

This article is forthcoming in *Fletcher Security Review*, vol. 6, no. 1 (2019).

## **Technology and Tensions in the Global Commons**

Kristi Govella

Assistant Professor, Asian Studies Program  
University of Hawai'i at Mānoa  
kgovella@hawaii.edu

For most of history, the domains of the global commons were unclaimed, largely because the technology to access and utilize them did not exist.<sup>1</sup> In areas such as the high seas and outer space, it was impossible for states to establish and maintain sovereign control. Even as the relevant technologies developed, costliness and controls kept them initially concentrated largely in the hands of just a few major powers such as the United States and the Soviet Union. For the United States, “command of the commons” became the military foundation of its hegemony, granting it the ability to access much of the planet and to credibly threaten to deny the use of such spaces to others.<sup>2</sup> Bipolar competition between the U.S. and the Soviet Union strongly influenced developments in the maritime and outer space domains. In the case of cyberspace, a more recent addition to the traditional global commons, the U.S. was also initially dominant due to its role in pioneering associated technologies. However, over time and particularly since the end of the Cold War, continuing technological innovation and diffusion have made these domains accessible to a growing number of countries.

This technological progress was born of both cooperation and competition between states. While some states chose to develop certain technologies indigenously, many acquired knowledge and equipment from abroad. Globalization of industry has made it easier for states to obtain a variety of foreign technologies, even lowering the threshold for them to procure disruptive military capabilities. In addition, over the last two decades, American primacy has been increasingly challenged by the rise of China, which has impacted the dynamics of technological development and diffusion across multiple domains. As China has acquired the technology to become more active in the commons, it has prompted major regional powers such as Japan and India to accelerate their own technological advancement, and other mid-sized and smaller countries have also become increasingly engaged.<sup>3</sup>

The consequence of this multiplication of technologically sophisticated actors has been the erosion of American primacy in the global commons. Although the U.S. still remains the most dominant player, it is faced with a more densely populated field, and management of these spaces has become more difficult. This article examines this trend in the high seas, outer space, and cyberspace since the end of the Cold War, with attention to the ways in which the rise of China and the relative decline of the United States have catalyzed greater engagement with the commons, particularly among the countries in Asia that find themselves most affected by this power transition. I argue that advances in and diffusion of technology have transformed the global commons into increasingly crowded domains characterized by interstate competition and

heightened tensions. Whether these tensions prevail depends on the creation and strengthening of regimes to manage interactions and promote shared rules and norms.

## **The High Seas**

On the high seas, American preeminence has been challenged by an increasing number of countries that are pursuing the technology to equip maritime forces capable of sustained operation across the deep waters of the ocean.<sup>4</sup> Much attention has focused on the technological advances made by China as a rising power seeking to modernize its naval forces. Since the 1990s, China's navy has rapidly expanded to over 300 ships, and it has also heavily invested in submarines, with roughly 80 in total today.<sup>5</sup> It put to sea its second aircraft carrier, its first domestically-built, in April 2018. In addition, reports indicate that the Chinese navy is currently working toward "technological breakthroughs in nuclear-powered aircraft carriers, new nuclear-powered submarines, quieter conventionally powered submarines, underwater artificial intelligence-based combat systems and integrated networked communications systems...in line with the service's aim of becoming a networked, blue water navy by 2025."<sup>6</sup> Although China still lacks the ability to project naval power on a global scale, it has strategically focused its efforts on developing the ability to challenge the U.S. in key places such as the Taiwan Strait and the South China Sea, particularly in pursuing anti-access capabilities such as radar, satellites, and missiles intended to neutralize some of the advantage possessed by powerful American aircraft carrier strike groups.<sup>7</sup> For example, high-speed ballistic missiles such as the DF-26, known as "carrier killers," are designed to strike moving ships as far away as Guam, and the YJ-12B anti-ship cruise missile that China has deployed in the South China Sea can reach the waters between Vietnam and the Philippines.<sup>8</sup>

Other countries in the region have made similar upgrades to their naval technology, prompted by increased Chinese activity as well as by their own domestic concerns, and as a result, it is increasingly the case that major regional players in Asia have the ability to dominate their immediate neighborhoods.<sup>9</sup> Large-deck vessels and submarines have proliferated across the region. For example, the Indian navy is undergoing modernization, with plans to become a 212-warship force by 2027 to guard India's geo-strategic interests, though funding has been a challenge. Despite the fact that Japanese spending on its Maritime Self-Defense Force is limited by its constitution and associated policy constraints, Japan has expanded its submarine fleet and indigenously developed maritime patrol aircraft to replace its aging stock. Plans are underway to convert Japan's two largest warships, the Izumo and the Kaga, into aircraft carriers.<sup>10</sup> South Korea has also been modernizing its navy and in October 2018 announced plans to create a blue-water fleet consisting of three squadrons and advanced Aegis destroyers. South Korea also launched the first of a planned fleet of nine indigenously designed KSS-III diesel-electric attack submarines in September 2018.

In Southeast Asia, Vietnam, the Philippines, and Malaysia have modernized and upgraded their maritime capabilities in response to increased Chinese presence in the disputed waters of the South China Sea. As China has engaged in land reclamation activities to build up small features in the area and erected infrastructure such as naval docks, landing strips, and radar and communications systems atop them, other claimant nations have come to feel that they too

need increased naval capabilities to cope with Chinese assertiveness. Some of these efforts have been supported by Japan, which has donated used vessels and provided training to Southeast Asian countries as part of its defense capacity building program.<sup>11</sup> Other Southeast Asian countries are also active in the maritime domain. Singapore has steadily invested in defense procurement due to its persistent sense of vulnerability, with recent acquisitions including new submarines featuring more firepower and combat options.<sup>12</sup> Indonesia has also begun modernizing its naval forces in an effort to keep up with Singapore and Malaysia.<sup>13</sup> As a consequence of technological development and diffusion, the amount of interaction and tension on the high seas has intensified. The maritime order is increasingly a multipolar one, with many players powerful enough to pursue their own interests, at least in their own neighborhoods. While this may be most evident in the South China Sea, it is also playing out in oceans as far-flung as the Arctic, where increased Chinese and Russian activity have also elicited more engagement from Japan and other countries.

## **Outer Space**

Far above the oceans, a similar pattern of technological progress and diffusion has emerged on another plane of the global commons: outer space. Although the United Nations took the position that outer space was to be used only for peaceful purposes and not subject to territorial claims by individual states, the domain was strongly shaped by the space race between the United States and the Soviet Union that began with the launch of Sputnik I in October 1957.<sup>14</sup> For decades, the U.S. and the USSR were the dominant players in outer space, until the end of the Cold War ceded the advantage to the United States. Over time, American predominance in this domain has gradually begun to erode due to internal budget pressures and growing competition from other states. Outer space offers states many opportunities to gain international prestige, to engage in cutting-edge research, and to launch satellites to facilitate military and civilian communications. Despite the high costs of developing space capabilities, late-developing countries have benefited from the ability to leapfrog developmentally by purchasing foreign space technology, avoiding the expensive mistakes inherent in trying to develop these complex technologies indigenously.<sup>15</sup>

As a result of this technological diffusion, a greater number of countries have become active in outer space, and as in the maritime domain, many of the academic and policy conversations have focused on the rise of China. China formally launched its manned space program in 1992, and it became the third country in history to launch a human into space in 2003. In 2007, it successfully conducted a direct anti-satellite (ASAT) weapon exercise, prompting concern that it might direct this new ability toward the satellites of other nations. China has explicitly linked its space program to its national security, and its activities have continued to expand. It plans to build a space station to support its long-term goals for space exploration and announced the first opportunity for all United Nations countries to apply to be involved in science missions in 2018, with the first module planned to launch in 2020. In January 2019, China became the first country to land a probe on the far side of the moon, a move that some link to plans for future exploitation of space resources.<sup>16</sup>

Chinese actions have prompted renewed competition, as other countries have sought both the technological capacity and the policy tools to become more active in outer space. While

Japan had long possessed relatively sophisticated space capabilities, the Chinese ASAT test and North Korean ballistic missile tests provoked it in 2008 to revise the domestic laws that had restricted its space program to peaceful purposes. This enabled Japan to procure a host of advanced military space capabilities to match or even exceed those of China, including dual-use assets in launch systems, communications and intelligence satellites, and counterspace capabilities.<sup>17</sup> Similarly, India has pursued a civil space program for decades, but technological advances by China and others have led it to expand its activities, to fund high-prestige exploratory missions, and to begin conducting military space activities. South Korea has rapidly developed its space capabilities since the early 1990s, focusing initially on satellite development, and more recently, on space launch vehicles. Other countries such as Australia, Indonesia, Malaysia, North Korea, Pakistan, the Philippines, Singapore, Taiwan, Thailand, and Vietnam are also beginning to play a significant regional or international role in space.<sup>18</sup> In addition, the United States has framed some of its recent activities in outer space as a response to challenges from China and Russia, with President Trump's 2018 proposal for the creation of a new Space Force as a sixth branch of the armed forces prompting Chinese criticism that the U.S. itself is promoting the weaponization of space.<sup>19</sup>

## **Cyberspace**

The role of technology is perhaps even more obvious in cyberspace, a relatively new addition to discussions of the global commons. Unlike outer space or the high seas, cyberspace is a virtual domain entirely constituted by technology; however, it is also more tangible than the other domains in some ways, since specific parts of its physical networks and infrastructure are actually owned by states and private actors. Advocates of including cyberspace as a new domain of the global commons point to the ways in which cyberspace is vast and difficult to control, as well as to the utility gained from its free and open use. Others claim that cyberspace is more akin to territorial seas to which access can be denied and argue that unfettered global access is no longer possible nor desirable.<sup>20</sup> While this definitional debate remains unresolved, there is growing consensus that the maritime, air, outer space, and cyberspace domains are fundamentally strategically interconnected.<sup>21</sup> Developments in cyberspace are not divorced from consequences in the physical world; cyber capabilities are often seen as complementary to military advances, for example, and attacks in the cyber realm can be used to destroy and disable physical infrastructure.

Research funded by the American government led to the creation of the Internet in the 1980s, and the United States was clearly the dominant player in the early days of cyberspace. However, in this domain as well, advances in and diffusion of technology have transformed cyberspace into a fundamentally more competitive virtual arena. In addition to boasting one of the world's fastest growing Internet economies, China is also home to one of its most active cyber operations programs. In the military realm, China has made a concerted effort to develop cyberspace capabilities to close the gap with the United States, as part of its anti-access area denial strategy, for example. American policymakers have voiced concerns about these developments and attempted to fortify themselves against potential attacks, though analysts point out that China itself also has a number of vulnerabilities.<sup>22</sup> Many also criticize China for its undemocratic policies in cyberspace, including censorship and surveillance of its citizens, as well as for increasing reports of Chinese economic espionage and intelligence gathering over the

Internet. As highlighted by the events surrounding the 2016 American presidential election, Russia has also developed a highly advanced offensive cyber program that American intelligence chiefs have said “poses a major threat to U.S. government, military, diplomatic, commercial, and critical infrastructure and key resource networks.”<sup>23</sup>

In cyberspace, technology can be a force multiplier that replicates the existing hierarchy of power, but it can also have a leveling effect, mitigating some of the advantages traditionally possessed by major powers and allowing smaller states and even non-state actors with limited resources to go on the offensive.<sup>24</sup> For example, fairly modest technological advances have enabled North Korea to become a major threat in the cyber realm. North Korea’s cyber operations are deliberate top-down efforts to target states such as the U.S. and South Korea that rely heavily on cyberspace for national and military activity.<sup>25</sup> North Korea is able to engage in these targeted attacks at a relatively low cost and low risk to itself in comparison to what it might face in engaging in other forms of conflict. Non-state actors have also emerged as threats in cyberspace, sometimes independently and sometimes working in tandem with governments, as in the case of China’s cyber militias and “patriotic hackers.”<sup>26</sup>

In recognition of these growing threats from both state and non-state actors, many other countries have moved to acquire the technology to develop their own cybersecurity programs. Largely in response to China, Japan has moved to develop its own domestic policy infrastructure and capabilities for defensive cybersecurity and to incorporate cyberspace into the scope of the U.S.-Japan alliance.<sup>27</sup> Focused primarily on North Korea, South Korea has also developed its cybersecurity policy infrastructure and strengthened its security protocols following several high-profile hacking incidents, including attacks on government agencies and on Korea Hydro and Nuclear Power in 2014. The countries of Southeast Asia have been slower to respond to the threats and opportunities of cyberspace due to the wide variation in their technological and institutional capabilities, but there has been some recent progress. As the sub-region’s most technologically advanced country, Singapore has driven much of the cybersecurity agenda of the Association of Southeast Asian Nations.<sup>28</sup> Other Southeast Asian countries have engaged in specific national cybersecurity activities, such as Malaysia, which has held annual public-private exercises to enhance its ability to protect critical infrastructure from cyber attack. As in the case of the high seas and outer space, as more states and private actors have gained the technological capability to become active in cyberspace, it has become more difficult to ensure the safety and stability of this domain.

## **Implications for Policy**

This examination of these three domains of the global commons—the high seas, outer space, and cyberspace—illustrates how first technological innovation and then subsequent technological diffusion have made accessible places and spaces that were previously largely inaccessible. In the early days of these domains, though no single country claimed sovereignty over them, they were dominated by the United States and, in the case of the high seas and outer space, by the Soviet Union as well. However, with the end of the Cold War and the rise of China, these domains appear to be becoming increasingly multipolar. In some ways, this pluralization of the global commons through technology is positive in that more countries than ever have the ability to utilize them and their resources. However, as the countries that are active in these

domains become more numerous, their interactions are also creating competitive dynamics that impact the security environment, particularly because the technological capacity of states to engage in the commons has developed more quickly than the regimes for their effective governance.

Although technology alone did not create these frictions between countries, many of which are rooted in long histories of complex interactions, the process of technological progress and diffusion has played an important—if sometimes inadvertent—role in exacerbating security tensions in the global commons.<sup>29</sup> To some extent, just the fact that a newcomer is acquiring the technology to become active in a domain may make other states feel threatened. The global commons are resource domains to which all nations have legal access, but they contain different kinds of resources that are subject to varying levels of excludability and subtractability.<sup>30</sup> Though it is often difficult to exclude others from using resources, each additional appropriator may reduce the amount of resources left for others, leading states to feel compelled to compete.

In addition, the specific nature of technological developments in the global commons has a tendency to exacerbate security dilemma dynamics in these domains. A key part of the security dilemma is that states are not explicitly trying to change the status quo; rather, their defensive intentions in developing or acquiring new technologies are difficult to credibly signal in an anarchic environment of uncertainty and mistrust, which results in misinterpretation by others.<sup>31</sup> Many of the technologies that have enabled states to become more engaged in the global commons are difficult to distinguish in terms of a state's offensive and defensive capabilities, further triggering this security dilemma logic. For example, due to the dual-use nature of space technologies, there is often inherent ambiguity to advances; civil and military uses cannot be truly separated. Therefore, the increasing technological sophistication of one state is perceived to decrease the security of other states, which in turn feel that they need to respond with similar technological countermeasures to defend themselves.<sup>32</sup> Moreover, while situations where defensive technologies have the advantage can be stabilizing, many countries feel that offensive forces may have the advantage in these domains, which further drives the acquisition of technologies that worsen the security dilemma.<sup>33</sup> Although the states discussed here are not engaged in the kind of full-scale arms race that can result from this action-reaction sequence, a clear trend toward competitive behavior has emerged. In terms of military competition in the areas of the commons addressed in this article, these dynamics are most pronounced in the maritime domain at present.

A pressing challenge for the future is that all of these domains are in need of stronger regimes that could help to ameliorate the security dilemma and ensure the good governance of the commons for the benefit the international community as a whole. The lack of a governing authority over the global commons and the misleading notion of their limitlessness make them particularly vulnerable to the current shifts in the international system.<sup>34</sup> Although the rules and norms of the high seas are the most developed of the domains discussed here, they have been increasingly challenged by the activities of states such as China, as seen with recent discussions surrounding the UN Convention on the Law of the Sea in the context of the South China Sea territorial disputes. The outer space regime grounded in the 1967 Outer Space Treaty needs a great deal more development to protect countries not only from anti-satellite and kinetic weapons but also from the growing problem of orbital debris, which threatens all space capabilities.<sup>35</sup>

Cyberspace is by far the least governed of these three domains, with its own regime still at an embryonic stage. In each of these domains, the development of technologies enabling states to access the commons has outpaced the development of the tools for their governance. Stronger regimes are necessary if only to promote transparency and information sharing, which existing scholarship suggests may help to reassure states, build trust, and reduce the risks of the security dilemma.

As a result of the increasing pluralization of power in the global commons, the United States increasingly depends on the newcomers to these domains to help promote their good governance. As these new players integrate into the existing system, they may come to see benefits from maintaining the stability and accessibility of the global commons, just as the United States did. However, it is likely that promoting shared perspectives regarding the global commons will require concerted effort and persuasion by those states most invested in such regimes. Cooperation between like-minded partners in the maritime, outer space, and cyberspace domains will be essential to protecting their peaceful use and ensuring that they remain open for the benefit of all.

Kristi Govella is an Assistant Professor in the Asian Studies Program at the University of Hawai‘i at Mānoa, a National Asia Research Program Fellow, and an Adjunct Research Fellow at the East-West Center. Her work deals with the intersection of economics, politics, and security in Asia, with a particular focus on Asian regionalism and Japanese politics. She is currently working on a number of projects related to economics-security linkages, regional institutional architecture, trade agreements, multinational firms, recent Japanese security reforms, and the global commons. Her publications include *Linking Trade and Security: Evolving Institutions and Strategies in Asia, Europe, and the United States* (2013). Prior to joining the University of Hawai‘i, Dr. Govella was a Postdoctoral Fellow at Harvard University and an Associate Professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies. She holds a Ph.D. and an M.A. in Political Science from the University of California, Berkeley and a B.A. in Political Science and Japanese from the University of Washington.

---

<sup>1</sup> As Vogler points out, “one shared characteristic of the global commons is their close association with scientific discovery and developing technological capability.” John Vogler, “Global Commons Revisited,” *Global Policy* 3, (1) (2012): 61–71.

<sup>2</sup> Barry Posen, “Command of the Commons: The Military Foundation of U.S. Hegemony,” *International Security* 28, (1) (2003): 5–46.

<sup>3</sup> For example, Japan has responded to increased Chinese activity across all three of the domains of the global commons addressed here. For an extended discussion, see Kristi Govella, “Securing the Global Commons? Japan in Outer Space, Cyberspace, and the High Seas” (Workshop on Conflict, Cooperation, and Interaction in the Global Commons, University of California, Berkeley, 2019).

<sup>4</sup> Kerry Lynn Nankivell refers to these countries as “blue-water middle powers.” See for example, Kerry Lynn Nankivell, “A Review of ‘Maritime Power and the Law of the Sea: Expeditionary Operations in World Politics’: By James Kraska. Oxford: Oxford University Press, 2011, 484 pp.,” *Ocean Development & International Law* 42 (4) (October 2011): 383–87.

<sup>5</sup> China Power Team, “How is China Modernizing Its Navy?” *China Power*, December 17, 2018, <<https://chinapower.csis.org/china-naval-modernization/>>.

<sup>6</sup> Mike Yeo, “China to Develop Its First Nuclear-Powered Aircraft Carrier,” *Defense News*, March 1, 2018, <<https://www.defensenews.com/naval/2018/03/01/china-to-develop-its-first-nuclear-powered-aircraft-carrier/>>.

- 
- <sup>7</sup> See for example, Michael Beckley, “The Emerging Military Balance in East Asia: How China’s Neighbors Can Check Chinese Naval Expansion,” *International Security* 42, (2) (2017): 78–119.
- <sup>8</sup> The United States has in turn responded to Beijing’s new anti-access area denial capabilities. See for example, Matteo Dian, “The Pivot to Asia, Air-Sea Battle, and Contested Commons in the Asia-Pacific Region,” *The Pacific Review* 28 (2) (2015): 237–57.
- <sup>9</sup> For example, Ritter refers to this as a “regional command of the commons.” See Tripp Ritter, “The Regional Command of the Commons: Japan’s Military Power,” *The Korean Journal of Defense Analysis* XVII (1) (2005): 235–58.
- <sup>10</sup> Felix Chang, “Japan’s New(ish) Aircraft Carriers: Reviving Japanese Naval Aviation,” *Foreign Policy Research Institute*, February 1, 2019, <<https://www.fpri.org/article/2019/02/japans-newish-aircraft-carriers-reviving-japanese-naval-aviation/>>.
- <sup>11</sup> See for example, Paul Midford, “Japan’s Approach to Maritime Security in the South China Sea,” *Asian Survey* 55 (3) (June 1, 2015): 525–47; and Kristi Govella, “Between Aid and Arms: Japan’s Emerging Approach to Defense Capacity Building” (American Political Science Association Annual Meeting, Boston, MA, 2018).
- <sup>12</sup> Lim Min Zhang, “Singapore Navy Launches First of Its Four New Submarines,” *The Straits Times*, February 19, 2019, <<https://www.straitstimes.com/singapore/spore-navy-launches-first-of-its-four-new-submarines>>.
- <sup>13</sup> For a brief overview, see Sheryn Lee, “Crowded Waters: Naval Competition in the Asia-Pacific,” APSI Special Report (Australian Strategic Policy Institute, 2015).
- <sup>14</sup> It is important to note that the technological advances of this period were also enabled by cooperation. Mai’a Cross argues that despite very visible competition among the main states involved, outer space was more accurately characterized as the product of international cooperation. See Mai’a Cross, “International Cooperation and Outer Space Exploration” (Workshop on Conflict, Cooperation, and Interaction in the Global Commons, University of California, Berkeley, 2019).
- <sup>15</sup> Alexander Gerschenkron, *Economic Backwardness in Historical Perspective* (Cambridge: Belknap Press, 1962).
- <sup>16</sup> See for example, Namrata Goswami, “The New Space Race Pits the US against China. The US Is Losing Badly.,” *The Washington Post*, January 10, 2019.
- <sup>17</sup> Saadia Pekkanen and Paul Kallendar-Umezu, *In Defense of Japan: From the Market to the Military in Space Policy* (Stanford: Stanford University Press, 2010); Paul Kallendar and Christopher Hughes, “Hiding in Plain Sight? Japan’s Militarization of Space and Challenges to the Yoshida Doctrine,” *Asian Security*, 2018.
- <sup>18</sup> For an excellent overview of these developments, see James Clay Moltz, *Asia’s Space Race: National Motivations, Regional Rivalries, and International Risks* (New York: Columbia University Press, 2012).
- <sup>19</sup> See for example, Tom O’Connor, “China Says Space is Not U.S. ‘Private Property’ as Donald Trump Plans to Build New Missile Defense There,” *Newsweek*, February 12, 2019, <<https://www.newsweek.com/china-space-property-trump-missile-defense-1329295>>.
- <sup>20</sup> Sam Tangredi, “From Global Commons to Territorial Seas: A Naval Analogy for the Nationalization of Cyberspace,” *Military Cyber Affairs* 3 (1) (2018).
- <sup>21</sup> See for example, Shawn Brimley, “Promoting Security in Common Domains,” *The Washington Quarterly* 33, (3) (2010): 119–32.
- <sup>22</sup> Jon Lindsay, “The Impact of China on Cybersecurity: Fiction and Friction,” *International Security* 39 (3) (2015 2014): 7–47.
- <sup>23</sup> Steve Ranger, “US Intelligence: 30 Countries Building Cyber Attack Capabilities,” *ZDNet*, January 5, 2017, <<https://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/>>.
- <sup>24</sup> On cyber technology as a force multiplier, see for example, Simone Dossi, “Confronting China’s Cyberwarfare Capabilities: A ‘Weapon of the Weak’ or a Force Multiplier?,” in *US Foreign Policy in a Challenging World*, ed. Marco Clementi, Matteo Dian, and Barbara Pisciotta (New York: Springer, 2018).
- <sup>25</sup> Jenny Jun, Scott LaFoy, and Ethan Sohn, *North Korea’s Cyber Operations: Strategy and Responses* (Washington, DC: Center for Strategic & International Studies, 2015).
- <sup>26</sup> While some of these actors’ activities are thought to be state-directed, there has been some research examining the emergence of regime-defending voices among Chinese individuals who are not state agents. For a nuanced account, see Rongbin Han, “Defending the Authoritarian Regime Online: China’s ‘Voluntary Fifty-Cent Army,’” *The China Quarterly* 224 (December 2015): 1006–25.
- <sup>27</sup> Paul Kallendar and Christopher Hughes, “Japan’s Emerging Trajectory as a ‘Cyber Power’: From Securitization to Militarization of Cyberspace,” *Journal of Strategic Studies* 20, (1–2) (2017): 118–45.
- <sup>28</sup> Elina Noor, “ASEAN Takes a Bold Cybersecurity Step,” *The Diplomat*, October 4, 2018.



---

<sup>29</sup> For example, for a discussion of the historical legacies exacerbating the security dilemma in Sino-Japanese relations, see Thomas J. Christensen, "China, the U.S.-Japan Alliance, and the Security Dilemma in East Asia," *International Security* 23 (4) (April 1999): 49–80.

<sup>30</sup> See for example, Susan Buck, *The Global Commons: An Introduction* (Washington, DC: Island Press, 1998).

<sup>31</sup> It is also important to note that in some cases states are actually explicitly trying to change the status quo, which does not follow the logic of the security dilemma. On this point, see Adam P. Liff and G. John Ikenberry, "Racing toward Tragedy?: China's Rise, Military Competition in the Asia Pacific, and the Security Dilemma," *International Security* 39 (2) (October 2014): 52–91.

<sup>32</sup> Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30 (2) (1978): 167–214.

<sup>33</sup> The issue of whether offense or defense has the advantage in cyberspace is still being debated. For a discussion of the advantages of defensive capabilities, see Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment," *International Security* 41 (3) (2016): 72–109.

<sup>34</sup> Carla Freeman, "The Fragile Global Commons in a World in Transition," *SAIS Review of International Affairs* 36 (1) (2016): 17–28.

<sup>35</sup> See Abraham Denmark, "Managing the Global Commons," *The Washington Quarterly* 33 (3) (2010): 165–82.