western region today. To compete with the West in cyberspace, China and other authoritarian states must risk becoming like their declared adversaries, a measure of democracy as a symptom of naval power and as the new ideology driving reality in cyberspace as that domain recaptures the lost virtue of the rise of the West.

Endnotes

1. For the assertion of the “greatest transfer of wealth in human history,” see Keith B. Alexander, Janet Jaffer, and Jennifer S. Brunet, “Clear Thinking about Protecting the Nation in the Cyber Domain,” *Cyber Defense Review* 2, no. 1 (Spring 2017): 30; Chris Demchak, “Defending Democracies in a Cybered World,” *Brown Journal of World Affairs* 24, no. 1 (Fall/Winter 2017): 143; and Peter Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 95.
2. William H. McNeill, *The Rise of the West: A History of the Human Community* (London: Cambridge University Press, 1963), 565–66.
3. Immanuel Wallerstein, *The Modern World-System I: Capitalist Agriculture and the Origins of the European World-Economy in the Sixteenth Century* (1974; repr., Berkeley, CA: University of California Press, 2001), 46, 39.
4. Alfred W. Crosby, *The Columbian Exchange: Biological and Cultural Consequences of 1492* (Westport, CT: Praeger, 1972, 2003), xxvi; and Jared Diamond, *Guns, Germs, and Steel: The Fates of Human Societies* (New York: W. W. Norton, 1997), 15–16.
5. David Landes, *The Wealth and Poverty of Nations: Why Some Are So Rich and Some So Poor* (New York: W. W. Norton, 1999), xviii.
6. Joseph Needham, *Science and Civilization in China*, vol. 1, *Introductory Orientations* (1954; repr., London: Cambridge University Press, 1996), 3.
7. Eric L. Jones, *Growth Recurring: Economic Change in World History* (New York: Oxford University Press, 1988), xv.
8. Joseph Needham, *Science and Civilization in China*, vol. 4, *Physics and Physical Technology*, pt. 3, *Civil Engineering and Nautics* (1971; repr., London: Cambridge University Press, 2000), xlviii.
9. Robert Finlay, “China, the West, and World History in Joseph Needham’s *Science and Civilisation in China*,” *Journal of World History* 11, no. 2 (Fall 2000): 282, <https://doi.org/10.1353/jwh.2000.0035>.
10. McNeill, *The Rise of the West*, 774. And see the author’s application of walls in cyberspace in Matthew Flynn, “A Wall in Cyberspace,” *Journal of International Affairs* (9 April 2019).
11. McNeill, *The Rise of the West*, 806.
12. Samuel P. Huntington, *The Third Wave: Democratization in the Late Twentieth Century* (Norman: University of Oklahoma Press, 1991), 58, 316. See also the collection of essays in a book recognizing democracy as in the ascendancy but asking if it can be sus-

- tained. *The Global Resurgence of Democracy*, ed. Larry Diamond and Marc F. Plattner (Baltimore, MD: Johns Hopkins University Press, 1996), x.
13. For globalization as a “world war,” see William I. Robinson, “Globalization: Nine Theses on our Epoch,” *Race and Class* 38, no. 2 (1996): 13. For globalization as Western or “neoliberal” and as failing to “redress” “inequalities,” see Stephen Gill, “Globalization, Market Civilization, and Disciplinary Neoliberalism,” *Millennium* 24, no. 3 (Winter 1995): 400, 422–23. For consumerism as vice, see David C. Korten, *When Corporations Rule the World* (Bloomfield, CT: Kumarian Press, 2001), 2; and Stephen Gill, “Globalization, Democratization, and the Politics of Indifference,” in *Globalization: Critical Reflections*, ed. James H. Mittelman (Boulder, CO: Lynne Rienner, 1996), 205–6. Historian Emily Rosenberg questioned this relationship as early as 1983. See Rosenberg, *Spreading the American Dream: American Economic and Cultural Expansion, 1890–1945* (New York: Hill and Wang, 1982).
 14. For globalization as a “universalization” of cultural forms merely advancing Anglo-American dominance, see *Globalization, Democratization, and Multilateralism*, ed. Stephen Gill (New York: St. Martin’s Press, 1997), 5. William I. Robinson casts doubt on the American wish for “democracy promotion”; rather, the nation favors “intervention in national democratization movements” to “shape their outcomes in such a way as to preempt more radical political change,” hence the consolidation of “polyarchic political systems” that favor the economic interests of Western powers. See Robinson, *Promoting Polyarchy: Globalization, US Intervention, and Hegemony* (Cambridge, UK: Cambridge University Press, 1996), 318–19.
 15. Francis Fukuyama, *The End of History and the Last Man* (New York: Avon Books, 1992), xi–xii.
 16. See globalization as “supraterritoriality” in Jan Aart Scholte, *Globalization: A Critical Introduction* (New York: St. Martin’s Press, 2000), 50. Kenichi Ohmae argues that government needs to get out of the way of consumers demanding and dictating the flow of goods to multinational companies so that the customers are creating a “borderless economy,” not suffering at the hands of an abusive business elite. See Ohmae, *The Borderless World: Power and Strategy in the Interlinked Economy* (New York: HarperCollins, 1990), x.
 17. More recently, one has to consider the cryptocurrency Bitcoin and its challenge to accepted banking practices. See Saifedean Ammous, *The Bitcoin Standard: The Decentralized Alternative to Central Banking* (Hoboken, NJ: Wiley, 2021), xv–xvi. Its use may speed a collapse of state borders.
 18. Howard Frederick, “Computer Networks and the Emergence of Global Civil Society,” in *Global Networks: Computers and International Communication*, ed. Linda M. Harasim (Cambridge, MA: MIT Press, 1993), 294, <https://doi.org/10.7551/mitpress/3304.003.0021>; and Walter B. Wriston, *The Twilight of Sovereignty: How the Information Revolution Is Transforming Our World* (New York: Charles Scribner’s Sons, 1992), 170–71.
 19. Michael Hauben, *Netizens: On the History and Impact of Usenet and the Internet* (Los Alamitos, CA: IEEE Computer Society Press, 1997), preface, 176–78.
 20. Wolff Heintschel von Heinegg, “Territorial Sovereignty and Neutrality in Cyberspace,” *International Law Studies* 89, no. 123 (2013): 140. Von Heinegg also stresses that there is little accord in defining what is critical infrastructure within a nation.
 21. Michael Chertoff, “The Strategic Significance of the Internet Commons,” *Strategic Studies Quarterly* (Summer 2014): 12–13.
 22. *The Tallinn Manual on International Law Applicable to Cyber Warfare*, ed. Michael N. Schmitt (Cambridge, UK: Cambridge University Press, 2013), 25, <https://doi.org/10.1017/CBO9781139169288>. Emphasis in original.
 23. Keir Giles with Andrew Monaghan, *Legality in Cyberspace: An Adversary View*, Letort Papers (Carlisle, PA: Strategic Studies Institute, U.S. Army War College Press, 2014), 15–16.
 24. Chris C. Demchak and Peter Dembrowski argue that the nation-state system helped lessen the impact of war and now that system must be duplicated in cyberspace. They

- write, "The ability of the state to provide stability and security within the increasingly unchallenged borders was necessary to internal development of social and economic progress." See Demchak and Dembrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* (Spring 2011): 35, 37.
25. Matthew J. Flynn, "Civilians 'Defending Forward' in Cyberspace: Aligning Cyber Strategy and Cyber Operations," *Cyber Defense Review* (Winter 2020): 30.
26. Matthew J. Flynn, "The Internet Federalist Papers," *Georgetown Journal of International Affairs* (11 November 2020).
27. John L. Esposito, Tamara Sonn, and John O. Voll, *Islam and Democracy after the Arab Spring* (New York: Oxford University Press, 2015), 4; Marina Ottaway, *A Tale of Four Worlds: The Arab Region after the Uprisings* (New York: Oxford University Press, 2019), 5; and Noah Feldman, *The Arab Winter: A Tragedy* (Princeton, NJ: Princeton University Press, 2020), xxiv.
28. Jinghan Zeng, "China's Date with Big Data: Will It Strengthen or Threaten Authoritarian Rule?," *International Affairs* 92, no. 6 (November 2016): 1443, <https://doi.org/10.1111/1468-2346.12750>; and Flynn, "Civilians 'Defending Forward' in Cyberspace," 32.
29. Brian M. Mazanec, "Military Matters: Constraining Norms of Cyberwarfare Unlikely," *Georgetown Journal of International Affairs* 17, no. 3 (Fall/Winter 206): 100; and to get past cyber security as a military reality, Myrian Dunn Cavelt, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review*, no. 15 (2013): 119, <https://doi.org/10.1111/misr.12023>.
30. Louise Marie Hurel and Luisa Cruz Lobato, "Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs," *Journal of Cyber Policy* 3, no. 1 (2018): 63, 73, <https://doi.org/10.1080/23738871.2018.1467942>; Laura DeNardis and Mark Raymond, "The Internet of Things as a Global Policy Frontier," *UC Davis Law Review* 51, no. 2 (2017); and Mark Raymond and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory* 7, no. 3 (2015): 610, <https://doi.org/10.1017/S1752971915000081>.
31. Vint Cerf, Patrick Ryan, and Max Senges, "Internet Governance Is Our Shared Responsibility," *IIS: A Journal of Law and Policy for the Information Society* 10, no. 1 (2014): 32; and Ronald J. Deibert and Masashi Crete-Nishihata, "Global Governance and the Spread of Cyberspace Controls," *Global Governance*, no. 18 (2012): 340.
32. Ebert Hannes and Tim Maurer, "Contested Cyberspace and Rising Powers," *Third World Quarterly* 34, no. 6 (2013): 1057–58, <https://doi.org/10.1080/01436597.2013.802502>.
33. Daniëlle Flonk, "Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control," *International Affairs* 97, no. 6 (2021): 1,926, <https://doi.org/10.1093/ia/iiab146>.
34. Tracey German, "Harnessing Protest Potential: Russian Strategic Culture and the Colored Revolutions," *Contemporary Security Policy* 41, no. 4 (2020): 543, <https://doi.org/10.1080/13523260.2020.1757251>; Julien Nocetti, "Contest and Conquest: Russia and Global Internet Governance," *International Affairs* 91, no. 1 (2015): 112, <https://doi.org/10.1111/1468-2346.12189>; Lincoln Pigman, "Russia's Vision of Cyberspace: A Danger to Regime Security, Public Safety, and Societal Norms and Cohesion," *Journal of Cyber Policy* 4, no. 1 (2019): 23, <https://doi.org/10.1080/23738871.2018.1546884>; and Matthew J. Flynn, "Strategic Cyber: Responding to Russian Online Information Warfare," *Cyber Defense Review*, special issue (2019): 193.
35. Ying Miao, "Managing Digital Contention in China," *Journal of Cyber Policy* 5, no. 2 (2020): 219–20, <https://doi.org/10.1080/23738871.2020.1748079>; and Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State," *Journal of Democracy* 30, no. 1 (2019): 54.
36. Matthew J. Flynn, "Cyber Rebellions: The Online Struggle for Openness," *Journal of International Affairs* (21 September 2018): 108.
37. Victor D. Cha and Nicholas D. Anderson, "A North Korean Spring?," *Washington Quar-*

- terly 35, no. 1 (Winter 2012): 8, <https://doi.org/10.1080/0163660X.2012.641728>; and Jieun Beck, "The Opening of the North Korean Mind," *Foreign Affairs* 96, no. 1 (January/February 2017): 106.
38. Matthew J. Flynn, "The Cyber Errand into the Wilderness: The 'Defending Forward' Inflection Point," *Georgetown Journal of International Affairs* 21, no. 1 (Fall 2020): 71.
39. See John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, accessed 15 December 2020. For the retreat from this sentiment to a post-liberal cyberspace, see André Barrinha and Thomas Renard, "Power and Diplomacy in the Post-Liberal Cyberspace," *International Affairs* 96, no. 3 (2020): 749, <https://doi.org/10.1093/ia/iiz274>.