Military Cyber Affairs
The Journal of the Military Cyber Professionals Association
ISSN: 2378-0789

Volume 3 | Issue 1 Article 5

2018

From Global Commons to Territorial Seas: A Naval Analogy for the Nationalization of Cyberspace

Sam J. Tangredi
U.S. Naval War College, sam.tangredi@usnwc.edu

From Global Commons to Territorial Seas: A Naval Analogy for the Nationalization of Cyberspace[1]

Sam J. Tangredi[2]

Abstract: As one of the engines of modern globalization, the internet is perceived as having broken down barriers between cultures, ideologies and societies, and created a "democratization of technology." An analogy generated by this perception is that cyberspace is a "global common" similar to the oceanic "high seas" to which individuals and nations can (or at least should) maintain equal and unfettered access. Not only is this analogy incorrect, its usage makes it is hard for political decision-makers to grasp the enormity of the threat to American infrastructure, global trade, and current prosperity posed by our cyber vulnerabilities. The reality is that authoritarian governments—with the Chinese Communist Party (CCP) in the lead—have transformed the cyber "global common" into "territorial seas" in which others pass unmolested only at their sufferance, and to which access can be denied. Unfortunately, once an analogy takes hold in the popular or academic minds, it becomes the central core of explanation and defies most logical counter-arguments. The analogy of cyberspace as a global common must be killed and replaced if decision-makers are to comprehend the future of the medium, which is not a return to unfettered global access. We must clearly admit that cyber activity sails on a mosaic of adjoining territorial seas, not a vast, open ocean. Cyberspace is a nationalizing and militarizing environment of coast guards and forward outposts. This different analogy will assist in creating a mind-set that helps insure that Western democratic infrastructure does not go down with the digital ship.

[1] Please cite as: Tangredi, Sam J., "From Global Commons to Territorial Sea: A Naval Analogy for the Nationalization of Cyberspace," in Demchak, Chris C. and Benjamin Schechter, eds. *Military Cyber Affairs: Cyber, Economics, and National Security* 3, no. 1 (2018).

[2] Director, Institute for Future Warfare Studies, U.S. Naval War College

It is hard for political decision-makers to grasp the enormity of the threat to American infrastructure, global trade, and current prosperity posed by our cyber vulnerabilities. Expedient businesses spend but the minimum for (apparent) protection—thereby maximizing profit and betting that the government will eventually provide security.[3] Influenced by false analogies generated by the troubadours of globalization (i.e., Thomas L. Friedman), intellectuals perceive cyberspace to be a "global commons" to which individuals and nations can (or at least should) maintain equal and unfettered access.[4]

As one of the engines of modern globalization, the internet is perceived as having broken down barriers between cultures, ideologies and societies, and created a "democratization of technology."[5] That might have been true during the unipolar moment.

Currently, authoritarian governments—with the Chinese Communist Party (CCP) in the lead--are transforming the cyber "global commons" into "territorial seas" in which others pass unmolested only at their sufferance, and to which access can be denied. ("Territorial seas" is a rough maritime equivalent to Chris Demchak & Peter Dombrowski's construct of a "Cybered Westphalia," but with several unique differences.[6]) Western governments—and, in particular, militaries--are taking actions to reduce vulnerabilities and protections, but the reality is that decision-makers and intellectuals are recognizing this transformation from "global commons" to "territorial seas" too slowly to protect Western nations from major economic crises.

[3] Albeit, it is true that internet firewall and computer protection companies are profitable businesses, particularly those supporting financial institutions. Many corporations have in-house cyber security. However, much of this protection consists of a tail chase of hacking and patching, and talent pool that provides the protection also conducts the hacking. Most corporate protection cannot withstand a foreign government cybered attack, which on a cost-benefit basis is used to justify limiting the amount of capital spent on cyber security. I thank an anonymous reviewer for bringing up this point.

[4] Thomas L. Friedman, *The Lexus and the Olive Tree*, rev. ed. (New York: Farrar, Straus & Giroux, 2000), xvii-xxi.

[5] Ibid, pp. 59-71. For maximum hype on the elimination of national barriers see John Perry Barlow, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation, Feb. 8, 1996, https://www.eff.org/cyberspace-independence.

[6] Chris C. Demchak and Peter Dombrowski, "The Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly*, Spring 2011, 32-61, http://dtic.mil/dtic/tr/fulltext/u2/a537560.pdf.

Learning by Analogy

Social scientists argue that humans learn best by analogy. Several scholars maintain that "analogy is at the center of cognition."[7] It is by the comparison of a previous unknown with a known that we can grasp a new and complex concept.

However, once an analogy takes hold in the popular or academic minds, it becomes the central core of explanation and defies most logical counter-arguments. Repeated in the popular or academic press, it literally takes on a life of its own as an established (and comfortable) "known." Simply reasoning against its premises often has limited effect. Logic without a persuasive visual image rarely unseats even a shaky analogy. Only another analogy can kill an established analogy.

The analogy of cyberspace as "global commons" was never particularly accurate and deserves to be abandoned. It was based on an idealistic view of the relationship between technology and human nature. It interferes with an accurate understanding of the ongoing nationalization of cyberspace, particularly by the political decision-makers responsible for the protection of cybered infrastructure. It leads them to perceive that cyber threats are transient phenomena that can be legislated or negotiated away in a cooperative world.

This perception is not confined to academic communities or the most optimistic.[8] The U.S. *National Defense Strategy* (NDS) signed by Secretary of Defense Donald Rumsfeld in 2005 clearly describes cyberspace as a global commons.[9] U.S. *National Security Strategies*, along with subsequent NDSs, have maintained this assumption with slight changes in wording. *The National Security Strategy of the United States of America of December 2017*—signed by a President widely

---

[7] In particular, Douglas R. Hofstadter, "Analogy as the Core of Cognition," in Dedre Gentner, Keith J. Holyoak and Boiche N. Kokinov, eds., *The Analogical Mind: Perspectives from Cognitive Science* (Cambridge, MA: MIT Press/Bradford Press, 2001), 499-538.

[8] A major academic project that used analogies to explain possible cybered warfare threat scenarios is the Naval Postgraduate's "Cyber Analogies" project created by Emily Goldman and John Arquilla. Their primary report is Emily Goldman and John Arquilla, eds., Cyber Analogies (Technical Report NPS-DA-14-001), February 28, 2014, https://calhoun.nps.edu/bitstream/handle/10945/40037/NPS-DA-14-001.pdf. However, Goldman and Arquilla's use of analogies is different than that or the current article. The analogies are intended to relate specific cyber issues to other events in history, rather than create an analogy for cyberspace itself. As the editors describe: "Cyber issues are inherently tough to explain in layman's terms. The future is always open and undetermined, and the numbers of actors and the complexity of their relations are too great to give definitive guidance about future developments. In this report, historical analogies, carefully developed and properly applied, help indicate a direction for action by reducing complexity and making the future at least cognately manageable."

[9] Donald H. Rumsfeld, U.S. Secretary of Defense, *The National Defense Strategy of the United States of America*, March 2005, 13, http://history.defense.gov/Portals/70/Documents/nds/2005_NDS.pdf?ver=2014-06-25-124535-143.

seen as critical of internationalism—refers to cyberspace as a "commons domain" belonging "within the framework of international law."[10]

The opposing reality is that not only is this "global commons" co-inhabited by cyber-criminals, hate and terrorist groups and malignant operators, but authoritarian governments in some of the largest countries don't view cyberspace as a "global commons" (free from national control) at all. Since cyberspace is not a physical dimension (outside of computers, cables and routers), it is hard to describe it in terms of clearly marked and absolutely controlled territory. However, there is an appropriate analogy drawn from maritime realm and naval strategy. Rather than a "global commons," cyberspace functions as a mosaic of adjoining, and sometimes overlapping "territorial seas."

Global Commons versus Territorial Seas

The global commons are the spaces and dimensions on (and above) the earth which are the territory of no one nation, but can be used by all in accordance with international law and political custom. Global commons are usually defined in a legal sense. The origins of the concept lay in both the writings of Hugo Grotius (in terms of "freedom of the seas") and in English custom and law (in terms of commons pastures located near villages). However, global commons can be functionally defined as mediums humans use for communications, transportation and commercial and information exchange, but cannot normally inhabit.[11]

On earth, the geographically largest and most physically accessible global commons are the oceans, which include the air above it, as well as most (but not all) of the seabed below it. Air space is a commons only above the oceans, which is why it is considered a part of the maritime commons. Over land, air space is territorial. Outer space is also a global commons, but is not as physically accessible. Obviously not physically accessible with predigital means, cyberspace has nevertheless been repeatedly conceptualized as a global commons and, if it were true, it would be

[10] President Donald J. Trump, *National Security Strategy of the United States*, December 2017, 41, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[11] For a more detailed explanation of the logic behind this definition, and how it relates to navies, see Sam J. Tangredi, "Beyond the Sea and Jointness," in Thomas J. Cutler, ed., *The U.S. Naval Institute on Naval Strategy* (Annapolis, MD: Naval Institute Press, 2015), 141-150.

the commons most utilized by individuals, albeit for information exchange rather than physical transfer of trade or discovery.

Following the long established concept of the "freedom of the (high) seas," global commons are presumed to be immune from boundaries and national jurisdictions. Importantly, the security and efficiency of international trade are dependent on unfettered access to global commons. In other words, the commons are essential for global free market economics. Yet, "freedom of the seas" (as with all international law) has been periodically challenged. Nations have had to fight to ensure their access to maritime trade; others have fought to deny such access to those they perceive to be enemies.

In contrast to global commons, territorial seas are ocean waters--extending to 12 miles off a coastline--in which the adjourning coastal state can legally apply certain sovereign rights.[12] There is also an additional 12-mile "contiguous zone" which functions similarly. However, there are nuances as to how sovereign rights may be applied. Unlike in internal waters, such as exclusive rivers and lakes, where a nation's sovereignty is absolute (similar to the airspace above national territory), international law provides for "innocent passage" through territorial seas, also called transit passage. Under innocent passage, vessels or aircraft of another state can pass as long as they do not (relatively) deviate from the most expeditious course transiting from the high seas across the territorial seas to regain the high seas. Nevertheless, the coastal state can effectively block access by determining that passage may not be innocent—for example, to search for illegal drugs, illegal fishing, other criminal activities, and sanctioned weapons (WMD), etc. Warships are generally not stopped lest the action causes war, but merchant traffic is halted with some frequency.

These nuances make it more appropriate to apply the territorial sea analogy to cyberspace access – particularly concerning use of the internet – than the global commons concept. It is difficult for nations participating in the global economy to block all "innocent cyber passage" (or

[12] A useful diagram of the separation between territorial seas, contiguous zone, exclusive economic zone, and high seas can be found on the New Zealand Environmental Organization's website: http://www.environmentguide.org.nz/issues/marine/marine-management/areas/. Originally, territorial seas were considered 3-miles in width (supposedly the maximum range of cannon fire in the 1700s), but were extended to 12-miles (the range of 5 inch coastal battery gun in the 1900s) under customary international law, and were codified as such under the UN Law of the Sea convention.

reception) without considerable costs. But it can block internet access on those subjects and functions that it chooses.

This is where the analogy of cyberspace as a territorial sea differs from Demchak and Dombrowski's "cybered Westphalia" analogy. While the allusion to the Westphalian construct has validity as concerns legal sovereignty, the practical situation is that it may be too costly for some authoritarian states to try to block or intercept all traffic—particularly if indirectly (or directly) benefits the internal economy or fosters personal relations. As in an example drawn from Thomas Friedman, Friedman's mother plays on-line bridge with players located in Siberia.[13] It may not behoove the Russian government to interfere with online bridge, but, instead, might expediently consider it "innocent passage" from one foreign mind to a citizen and back to the foreign mind. Yet, as if in a territorial sea, the Russian government can functionally choose to block any internet traffic that it deems objectionable, such as news or opinion unfavorable to its authoritarian government.

Expanding Territorial Seas and Shrinking the Global Commons

Another rationale for the territorial seas analogy has been generated by a growing effort by authoritarian states to shrink the access of others to the global commons. This parallels the efforts to take sovereign control over cyberspace and internet access.

Today a number of coastal states, most with authoritarian governments, attempt to claim sovereignty over segments of the maritime commons despite its specified codification under the United Nations Convention on the Law of the Sea (effective 16 November 1994). The most outstanding example is the People's Republic of China (PRC), which—despite being a signatory to the Law of the Sea--claims almost the entirety of the South China Sea, which is also bordered by Taiwan, Vietnam, the Philippines, Indonesia, Brunei and Singapore. The claim is based on an assertion of "historical rights," which are themselves based on a largely spurious history.[14] To put it in the perspective of distance, the PRC claims sovereignty over South China Sea islets that are

[13] Friedman, xvii-xix.

[14] Bill Hayton, "The Modern Origin's of China's South China Sea Claims: Maps, Misunderstandings, and the Maritime Geobody," *Modern China*, May 4, 2018; "China's Claim to the Spratly Islands is Just a Mistake," *Center for International Maritime Security*, www.cimsec.org, May 16, 2018.

over 800 nautical miles from its own internationally recognized coastline, but within 250 nautical miles from that of Vietnam.

If the "historical claim" justification was applied to cyberspace as the Chinese government argues, then – ironically – the global internet would clearly be under the legal sovereignty of the United States as initial creator.

Additionally, many states perceive the transit of warships to be other-than-innocent passage by definition and attempt to restrict military traffic. This is a primary claim of the PRC; however, several other nations hold similar perceptions although few have ever attempted to interfere with such transit. In some cases, unique face-saving procedures were adopted. For many years, Indonesia claimed that warships transiting the Lombok Strait (a recognized international strait) required their permission. In an almost humorous solution, the United States would announce as a courtesy to the Indonesian government and to ensure navigational safety, but without seeking permission, that its warships intended to transit the strait. The Indonesia inevitable gave its "permission," since it chose to interpret these announcements as a request.

As previously noted, a number of states, most with authoritarian governments, have effectively declared sovereignty over their 'own' segments of cyberspace by monitoring, controlling, censoring and modifying the content and routing of the internet and cybered communications across and within their borders. If one accepts for the moment that cyberspace is indeed a global commons, then the actions to control the flow of cybered communication across borders also reduces the overall "size" of the cyber commons, effectively reducing the transit rights of the users. Unfortunately, no one has come up with the equivalent of a Lombok Strait solution.

Unlike the attempts to challenge the unilateral claims reducing the maritime commons, through "freedom of navigation" operations consisting of warship transits, there seems no practical way to publicly challenge claims of sovereignty to "territorial" cyberspace. In Western nations, internet access is considered a commercial product, subject to only limited regulation, not a government-controlled function. Thus, even if Western governments were interested in becoming involved in challenges to sovereignty, there is no legal basis for them to "force" the passage of digital packets across the "internet borders" of another nation. Such might be done surreptitiously

through hacking, but surreptitious actions are not considered a means of upholding legal rights. A freedom of navigation operation is conducted overtly, often generating very public controversy.[15]

This inability to publicly claim a right to access is yet another reason to kill the analogy of cyberspace as a global commons. Instead, authoritarian states can simply patrol their territorial cyber seas with a "coast guard" of censoring and blocking devices. Commercial traffic can be allowed through if deemed truly innocent passage, but the cyber "coast guards" can determine their own interpretations of what is innocent. There is no accepted international definition, unlike under the Law of the Sea. Yet, like maritime territorial seas, smugglers (hackers) might be able to evade the controls, and the cyber commands of militaries may be able to force passage of its "warships" without triggering an overt war. Thus, cyberspace functions as territorial seas under the varying interpretations of democratic and authoritarian states. Democratic states tend to examine only a small percentage of traffic based on just cause; authoritarian states attempt to examine it all.

The Nationalization and Militarization of Cyberspace

Returning to the (dying) analogy of cyberspace as a global commons, the incentive for "militarization" as well as nationalization (using military methods) of the presumed "peaceful" global commons of cyber space (as a means for closing it off) is obviously high for those governments who seek to control access to the "territorial (cyber) sea." However, there is a further incentive.

The ability of the U.S. to utilize and—if it so chooses--to militarily control access and use of the maritime and space commons by others have been acknowledge by scholars and practitioners alike as primary sources of our global military strength.[16] Without access to the commons, the United States could not effectively deploy its joint force on a global basis. The U.S. possesses both the transport and logistics capabilities and the alliance structure to gain results from the movement of its forces through the global commons. Other nations do not, or can do so to only a limited extent.

[15] Concerning a recent example see Ben Werner, "Pentagon Pledges More Freedom of Navigation Operations in the South China Sea," *USNI News*, May 31, 2018, https://news.usni.org/2018/05/31/34016?utm.

[16] Barry Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28 (Summer 2003), 5-46.

Moreover, the massive global sea power of the United States—taking the example of the maritime commons—can effectively shut off access to the maritime commons by any other nation, if used (and concentrated) for that purpose. (The ability to do so concerning space is currently under debate.) Fully legal access to the maritime commons in peacetime by U.S. naval and military assets allows American to position its forces forward in advance of any crisis or conflict, thereby increasing its conventional deterrence capability. It is therefore in the interests of nations hostile to the United States—as a logical part of their anti-access strategies--to continuously seek a reduction in the size and scope of all the global commons through peacetime lawfare.[17]

To transform a "legal" cyber commons into a territorial sea is a step in preventing potential U.S. access to one of the sources of its greatest strength—soft power.[18] Most authoritarian states assume that American soft power buttresses and facilitates the hard power of the United States. With the digitalization of society, much of this soft (cultural) power is most easily transmitted via the internet. From the authoritarian perspective, the militarization of cyberspace is a logical component of any anti-access strategy. This involves an offensive approach that can make the coast guards of cyberspace censorship and control even more effective. Instead of merely positioning forces within one's cyber territorial seas, one could face the U.S. forward in its own territorial cyber waters through the use of military-grade hacking or intrusion. Or one can enlist ostensibly non-military proxies to conduct such activities, in the same way that the PRC's People's Liberation Army Navy uses a paid maritime militia of ostensibly-commercial and fishing vessels to routinely harass sovereign vessels of the United States and others in the South China Sea, sometimes appropriating their equipment.[19]

---

[17] The most detailed discussion of anti-access strategies and its relationship to global commons is in Sam J. Tangredi, *Anti-Access Warfare: Countering A2/AD Strategies* (Annapolis, MD: Naval Institute Press, 2013).

[18] Joseph Nye is the creator of the "soft power" concept. He has since written numerous pieces on its application in different contexts, most recently in cyberspace. See Nye Jr, J. S. (1990 (reprint 2016)). *Bound to lead: The changing nature of American power*, Basic Books.

[19] The most notable appropriation incident was PRC seizure of an ocean glider operated by USNS *Bowditch* on December 15, 2016. It was returned after several days of examination and media attention. See such reports as Dan Lamothe and Missy Ryan, "Pentagon: Chinese naval ship seized an unmanned U.S. underwater vehicle in the South China Sea," *Washington Post*, December 17, 2016, https://www.washingtonpost.com/news/checkpoint/wp/2016/12/16/defense-official-chinese-naval-ship-seized-an-unmanned-u-s-ocean-glider/; Sam LaGrone, "Updated: Chinese Seize U.S. Navy Unmanned Vehicle," *USNI News*, December 16, 2016, https://news.usni.org/2016/12/16/breaking-chinese-seize-u-s-navy-unmanned-vehicle; Sam J. Tangredi, "Tax China for Gray-Zone Infractions," *Proceedings Today*, May 2017, https://www.usni.org/magazines/proceedings/2017-05/tax-china-gray-zone-infractions.

Additionally, the PRC has constructed a series of islands on reefs and awash shallows within international waters and within the disputed Exclusive Economic Zones (EEZs) of other nations. These artificial islands—sometimes dubbed the "great wall of sand"—have runways and are armed with anti-air weapons, with indications that tunnels for additional weapons and hardened shelters for strike missiles are now being built.[20] Although a signatory of the United Nations Law of the Sea Treaty (UNCLOS), the PRC refuses to accept international court decisions concerning its possession and control of these artificial features. A piece of the maritime global commons has therefore become a de factor territorial sea. This denial of a piece of the maritime commons through militarization is a potential model for "national outposts" within the cyberspace of the global internet overall. The new territorial seas analogy once again holds.

Killing and Replacing the Analogy

The analogy of cyberspace as a global commons must indeed be killed if decision-makers are to truly comprehend the future of the medium. The future is not a return to unfettered global access—unless by a miracle the most powerful authoritarian states become democratic. As seen in the South China Sea, the efforts of the PRC to nationalize rocks in the middle of the sea and create de facto territorial waters are ongoing and difficult to counter in practical terms. As noted elsewhere, freedom of navigation operations can be publically ignored (thereby lessening their public effect) and soon only international lawyers will care.

If academics and analysts cling to the analogy—let's call it fantasy—that cyberspace is still, or should be a global commons (if it ever was), decision-makers will not recognize the reality and will not take cybered threats as seriously as they deserve. Neither will the analogy help persuade businesses to pay for safeguards to maintain innocent passage.

As a first step, the global commons analogy must be driven out of future National Defense and National Security Strategies. Perhaps the USCYBERCOM staff can take on that task as part involvement in Joint Staff reviews and the strategy guidance drafting process. We must clearly admit that cyber activity sails on a mosaic of adjoining territorial seas, not a vast, open ocean. It is a nationalizing and militarizing environment of coast guards and forward outposts. The different

[20] Asia Maritime Transparency Initiative, "A Constructive Year for Chinese Base Building," December 14, 2017, https://amti.csis.org/constructive-year-Chinese-building.

analogy will assist in creating a mind-set that helps insure that Western democratic infrastructure does not go down with the ship.