SSQ

STRATEGIC STUDIES QUARTERLY

WINTER 2016 VOLUME 10, NO. 4

Commentary

NASA in the Second Space Age: Exploration, Partnering, and Security
Todd Harrison and Nahmyo Thomas

Why Washington Doesn't Debate Grand Strategy
Benjamin H. Friedman and Justin Logan

Liberating Cyber Offense
James E. McGhee

Does China Have a Monroe Doctrine? Evidence for Regional Exclusion
Steven F. Jackson

Prohibiting Interference with Space-Based Position, Navigation, and Timing
Jonty Kasku-Jackson

Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot
Mark Raymond



Chief of Staff, US Air Force
Gen David L. Goldfein, USAF

Commander, Air Education and Training Command
Lt Gen Darryl L. Roberson, USAF

Commander and President, Air University
Lt Gen Steven L. Kwast, USAF

Director and Publisher, Air Force Research Institute
Dale L. Hayden, PhD

Editorial Staff
Col W. Michael Guillot, USAF, Retired, *Editor*
Donna Budjenska, *Content Editor*
Michele D. Harrell, *Prepress Production Manager*
Tammi K. Dacus, *Editorial Assistant*
Daniel M. Armstrong, *Illustrator*

Advisors
Gen Michael P. C. Carns, USAF, Retired
Allen G. Peck
Christina Goulter, PhD
Robert P. Haffa, PhD
Jay P. Kesan, PhD
Charlotte Ku, PhD
Benjamin S. Lambeth, PhD
John T. LaSaine, PhD
Allan R. Millett, PhD

Contributing Editors
School of Advanced Air and Space Studies
Stephen D. Chiabotti, PhD
Mark J. Conversino, PhD
The Spaatz Center
Charles E. Costanzo, PhD
Kimberly A. Hudson, PhD
Robert M. Kerr, PhD
Michael R. Kraig, PhD
Dawn C. Murphy, PhD
David D. Palkki, PhD
Paul J. Springer, PhD

Strategic Studies Quarterly (*SSQ*) (ISSN 1936-1815) is published quarterly by Air University Press, Maxwell AFB, AL. Articles in *SSQ* may be reproduced free of charge. Notify editor and include a standard source credit line on each reprint.

STRATEGIC STUDIES QUARTERLY

An Air Force-Sponsored Strategic Forum on National and International Security

WINTER 2016 VOLUME 10, NO. 4

Commentary

NASA in the Second Space Age: Exploration, Partnering, and Security 2
Todd Harrison and Nahmyo Thomas

Feature Article

Why Washington Doesn't Debate Grand Strategy 14
Benjamin H. Friedman and Justin Logan

Perspectives

Liberating Cyber Offense 46
James E. McGhee

Does China Have a Monroe Doctrine? Evidence for Regional Exclusion 64
Steven F. Jackson

Prohibiting Interference with Space-Based Position, Navigation, and Timing 90
Jonty Kasku-Jackson

Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot 123
Mark Raymond

Book Review

Mankind Beyond Earth: The History, Science, and Future of Human Space Exploration 150
By: Claude A. Piantadosi
Reviewed by: Maj Ryan Sanford, USAF

Relevant Online Reviews 152

NASA in the Second Space Age: Exploration, Partnering, and Security

The launch of Sputnik in 1957 and the dawn of the space age set off a frenetic competition between the Soviet Union and the United States. In the years that followed, both nations developed and orbited military satellites with increasingly sophisticated capabilities for intelligence collection, communications, and missile warning—capabilities largely intended to support strategic nuclear forces.[1] For more than three decades the competition between these two superpowers was relatively stable, marked by notable periods of cooperation and engagement. Since the end of the Cold War, however, a gradual change has been under way, driven in part by advances in technology and the proliferation of space capabilities. This transformation has ushered in what the National Aeronautics and Space Administration's (NASA) Tom Cremins has termed the "second space age."[2]

The second space age arguably began with the 1991 Gulf War. This conflict demonstrated, for the first time, the distinct advantages space-based capabilities can provide in conventional war fighting. The collapse of the Soviet Union also changed the geopolitical landscape and weakened the superpower duopoly in space. The 2011 National Security Space Strategy (NSSS) defines this new era by what has become known as the three Cs: congested, competitive, and contested.[3] Space has become congested as more nations and private companies are launching and operating satellites for a variety of missions and increasingly competitive as they vie for economic and strategic advantage. According to the Space Foundation, global space activities generated some $330 billion in economic activity in 2014, more than three-quarters of which came from commercial space products, services, infrastructure, and support.[4] A robust group of space startup companies has also emerged in recent years, injecting a fresh wave of innovation and competition in the space industry.

Perhaps the most disturbing attribute of the second space age is that space has become an increasingly contested domain. The United States is not alone in its use of space for military applications; more than 20 nations currently operate military satellites, making space a critical domain in modern warfare.[5] Because of the many military advantages

space offers, potential adversaries have made advances in antisatellite technologies—both kinetic and non-kinetic—to deny the United States and its allies the benefits of space-based capabilities. And as the 2007 Chinese antisatellite missile test demonstrated, widely accepted norms of behavior in space remain lacking.[6]

At the same time, NASA's role in space exploration is at an inflection point. The International Space Station (ISS) and human spaceflight to low Earth orbit (LEO) have been the centerpieces of NASA's mission for decades. Since the retirement of the space shuttle in 2011, however, NASA no longer has the ability to launch astronauts. Servicing of the ISS for both cargo and crew has transitioned to commercial companies and the Russian Federation. With the ISS currently scheduled for retirement in 2024 and work on the new Space Launch System (SLS) and the multipurpose crew vehicle known as Orion still in progress, NASA is shifting its attention to human exploration beyond LEO.

The 2011 NSSS states that, "Our strategy requires active U.S. leadership enabled by an approach that updates, balances, and integrates all of the tools of U.S. power."[7] But one of the most powerful tools available to the United States is not mentioned in this strategy. NASA and its vast network of commercial and foreign government partners are a key component of US national power and influence in the space domain. Virtually every nation that aspires to play a significant role in space wants to partner with NASA due to its technological expertise and powerful brand image. For many, it is an important symbol of prestige and power to join the club of responsible, spacefaring nations led by NASA.

This confluence of circumstances—the increasingly congested, competitive, and contested nature of the second space age and NASA's shift in mission focus beyond LEO—presents a once-in-a-generation opportunity to define the terms by which the second space age will operate. Will the space domain be a wild frontier where nations go it alone? Or will it be a more cooperative domain where norms are respected and the United States retains its leadership position? The next administration should seize this opportunity to set a new space exploration strategy for NASA that advances US interests in space by pushing the boundaries of human knowledge, bringing new partners into the club of responsible, spacefaring nations, and extending US leadership in this vital domain.

A Space Exploration Strategy

A new strategy for space exploration beyond LEO must include long-term exploration objectives that excite and inspire public support and near-term milestones that are technologically and fiscally achievable. In April 2010 Pres. Barack Obama gave a major address on space exploration at Kennedy Space Center. In his address, the president laid out a series of incremental improvements in capabilities, including: a new space telescope to replace Hubble; increased Earth-based observation for climate monitoring; extending the life of the ISS and working with private companies to deliver cargo and crew to the ISS; increased robotic exploration of the solar system, including scouting missions to Mars and other celestial bodies; continuing the Orion space vehicle program; and building SLS to provide a heavy lift launch capability for future missions. But the president only briefly mentioned his long-term objectives for where these space-exploration capabilities would take the United States. He called for sending humans to an asteroid sometime in the mid–2020s, to orbit around Mars in the mid–2030s, and eventually to land on Mars without any specific timeframe mentioned.[8] In the NASA Authorization Act of 2010, the most recent policy bill enacted for the agency, Congress stipulated that future missions beyond LEO should be designed to incorporate international contributions and that SLS and a multipurpose crew vehicle should be the building blocks for these future missions.[9]

At the most basic level, strategy is about bringing ends, ways, and means into alignment. For NASA, the desired "ends" are its exploration objectives, whether to cislunar space, an asteroid, Mars, or beyond. The "ways" are how NASA plans to achieve its objectives—the specific programs and activities it undertakes and the ways it engages with partners. But having a desired end state in mind and a plan to get there is not sufficient. The "ends" and "ways" of a strategy may be constrained by the "means." NASA's means include the people it employs, the labs and facilities it maintains, the annual budget it receives from Congress, and the many industry and international partnerships it sustains. An exploration strategy set without regard for the means required risks being un-executable in practice. Furthermore, the heart of an effective strategy is not just determining what one *will* do but also what one *will not* do.[10]

In his 2010 speech, President Obama proposed increasing NASA's budget by $6 billion over the next five years. Due to budget constraints imposed by the Budget Control Act (BCA), however, NASA's budget

declined by 12 percent in real terms from FY10 to FY15.[11] The BCA budget caps are set to remain in effect through FY21, meaning that without a broader budget deal NASA is unlikely to receive a significant increase in funding in the near future. Moreover, because NASA's budget falls within the nondefense side of the budget caps, it competes directly with other domestic programs which are projected to continue growing for the foreseeable future. That means any increase in funding required for new exploration missions must be offset in part by reductions in legacy missions or the reallocation of science and technology investments to more directly support the exploration challenges ahead.

Challenges That Are NASA-Hard

When setting its exploration objectives, NASA should focus squarely on challenging missions where there are significant risks that only NASA can or should assume—challenges that are truly "NASA-hard." For example, in space exploration there is always the possibility that a mission may fail to achieve its objectives or discover anything of value. The risks of mission failure are often highest when pushing the outer limits of human knowledge—looking beyond where humans have explored—because there may be nothing of interest. When the mission risk-reward imbalance is too great, commercial firms and other government agencies are often reluctant to engage in this type of exploration. Yet these are exactly the type of high-risk ventures an agency like NASA ought to undertake to expand the boundaries of human knowledge.

Another type of risk only NASA should assume is extreme risk to human life. While sending humans into LEO remains risky, the safety of human spaceflight has improved to the point that NASA has begun the process of ceding human spaceflight in LEO to commercial companies, and numerous commercial ventures are on the verge of creating a space tourism industry. The technological advancements that made this possible are the result of billions of dollars invested in research and development and real-world experience by NASA over the course of nearly six decades. Human spaceflight beyond LEO, however, is less well understood, and further research and development remain to be done. Only nine manned missions flew beyond Earth orbit as part of the Apollo program, six of which landed on the moon, while there have been hundreds of manned missions to LEO. The risks to humans for missions to the moon, Mars, and beyond remain high—perhaps too high for

nongovernment entities to undertake at this point, notwithstanding statements by SpaceX's Elon Musk, who, regardless of ambition, must continue to rely on NASA's help and expertise.[12] With groundbreaking investments in exploration by NASA, however, human missions beyond LEO could one day be opened to commercial ventures at a more acceptable level of risk.

A final type of risk that NASA is uniquely positioned to assume is the risk associated with large capital public goods projects. The ISS, for example, is effectively a massive infrastructure project in space that provides a public good for humanity: a zero-gravity laboratory that serves as a platform for many other missions and scientific experiments. It does not make economic sense for a private company to fund projects like the ISS, with its price tag of over $100 billion. Even if a company were so inclined, it is unlikely that it could raise the capital required for such a project or ensure a healthy return on investment. Some space missions, like the ISS, are so large that they can only be undertaken by NASA. However, once these investments are made, they can be leveraged by private companies for commercial purposes, such as testing new drug-manufacturing technologies or as a destination for space tourism.[13] NASA's investments in space infrastructure, like the ISS, may also serve as an impetus for private companies to invest in the development of smaller human platforms to retain these capabilities once the ISS is retired.

Strategic Partnering

Armed with a space-exploration strategy that has long-term objectives, near-term milestones, and a focus on challenges that are NASA-hard, the next challenge is to build a coalition of industry and international partners with a shared interest in the mission. Partners are a critical component of any future space exploration strategy because NASA is not likely to have the resources or capabilities to pursue its ambitions alone. One of the key challenges for NASA in executing a new space-exploration strategy is determining what capabilities it should keep internally and what it should outsource to others. While the exploration objectives may be things that are truly NASA-hard, the capabilities required to pursue these objectives may not be the exclusive domain of NASA. Capabilities that once were core to NASA's identity, such as human spaceflight to LEO, are quickly becoming the domain of commercial firms. The ISS, for example, may soon be approaching the point where it can transition

to commercial operations, either partially or in full, which would free up resources within NASA that could be applied to new missions. As NASA shifts its focus to new objectives, it will need to refocus its internal capabilities—including science and technology investments—on areas in which no commercial market exists and ruthlessly divest itself of internal capabilities that can be more effectively provided by industry. However, when leveraging the innovation and expertise of industry, NASA must also be careful not to become overly dependent on companies with untested business models or objectives that may diverge from NASA's interests.

An ambitious space-exploration agenda also presents an opportunity to extend and expand NASA's network of international partners to advance broader US foreign policy and national security objectives. The 2011 National Security Space Strategy states that the United States "will encourage responsible behavior in space and lead by the power of our example."[14] NASA is perhaps the best example the United States has to offer for the peaceful and responsible use of space. Moreover, NASA's vast network of international partners is a source of strategic advantage for the United States that can be leveraged to help promote stabilizing norms of behavior in space.

Since many other nations do not maintain a clear separation between military and civil space activities, decisions on whom to partner with on civil space programs must take into account potential security implications. However, geopolitical competition and even antagonism between nations do not necessarily preclude the possibility of cooperation in civil space exploration. History has shown that cooperation in civil space programs that is mission focused and mutually beneficial can proceed largely independent of competition in other areas.

Perhaps the best example of this is the cooperation between the United States and the Soviet Union that took place throughout the Cold War. Beginning with the Kennedy administration, the two superpowers engaged in a series of cooperative ventures that included sharing weather satellite data, mapping the Earth's geomagnetic field, and experimenting with communication relays in space. In the 1970s, the two rivals embarked on a joint human spaceflight program known as the Apollo-Soyuz Test Project. While US cooperation was through NASA, the Soviet civil space program was secretive and intermixed with the military's space command. As Russian physicist (and former science advisor to Soviet

Pres. Mikhail Gorbachev) Roald Sagdeev and international security and space policy expert Susan Eisenhower have noted, this cooperation gave the United States valuable insight into the largely shrouded Soviet space enterprise.[15] Following the breakup of the Soviet Union, cooperation and insight into Russian space programs continued first with visits of the US space shuttle to the Russian Mir space station and then with the Russian Federation joining the ISS consortium—a partnership that continues today. Perhaps the longest-running example of international partnership in space is the US-Russian Joint Working Group on Space Biology and Medicine, which has been active since 1971 and has spanned the Apollo-Soyuz, Shuttle-Mir, and ISS programs.[16]

As this example demonstrates, partners do not have to like each other to cooperate successfully if the basis of their partnership is a shared interest in the mission. Despite a marked decline in the US-Russian relationship in recent years, cooperation on civil space programs has so far not been affected. Both the United States and Russia have a shared interest in continuing to cooperate because neither can maintain the ISS or a robust human spaceflight program on its own. Nevertheless, one must be mindful of the geopolitical risks and opportunities involved in partnerships that create an interdependence with other nations.

Partnerships can also be beneficial for strategic reasons beyond just the mission at hand. For example, the United States could partner with another nation to influence the direction of that country's space activities and encourage norms of behavior ranging from limiting the production of space debris to sharing scientific data. The United States can also use the enticement of partnering on civil space programs to discourage other countries from engaging in activities that would be detrimental to US interests.

Partnerships on civil space programs can also provide valuable insight into the organizations and space activities of other countries. For example, China does not make the same distinctions between civil and military space programs as the United States. This comingling of programs leads to great uncertainty and mistrust on the part of the United States, which has been noted by the US-China Economic and Security Review Commission. In its 2015 report, the commission quotes one expert as saying, "China's space program does not have structures in place that make meaningful divisions between military and civil programs, and those technologies acquired and systems developed for ostensibly civil

purposes can be applied—and most frequently are—for military purposes."[17] The lack of separation between military and civilian programs invites suspicion and should not be ignored. But just as the United States partnered with the Soviet Union during the Cold War, partnering with China on select civil space programs could provide greater insight into an otherwise opaque system. This kind of partnership can reduce uncertainty regarding China's space activities and help encourage investment in more peaceful and stabilizing space capabilities. It could also lay the groundwork for military-to-military contacts between the US and Chinese militaries' space commands, something that is sorely needed and is vital to stability and mutual understanding in a crisis situation.

When selecting partners, one must also be mindful to avoid incentivizing others to develop or mature dual-use technologies with national security implications. In 1996, the failed launch of a Chinese Long March rocket carrying a US commercial satellite led to a US company transferring technical data to the Chinese that helped improve their launch capabilities. Since this technical data was also relevant to China's long-range missile programs—a key national security concern for the United States—it led to strict controls being put in place to prevent future technology transfers.[18] Technology transfers such as this are clearly prohibited by law, and partnerships for civil space programs should go one step further and avoid partnering in any way that could incentivize or assist a rival power in the development of military space capabilities. Instead, partnerships with military rivals should be focused on missions that have little if any direct military applications, such as human spaceflight and deep space missions.

Guiding Principles for International Partnerships

International partnership decisions should be informed by a fundamental set of guiding principles. These principles must be consistent with NASA's exploration strategy and considerate of geopolitical factors and domestic politics in the United States and its partner countries. Based on the past experiences of NASA, the European Space Agency (ESA), and other space agencies as well as best practices gleaned from other international organizations, four fundamental guiding principles for international partnerships stand out for consideration.

1. **International partnerships should be based on areas of mutual interest and benefit**. As Dr. Jean-Jacques Dordain, the former director general of ESA, has noted, when it comes to building strong relationships, mutual interest is in many ways more powerful than love. Partners do not need to love each other or even like each other—they merely need to have a shared interest in the mission.[19] Partnerships should be structured in a way that each partner is better off in net from partnering than from not partnering. The benefits each partner derives from cooperation, however, do not need to be symmetrical. For example, a smaller space agency may benefit from the prestige and resources of partnering with NASA, while NASA may benefit from getting access to facilities, geographical locations, or specific technical expertise.

2. **New partners should not come at the expense of existing partners.** For multinational endeavors, all parties should be consulted and should consent to adding new partners, and new partners should bring value that benefits each of the existing partners. Moreover, NASA must be careful to consider how new bilateral agreements—even if they involve separate and distinct mission areas—could affect existing partnerships in other areas. When reaching out to new partners, careful coordination and open communication can help prevent existing partners from feeling isolated or undermined.

3. **Each international partner should self-fund its part of the project**. While not an absolute rule, this structure helps prevent the need for complex contracting and fund-transfer agreements and is one of the guidelines for international cooperation NASA already follows.[20] It also helps alleviate negative competition or resistance from each country's industrial base, where fears of commercial loss often result in resistance to international partnerships. Moreover, self-funding avoids putting partner governments in the sometimes awkward position of appropriating funds for another government's agency and industrial base. When each partner funds its own contribution to the project, it keeps the partnership focused on the mission rather than on the financial details. In the no-exchange-of-funds model, each partner also assumes the risk of cost overruns for its part of the project, creating a strong incentive for each partner to manage and control the cost of work under its direction.

4. **International partnerships should be structured so that they do not rely on the exchange of technology**. The transfer of technology, particularly in the area of space systems and launch vehicles, is a sensitive issue even among close allies. In the no-exchange-of-technology model, each partner is responsible for developing and applying its own technology for its part of the project. The exchange of technical information can then be limited to the minimum level of information needed for technical interfaces between mission modules—another guideline for international cooperation NASA already employs.[21]

Conclusion

NASA is at an inflection point. With the impending retirement of the ISS and the opportunity for human exploration beyond LEO, NASA is well positioned to continue its leadership role in the second space age. But to make this transition a success, it needs two things. First and foremost, it needs a space exploration strategy with clear, long-term objectives that are truly NASA-hard to excite and inspire public support. Just as important, it also needs a robust network of industry and international partners that shares its exploration objectives and has meaningful capabilities to contribute.

In many ways, NASA's challenge is to make a dime out of 10 pennies. It must bring together a network of industry and international partners—including new and nontraditional partners—in a cohesive and coherent manner to advance its exploration objectives. With a clear strategy that sets long-term objectives that excite and near-term milestones that are achievable, NASA can reorient itself to work with new partners in more innovative and effective ways. Without such a strategy, however, NASA risks spending a penny here and a penny there and not having a dime to show for it.

NASA's leadership still has no equal or substitute in the second space age to foster international cooperation, to push the technological envelope, and to promote responsible and stabilizing norms of behavior. While the hard power of NASA's technical prowess has long been held in high regard, the soft power of NASA's influence through agreements with industry and foreign governments has yet to be fully realized. US national security relies on commercial and military space-based capabilities that are

increasingly at risk, and other nations, private companies, and the rest of the US government look to NASA to promote cooperation and the peaceful use of space. While NASA was the indispensable partner of the first space age, NASA's network of partnerships is the indispensable ingredient for security and continued US leadership in the second space age. SSQ

Todd Harrison
Director, Aerospace Security Project and Senior Fellow
Center for Strategic and International Studies

Nahmyo Thomas
Director, Executive Education and Abshire-Inamori Leadership Academy
Center for Strategic and International Studies

Notes

1. Lt. Gen. Ellen Pawlikowski, Doug Loverro, and Col. Tom Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," *Strategic Studies Quarterly* 6, no. 1 (Spring 2012): 30, http://www.au.af.mil/au/ssq/2012/spring/pawlikowski.pdf.

2. Tom Cremins, *A New Space Age: Maximizing Global Benefits*, report (New York: World Economic Forum, 2014), http://reports.weforum.org/global-strategic-foresight/thomas-e-cremins-nasa-a-new-space-age/.

3. Department of Defense (DOD) and Office of the Director of National Intelligence (DNI), *National Security Space Strategy: Unclassified Summary* (Washington, DC: Director of National Intelligence, January 2011), 1, http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf.

4. Space Foundation, *The Space Report* (Colorado Springs, CO: Space Foundation, 2015), 1, http://www.spacefoundation.org/sites/default/files/downloads/The_Space_Report_2015_Overview_TOC_Exhibits.pdf.

5. Union of Concerned Scientists, "UCS Satellite Database," accessed 25 February 2016, http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.VeRUq_ZVhBc.

6. Todd Harrison, "Operating in the Dark: Rules of Engagement Needed for Space," *For Your Situational Awareness* newsletter, Center for Strategic and International Studies, http://fysa.csis.org/2015/09/29/operating-in-the-dark-rules-of-engagement-needed-for-space/.

7. DOD and DNI, *National Security Space Strategy*, 1.

8. Barack H. Obama, "Space Exploration in the 21st Century" (address, Merritt Island, FL, 15 April 2010), https://www.whitehouse.gov/the-press-office/remarks-president-space-exploration-21st-century.

9. National Aeronautics and Space Administration Authorization Act of 2010, Public Law 111–267, Sec. 301, http://www.nasa.gov/pdf/649377main_PL_111-267.pdf.

10. See Andrew Krepinevich, "The Pentagon's Wasting Assets: The Military Foundations of US Dominance Are Steadily Eroding," *Foreign Affairs* 88, no. 4 (July/August 2009): 18–33, http://www.jstor.org/stable/20699619.

11. Calculations derived from Office of Management and Budget, *President's Budget for Fiscal Year 2017, Public Budget Database: Budget Authority* (Washington, DC: GPO, 9 February 2016), https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/budauth.xls.

12. Christian Davenport, "Elon Musk Provides New Details on His 'Mind Blowing' Mission to Mars," *Washington Post*, 10 June 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/06/10/elon-musk-provides-new-details-on-his-mind-blowing-mission-to-mars/.

13. Jeff Foust, "Former NASA ISS Manager Planning Commercial Space Station Venture," *Space News*, 23 June 2016, http://spacenews.com/former-nasa-iss-manger-planning-commercial-space-station-venture/.

14. DOD and DNI, *National Security Space Strategy*, 5.

15. Roald Sagdeev and Susan Eisenhower, "United States-Soviet Space Cooperation during the Cold War," *NASA Magazine: 50 Years of Exploration and Discovery*, http://www.nasa.gov/50th/50th_magazine/coldWarCoOp.html.

16. Briefing by David Tomko and Steve Davison to NASA Advisory Council Research Subcommittee, subject: International Coordination, 12 September 2014, 18, https://www.nasa.gov/sites/default/files/files/NAC_Research_SubCom_International_2014Sept12.pdf.

17. U.S.-China Economic and Security Review Commission, *2015 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: US Government Publishing Office, 2015), 273, http://origin.www.uscc.gov/sites/default/files/annual_reports/2015%20Annual%20Report%20to%20Congress.PDF.

18. Jeff Gerth, "2 Companies Pay Penalties for Improving China Rockets," *New York Times*, 6 March 2003, http://www.nytimes.com/2003/03/06/world/2-companies-pay-penalties-for-improving-china-rockets.html.

19. Dr. Jean-Jacques Dordain (former director general of the European Space Agency, Syracuse, NY), interview by the authors, 5 November 2015.

20. Tomko and Davison, "International Coordination," briefing, 3.

21. Ibid.

Why Washington Doesn't Debate Grand Strategy

Benjamin H. Friedman and Justin Logan

Abstract

Debate over grand strategy is nearly absent in US politics. Relative military power, over time, generated bipartisan support for primacy, a grand strategy that sees global US military dominance as the basis for US security. The elite consensus in favor of primacy saps political demand for critical analysis of it or consideration of alternative grand strategies. Because Washington think tank analysts and public intellectuals mostly answer to political masters, they have no incentive to buck the conventional line and question primacy. They focus on operational questions about how to implement primacy, unlike academic analysts, who debate the merits of alternative grand strategies. In this article we demonstrate the limits of debate about grand strategy in US politics and explain this absence of debate. We also explain why think tank analysts, more than academics, conform to this consensus and conclude by considering implications for analysts in both academia and Washington.

* * * * *

The vast majority of US foreign policy makers are devotees of *primacy*, a grand strategy that sees global US military exertions—alliances, foreign bases, patrols, military training, regular wars, and continual airstrikes—as the only guarantee of national security, global stability, and free trade. Foreign policy debate in Washington, when it exists, mostly concerns how to implement primacy rather than alternative grand strategies. This article explains why the foreign policy establishment tends to

---

Benjamin H. Friedman is a research fellow in defense and homeland security studies at the Cato Institute and coeditor of two books. He is a graduate of Dartmouth College, a PhD candidate in political science at the MIT, and an adjunct lecturer at George Washington University's Elliott School of International Affairs.

Justin Logan is the former director of Foreign Policy Studies at the Cato Institute. He earned a master's degree in international relations from the University of Chicago and a bachelor's degree in international relations from American University.

avoid debating strategic ends and focuses instead on means. We call that tendency the *operational mind-set.*[1]

Because primacy serves the interests of US political leaders, there is little demand for arguments questioning it. Ambitious analysts avoid evaluating strategy and focus instead on operational analysis. The stream of books, papers, reports, panel discussions, testimony, televised arguments, and the like from government agencies, Congress, bipartisan commissions, and think tanks gives the impression that US foreign policy is the result of rigorous argumentation occurring in a true marketplace of ideas. However, policy makers use social science, including the shallow sort Washington produces, more to legitimize policy than to form beliefs about which policy to pursue. The sheen of independent expertise heightens the appeal of a particular policy and protects it from dissent. Left unevaluated, primacy has gained adherents and become more like an article of faith one invokes rather than an idea one evaluates.

It is naïve to expect think tanks to evaluate grand strategy absent demand from political patrons. True strategic debate in Washington would require a change in consensus politics. Because that is currently unlikely, if academics do not interrogate the assumptions underlying US foreign policy, no one will. Doing so will not produce immediate results. Policy makers tend to ignore academia, not because it is considered a "cult of irrelevance," meaning esoteric subject matter and complex methods, but because of academics' disinclination to tell policy makers only what they want to hear.[2] Academia should reward policy relevance but understand that "relevance" often means being a naysayer.

In this article, we first show the dearth of debate in Washington about grand strategy. Then, we explain this absence of debate and how primacy achieved dominance. Next, we discuss the politics that encourage think tank analysts, more than academics, to conform to the prevailing consensus. In conclusion, we explore what the argument suggests for analysts in both academia and Washington.

The Missing Debate

The US foreign policy establishment—the group of people typically appointed to security posts in the federal government, writing for the major opinion pages, and hired by most prominent think tanks—barely debates grand strategy.[3] This claim may be surprising given the vast attention Washington pays to foreign policy and the many people there

who analyze it for a living. Certainly foreign policy analysts produce many arguments, and the think tank industry is healthy and growing. Several large US think tanks dealing with foreign policy opened in the last decade, while the previously existing ones grew substantially.[4] (In 2011, think tanks that included foreign policy departments spent over $1.2 billion, an increase of approximately 40 percent over the decade, adjusting for inflation.[5]) In theory, think tanks function as universities without students, places where intellectuals freely research public policy and propose ways to improve it. In what might be termed the *marketplace of ideas view*, political leaders and the interested public evaluate and choose among such proposals.[6] In this view, debate exposes poor ideas and selects the best, as markets do with products.

The usual complaint about the Washington foreign policy debate is that it is excessive and overly partisan, not that it is insufficient. Pundits and politicians frequently call for a more bipartisan foreign policy, an end to politics beyond the water's edge. They bemoan the loss of the Cold War strategic consensus around containment. Even political scientists who understand that the Cold War actually included plenty of partisan division about foreign policy and the meaning of containment still tend to lament the increased partisanship in US foreign policy since the Cold War.[7] Anyone watching cable news or reading major opinion pages knows that each source features considerable, often bitter, debate about foreign policy decisions.

Why worry about the limits of a debate that is so heated and widely lamented? The answer is that the rancor of arguments tells us little about their stakes. Despite the partisanship infusing Washington's foreign policy debate and the expansion of think tanks participating in it, shared assumptions narrow the disputed terrain. Debate focuses on how to enact the goals of the grand strategy of primacy, not their wisdom. The debate is more about operational analysis than grand strategy.

O*perational analysis* considers how to best implement goals without evaluating the goals themselves—taking objectives as given.[8] An operational mind-set means doing that all the time. It is the approach of a passenger riding shotgun who studies the map to find the ideal route, adjusts the engine if need be, and always accepts the destination without protest. There is nothing inherently wrong with that approach. Even opponents of government programs should want them to run more efficiently.[9] The problem occurs when operational thinking becomes a

widespread habit that occurs at the expense of—or masquerades as—an evaluative mind-set, where analysts ask whether the ideas animating policies, even sacred ones, are sound.[10] Unexamined strategic goals can become a kind of operational code or guiding ideology, their wisdom taken for granted.[11]

Strategy is logic for a choice among options; it prioritizes. Strategy is "grand" when it aims to guide other foreign policy goals and decisions. Those subsidiary goals, in theory, steer diplomatic goals and military strategy, which in turn drive agency choices, down to the smallest decisions. Grand strategies are general theories of how states create security for themselves. Grand strategy is unavoidable and occurs whenever states have security policies informed by causal ideas, which is virtually always. The permanence of competing parties and goals, however, ensures that grand strategy is never fully realized. It is particularly difficult to achieve without pressing dangers to unify people, and the degree of realization varies across and within states.

Academics—generally within the security or international relations fields of political science—weigh competing grand strategies, like selective engagement, restraint, and primacy, both explicitly and by evaluating their underlying theoretical claims.[12] Political scientists also occasionally study operational issues. Analysts within the foreign policy establishment, by contrast, focus on operational questions. They do produce occasional writing and conferences on grand strategy but rarely evaluate primacy. They tend instead to reify it, often in the guise of new buzzwords and murky geopolitical analysis.

Primacy Ascends

In current US foreign policy, primacy, also known as "liberal hegemony," consists of an interlocking set of beliefs.[13] One is that US leadership is crucial to the maintenance of "the global order," which refers generally to peace among great powers, international commerce, and state cooperation through international organizations.[14] A second belief is that US leadership largely comprises military commitments—allies, overseas bases, naval patrols, and threats or acts of war.[15] The reasoning is generally that US military power deters aggression, limiting the need for states to defend themselves, preventing security dilemmas: self-reinforcing dynamics of mutual alarm.[16] US military power therefore functions like a global police force, averting the need for states to secure

themselves. Because of these beliefs, primacy places a high value on allies, and its adherents support the permanence of US defense alliances like NATO, often support their expansion, and generally push for new alliances when they perceive new threats.[17]

Primacy's advocates see many threats to the United States. They worry about the credibility of the many promises the United States makes to defend allies. They fear proliferation of weapons technology, especially nuclear weapons.[18] Primacists tend to argue that internal conditions abroad (foreign civil wars, failed states, or illiberal governments) can easily undermine US global leadership, creating danger. These fears translate into heavy work for the US national security establishment. So, primacists tend to favor high military spending and regular uses of force—patrols, military-to-military training, deployments of forces, commitments to defend nations, or acts of war.

Primacy, in other words, is conducive to war.[19] Its expansive view of threats creates a grab bag of reasons to support proposed wars or military strikes and few arguments for peace. Liberal internationalists, the Democratic primacists, and the neoconservatives and hawkish nationalists comprising the Republican cohort typically offer overlapping but differing rationales for wars. For example, in advocating the invasion of Iraq in 2003, Republican primacists emphasized the need to demonstrate US credibility, pro-democracy arguments, and preventive-war logic of stopping terrorists from getting nuclear weapons, while liberal internationalists emphasized nonproliferation concerns and the Saddam Hussein regime's violation of international law and humanitarian abuses.[20] Most recent US wars produced a similar pattern of complementary rationales.

Primacists do not agree on everything. The Republican variety mostly sees international institutions, especially the United Nations, as worse than useless in that they can impede US activism.[21] Liberal internationalists believe in at least the appearance of cooperation with international institutions, mainly because the seal of multilateral approval makes the exercise of US power more palatable abroad.[22] Right-leaning primacists are more skeptical of humanitarian rationales for wars but usually support the same wars for other reasons.

Partisanship highlights these narrow areas of disagreement among primacists, drawing attention away from their large realm of agreement. While foreign policy elites debated primacy's tenets early in the Cold War, it has increasingly become a bipartisan ethos. Primacy reigns at the

major US think tanks, both right- and left-leaning.[23] Today it is hard to imagine how a president could fill the national security bureaucracy with non-primacist appointees, unless he or she was willing to rely on inexperienced academics.

Because primacy is a hawkish grand strategy, its dominance in Washington limits analysis of US war goals. In the last two decades at least, wars have commenced without much debate in the foreign policy establishment. Even the decision to invade Iraq, easily the most controversial war in recent decades, generated only limited debate. Though a majority of House Democrats and 21 of 50 Democratic senators voted against the resolution to use force in October 2002, their objections focused more on timing and tactics—the imminence of the threat, the strength of war plans, and the danger of taking attention from the war in Afghanistan—than on the broader wisdom of occupying Iraq and overthrowing its government.[24]

The George W. Bush administration debated how to market the war but not whether to have it.[25] Few of the principals can even say when that decision occurred.[26] According to Bob Woodward, then-Secretary of State Colin Powell hoped to dissuade the president from war but never actually opposed it.[27] The intelligence community raised doubts about the quality of intelligence on Iraq's arsenal and the difficulties of achieving postwar stability. President Bush and his top advisors seem to have taken these warnings mostly as a threat to their effort to win support for war.[28] The same goes for the cautiously antiwar statements offered by officials from the George H.W. Bush administration, most notably Brent Scowcroft, the former national security advisor. There is no evidence that George W. Bush administration officials debated the merits of these claims.[29]

Think tank analysts and pundits were not much better. Prior to the invasion, their focus was mostly how to make war and the postwar plan. One study showed that only 4 percent of the guests appearing on the nightly news to discuss the potential war during the early weeks of February 2003 expressed any skepticism about its prudence.[30] The *Wall Street Journal*'s editorial page editor, Paul Gigot, dismissed the relevance of the antiwar views expressed by Cato Institute scholars, suggesting they represent "four or five people in a phone booth."[31] That is a reasonable description of how primacy's critics feel in Washington.

Over the last decade, the wars, along with economic slowdown and debt, made the foreign policy establishment more dovish, especially

about occupational wars.[32] But that shift came without much strategic reevaluation. Only when the public and major Democratic politicians turned against the wars did left-leaning think tanks begin openly to support their end. Even then, there were precious few efforts to revisit the rationales that had sustained the wars. The establishment now pursues the same broad set of goals with less tolerance for risk in their pursuit. Recent debates about Syria, Yemen, and Ukraine concern degrees of activism, whether to go from sanctions to lethal aid to bombing. No one in or near power publicly suggests that US interests in these places are insufficient to warrant much effort.

For example, Washington's debate about the 2011 US bombing campaign in Libya was quiet and narrow, despite the rather incredible claims that the administration and other war backers made: that war would produce liberal democracy in Libya and enhance its prospects in the region by convincing other tyrants to tolerate protest or revolutionary movements.[33] The administration also made dubious claims about the vast humanitarian value of the intervention.[34] Congress paid virtually no attention to the war's rationale. Think tanks focused more on the conduct of the war and the organization of Libya in its aftermath than on its wisdom. Hardly anyone outside academia suggested that Muammar Qaddafi's fall was likely to bring long-term instability.[35] Libya's descent toward chaos since the war has not stopped its advocates from celebrating their wisdom and urging similar tactics in Syria.[36]

Current Trends: More of the Same

Two recent developments show the strength of the establishment consensus. First, Republicans leaders, especially those who ran for president, vociferously criticized the Obama administration's foreign policy for being weak yet proposed no clear alternative. An example is the recent book by former Vice President Dick Cheney and his daughter Liz.[37] After three lengthy chapters attacking the Obama administration for "retreating" or "appeasing" on defense policy, the Cheneys' conclusion suggests no new wars, no new theaters for existing wars, and no new military alliances. They excoriate the Iran nuclear weapons deal but argue for a better one. They portray ISIS (the Islamic State) as a cataclysmic threat in rapid advance, but they do not call for regular US ground forces to directly fight it. Their great concern about Russia's uncontained aggression leads them to propose doing more of what is being done: more NATO

exercises, sanctions, and aid to Ukraine. Former presidential candidates like Jeb Bush, Marco Rubio, and Ted Cruz took similar lines.

The problem for Republicans is that the Obama administration subscribes to primacy, albeit with a partial dissent on the importance of credibility.[38] The administration seems to support most current alliances, has increased efforts to counter Russia and China, and is making war, with special operations forces, conventional airpower, or drone strikes, in seven countries. Republicans have little room to show their relative hawkishness beyond proposing larger deployments of US ground forces, which is electorally dangerous, and spending more on defense. So for all their rhetorical assaults on the Obama's administration's foreign policies, conventional Republicans propose doing more of the same, with more tough talk.

The second example is the reaction to Donald Trump's presidential campaign. Trump deviated to a limited extent from the primacy consensus by questioning the value of NATO and suggesting that South Korea and Japan acquiring nuclear weapons might reduce the US defense burden. That seemed to have helped him with the Republican electorate, which, as noted, does not share the establishment's belief in primacy. But Trump's statements caused apoplexy among both the liberal internationalist and neoconservative bands of primacists.[39] Their unified opposition to Trump's foreign policy views reflects their unified belief in primacy.

How Primacy Achieved Dominance

US relative power explains why primacy rules in Washington. Relative power comes from military capability, wealth, and geographic advantage. These factors give the United States the ability to adopt ambitious objectives abroad. They also keep the US public remote from the consequences of US security policy and thus generally disinterested. This circumstance permits political leaders to pursue primacy without much fear of electoral consequence.[40] US power also encourages American political leaders to embrace the global military role that primacy justifies. Washington's foreign policy analysts accept these goals because of professional incentives and the socialization they produce over time. Before elaborating on that explanation, we reject two others. One is that primacy became the nation's grand strategy by winning intellectual battles. The second is that primacy reflects democratic will.

One argument for primacy's dominance in Washington is that it won out in a reasoned debate. Peter Feaver remarks, "Radical critiques of American foreign policy are known and given lots of air time proportional to their influence. You can't swing a dead cat without hearing a serious critique of American foreign policy at an academic conference, for example. These views are known, considered, and rejected."[41]

That view, where Washington rejects alternatives to primacy after giving them a fair shake, predicts that its advocates rely on a solid intellectual case. If that is so, they might build on well-established international relations scholarship and history. Or finding hostile theory and scholarship, primacy's backers would explain the flaws that cause them to reject it, essentially building up a theoretical alternative. Neither occurs.

International relations scholarship rarely produces clear conclusions. One can find support for competing grand strategies by picking on one set of articles or another. Still, on balance, primacy's core arguments rest on poor theoretical footing. The emphasis on alliances, for example, hinges on several doubtful assumptions. One is that states lacking a US alliance will generally kowtow to more powerful ones—*bandwagoning*, in international relations jargon—allowing aggressors to gather strength and ambition, as occurred with Nazi Germany. A second assumption is that if states do not "bandwagon" and instead work to defend themselves by balancing stronger power, danger will result, either because the balancing among rivals creates mutual fear conducive to war or because other states' independence undermines US leadership. International relations scholarship, however, suggests that states, especially strong ones, often balance power; that most balances are stable, particularly where geography makes borders more defensible; and that few foreign wars greatly impact the United States.[42]

Primacy's insistence that US military alliances impede nuclear weapons proliferation casts aside well-established arguments: that US military presence and power encourage proliferation among threatened states and that nuclear weapons can create mutual deterrence conducive to peace.[43] The same goes for primacists' claim that US military presence enables global trade. The argument implies without basis that trade is brittle or easily disrupted and that other states are unlikely to police their own trade if the US Navy does not.[44] Primacists also argue that a global US military presence caused the decline of war among states in recent decades.[45] Prominent academic studies attribute the current

era of relative peace to other causes.[46] Even the theories of liberal and capitalist peace, which might seem to better accommodate primacists' claims, do not argue that US military exertions abroad generally spread liberal or capitalist systems.[47] Scholarship suggests, rather, that US military actions are often counterproductive to those ends.[48]

Doubtful hypotheses also inform the establishment take on the threats energizing primacy. Credibility fears follow from the idea that coercive threats are difficult to uphold and that reputations for acting on them travel easily across time and space. Scholarship on the matter suggests instead that the credibility of threats is more contextual: credibility depends on the interests and military power of the state making threats.[49] Primacy's fear of disordered states turns on the belief that they produce international terrorism and other ills. But few failed states produce these troubles.[50] Moreover, primacy's enthusiasm for trying to repair such states often means downplaying a threat with a substantial historical pedigree: that of nationalism and other identity politics conducive to violent resistance against occupiers.[51]

We cannot exhaustively catalog all of primacy's flaws or debate the rare academics who defend it using international relations literature.[52] The point here is to exemplify weakness in the case for primacy. That helps explain the academic crowd in range of Feaver's swinging dead cat. Primacy's flaws are the big reason why international relations scholars, especially those who study security, tend to critique it.[53]

Academics' dovish take on war and defense spending suggests their skepticism about primacy. In 2007, roughly 80 percent of academics in the international relations field reported having opposed the war in Iraq at its outset.[54] Even if the war's course generated some false reporting, the true number is surely far higher than in the establishment, where initial opposition was rare. The 2009 Afghanistan surge was probably equally unpopular in academia. Columbia University professor Jack Snyder remarked then that "pretty much everyone [in the academy] thinks that the conditions in Afghanistan are terrible, that the political situation is terrible, and thus that the conditions for successful counterinsurgency and state-building are inauspicious."[55] A 2004–2005 survey of international relations scholars asked, "Do you think that the United States should increase its spending on national defense, keep it about the same, or cut it back?" Just short of half—49 percent—answered, "Cut," while 41 percent chose, "Keep same." Only 10 percent answered, "Increase."[56] When

the researchers asked the question again in 2008–2009, 64 percent said, "Cut" and 30 percent chose, "Keep the same"; this time, only 6 percent called for an increase.[57] On taking office in 2009, Barack Obama, the most liberal American president in at least 30 years, proceeded to increase military spending that had nearly doubled in the previous decade.[58] Little objection came from the foreign policy establishment.

Some will object that liberal politics, not knowledge, turns academics against primacy. There is likely some truth in this, but liberalism, at least in the sense of supporting Democrats, does not preclude supporting primacy. Democratic foreign policy elites, after all, typically embrace primacy's liberal internationalist variant. The same is true of many academics. Also, in the American international relations field, the dominant academic critique of primacy comes from realism. Realism grew in opposition to legalist or missionary approaches to foreign policy promoted by Wilsonian progressives. It travelled historically with the political right. That link has weakened, but still many prominent realists lean right politically, albeit idiosyncratically. Despite some variation, primacy is unpopular with academics mostly because it is a set of bad ideas.

Had primacy succeeded on its intellectual merits in spite of scholarly criticism, its establishment advocates would make its theoretical case themselves, or at least cite those that do. Instead, they ignore the problem. If leading politicians are aware of primacy's theoretical failing, they do a good job pretending otherwise. Even think tank analysts, many of whom hold advanced international relations degrees, mostly avoid engaging academic criticism of primacy. If they mention alternative grand strategies, it is to dismiss straw man versions in a few sentences, often by labeling them politically irrelevant.[59] Few cite even the academic works taking their side.[60] Many policy makers and think tank scholars appear to be unaware that they employ theories about international politics; some even deny having a theory.[61] Primacy's theoretical weakness does not concern its advocates in Washington.

General Public versus Elites

The democratic explanation for primacy's dominance also lacks support. According to a 2014 Chicago Council on Global Affairs study, the public is far less enthusiastic about taking an "active" role in global affairs and global leadership than elites.[62] That divide holds across partisan lines. There is a substantial gap between elites identifying as Democrat,

Republican, or Independent and the public for each group. Similarly, elites are more supportive of using force to defend allies and long-term US military bases and more likely to agree that those garrisons produce stability.[63] Various studies show that the public is historically less hawkish on issues of war and defense spending than elites.[64]

Recent wars also reflect the divide. A November 2009 Pew poll, taken just before the president announced the surge of US troops in Afghanistan, found that 32 percent of the American public wanted more US troops in Afghanistan, and 40 percent wanted to decrease the troop presence.[65] In a companion poll, Pew found that 50 percent of Council on Foreign Relations members wanted a troop increase and 24 percent wanted a decrease.[66] In 2014, the Chicago Council found even wider gaps between foreign policy elites and the public on the question of keeping troops in Afghanistan.[67] Similar dynamics—a foreign policy elite pushing a reluctant public to support military escalation—occurred in recent years with Libya and Syria.[68]

These results suggest that the foreign policy establishment pushes the public toward primacy, not the other way.[69] A more accurate explanation for primacy's success is that it rationalizes policies that leaders already support. Relative power, especially the military capability to act abroad, allows those policies and creates constituencies that support them—a set of beneficiaries who support primacy. Power and geography also keep the costs of the policies low and distributed enough so that the public is disinterested, giving leaders a relatively free hand.

Taking the cost side first, geography and the wealth to generate military power insulate the United States from the consequences of security policy, including war. The public lacks incentive to closely monitor foreign policy. It remains rationally ignorant.[70] Unlike pocketbook issues, foreign policy questions are rarely salient: they generally rank low among voters' concerns and contribute little to their voting decisions. So politicians seldom have strong electoral reasons to cater to voters' foreign policy views.[71] Voters are more dovish than foreign policy elites for the same reasons. They are mostly too disinterested to listen to the establishment's hawkish tenets. For most Americans, the only direct cost of foreign policy fiascoes is marginally higher tax rates and unsettling newscasts. Since the draft ended, war kills "only" the volunteer military and foreigners.[72] By contrast, for Europeans living 100 years ago, losing wars potentially meant conquest and its depredations. Even successful

wars could kill off large swaths of young men and consume considerable portions of national wealth.

Wealth creation has reduced the economic burden of US security policy without curtailment of its ambitions. Americans now spend around what they did on defense at the height of the Cold War, in real terms, but the percentage of wealth devoted to that purpose is far lower. It takes less than 4 percent of gross domestic product, which keeps down the tax burden and leaves plenty of funds for other programs. The interest groups associated with low taxes and those programs have less reason to oppose primacy's policies.

Primacy Unopposed

The absence of rivals leaves the United States free to roam.[73] Few states combine the desire and ability to resist US military deployments. True, the military would run into trouble if it invaded China or approached various other hostile coasts.[74] And the price of occupying restive lands has also proved restrictive. Still, opportunities for US military aid outnumber obstacles. Many countries invite US forces in to subsidize their defense. The world never lacks for civil unrest whose victims US forces might protect, and outraged editorialists reliably take up the cause.

These conditions produce a support base for primacy.[75] As is the case with other public policy areas (like farm subsidies) that create diffuse costs and concentrated benefits, a minority of special interests rules a majority of the apathetic.[76] This set of minority interests (that is, the foreign policy establishment) functions as a kind of oligarchy in its domain, but only insofar as its prescribed policies do not concentrate costs that awaken organized opposition. That occurs if defense spending threatens other spending and programs dear to other powerful special interests. Likewise, when wars impose high costs without clear benefit, the public gets engaged and pressures elected leaders to limit or end the war, as occurred eventually with the Vietnam and Iraq wars.[77]

It is a simplification to speak of the foreign policy establishment as a singular entity. There is certainly conflict among its elements. But US power limits that conflict. A lot of interests get their wishes, and the nation, as a result, pursues security objectives so broad that in sum they approach global management.[78] The key actors here can be called the military-industrial-congressional complex: those interests, organizations, and elected officials that share an interest in high military spending.[79]

That includes the military services, whose budgets fund bases and production contracts important in many electoral districts, the companies and unions drawing on those budgets, and the elected officials representing those districts, who usually seek seats on defense committees.[80] Other interests conducive to primacy are lobby groups favoring particular countries, civic groups supporting particular military services, and various research entities, including arms of universities and think tanks that receive military or foreign-government research grants.

Primacy is useful less as a rationale for particular policy goals than as justification for limiting choices among them. US policy makers strain for compromise because they divide power in a system that is open to the influence of diverse interest groups.[81] Senators and representatives fight across party and committee lines to direct policy. The presidency, despite the more dominant role it assumed over the direction of foreign policy during the Cold War, still shares those powers with Congress.[82] The State Department, the intelligence agencies, and the Pentagon compete for power. The Pentagon spreads authority among four military services, unified combatant commands, the Joint Chiefs of Staff, and the Office of the Secretary of Defense.

This division of power militates against strategic coherence, especially when threats are limited.[83] By voting for budgets, as they generally must, politicians essentially endorse the whole package, including items of no direct importance to them. In explaining their votes, it is insufficient to simply admit the need for compromise among parochial and bureaucratic agendas. Those arguments may be honest, but they offend the notion that leaders elected by states or districts should serve the national interest, especially in the security realm. That is true especially of presidents, who are elected nationally, of course, but forced by the limits of time and influence to compromise with the various parochial or narrow interests.[84]

Grand strategies, or the simpler versions of them politicians express, can serve that rationalization function. They try to align the various goals within defense budgets into an expression of national interest. In the United States, primacy is especially useful in this regard because it discriminates so little. By justifying activist US military policies virtually anywhere, primacy accommodates a host of agendas. These interests would compete more if the United States had less power. Primacy results from the luxury to avoid choices among programs, dangers, and

regions.[85] It is a pretense of strategy, helping avoid the choices that true strategy entails.

Primacy's popularized story has been the dominant rationale, under various names, with various tweaks, at least since the Cold War's end. Arguably, its reign began when the Truman administration imagined the Soviet Union's containment as a global struggle with communism.[86] Its popularity has risen along with US relative power. As with other successful ideologies, the story's repetition by influential people convinces others, some of whom are or become leaders.

Intellectual dominance also gives primacy social cachet. People in Washington's foreign policy circles adopt it outwardly even if they are not fully convinced, which in turn convinces others or encourages them to act convinced.[87] So primacy's promoters are both those that benefit from power's exercise and those convinced by their story. The groups overlap considerably, especially in the foreign policy establishment. Most of primacy's supporters do not choose to believe in it so much as they absorb it through a combination of ambition, compromise, and socialization.

Why Think Tanks Conform to Consensus

Washington's think tank analysts broadly embrace primacy because they are not independent of the politics they study. The marketplace of ideas view misconstrues power's relationship with social science, especially the sort think tanks produce. Most think tanks exist more to serve power than to guide it.

With relatively weak parties and power divided among branches, agencies and congressional committees, the US government has many points where political leaders—elected and appointed government officials—might seek the advice of outside experts.[88] Leaders seek three major sorts of help from experts: guidance as to what policy goals to pursue, evaluation of alternative means to reach those goals, and validation that helps with marketing policy goals.[89] Think tanks serve in all three roles but tend to emphasize the first, as befits the marketplace of ideas story. But what leaders most often want from outside experts is help with marketing—the imprimatur of scholarly credibility—affirmation in the guise of consultation.[90] Leaders, in other words, rarely want the policy equivalent of architects so much as real-estate brokers.

Some exceptional politicians and officials defy this generalization. And there are times where an election, crisis, or new assignment sends leaders

looking for broad intellectual guidance from independent analysts.[91] There are, however, several reasons why those are the exceptions. First, other leaders, staff, interest groups, and parties compete for the policy guidance role, limiting outsiders' roles. Second, leaders' circumstances generally push them to focus on implementing existing goals rather than identifying new ones. Those in government are often short on time to make the kind of study needed to formulate new directions. And political leaders mostly got where they are by acting on strong beliefs, which are hard to modify.[92]

The Lure of Validation

The nature of the US political system is the third and most important reason why leaders use experts especially for validation. The diffusion of power makes it difficult to form and maintain coalitions of support for policies, especially new ones. Leaders struggle to sell their preferred policies to each other, interest groups, and the public.[93] They can heighten support for a policy by convincing others that it serves not only its sponsors and some narrow set of economic or geographic interests but also the general good. Experts armed with advanced degrees and impressive résumés can credibly claim to speak for the national interest. Their endorsement is especially valuable when they seemingly have no incentive to give it—when their institutional affiliation indicates independence from political authority.

Think tanks have a competitive advantage in performing this function: their balance of independent expertise and subordination to a political agenda.[94] Lobbyists have expertise, but the fact that it is expressly for hire limits the value of their endorsement. Academics may be more impressive scholars, but their profession makes them less attuned to what political leaders want. To be clear, it is not our argument that think tanks will say anything or lack scholarly standards. If their support is obviously for sale, rather than a result of study, they destroy the value they provide to funders. On the other hand, if think tanks were really universities without students, with no obvious policy agenda, few would attract funding.

One senator described this legitimization function this way: "You can find a think tank to buttress any view or position, and then you can give it the aura of legitimacy and credibility by referring to their report."[95] Rory Stewart, an expert on Afghanistan who opposed the 2009 surge,

describes how this dynamic played out in his consultation with Obama administration officials planning the surge: "It's like they're coming in and saying to you, 'I'm going to drive my car off a cliff. Should I or should I not wear a seatbelt?' And you say, 'I don't think you should drive your car off the cliff.' And they say, 'No, no, that bit's already been decided—the question is whether to wear a seatbelt.' And you say, 'Well, you might as well wear a seatbelt.' And then they say, 'We've consulted with policy expert Rory Stewart and he says . . . .' "[96]

Motivations for Operational Mind-Sets

So far we have described why policy makers seek think tanks' approval, but not why think tanks play this role. Why are they subordinate to politics? Why not follow academics in evaluating grand strategy? Think tanks' diversity makes it difficult to generalize about their internal politics. Each has different sources of support. Some seek influence primarily among policy makers, while others court broader audiences. Some follow the direction of a few funders, often foundations or a government agency. Some support a political party; others, an ideology. In recent years, several think tanks, most prominently, the Center for American Progress and Heritage Foundation, organized separate branches for lobbying and supporting candidates. Federally funded research and development corporations (FFRDCs) exist to help elements of the government manage particularly technical issues.[97] The most famous of these, the RAND Corporation, originally served as a home for Air Force scientific advisors and later branched out into other disciplines and government funding sources.

Still, we can identify four factors, active to varying extents in different think tanks, that encourage analysts to adopt the operational mind-set. The first is money. Some analysts profit directly from their views by serving as consultants to defense contractors or lobbyists.[98] They have good reason to go along with policy arguments that benefit their funders. More important are think tanks' operational funds. Some rely almost entirely on US government funds and require analysts to finance their own projects and pay by winning research contracts. Some think tanks receive considerable funding from major defense contractors.[99]

These funding sources encourage an operational mind-set. One reason is that the funder often asks the research questions. Because of the funder's function and interests, these are usually operational questions. Because analysts cannot know with certainty who their next funder will

be, they may refrain from criticizing the beliefs, like primacy, held by other potential funders. The result is circumstanced speech, not necessarily dishonesty. Also, think tanks dependent on these funds will be unlikely to hire or reward analysts that question primacy and risk alienating funders.[100] Anyone seeking to be hired as an analyst by a think tank will likely consider several options, meaning that they should consider how their views fit with various think tanks. That uncertainty induces caution.

Foundation grants also create pressures to avoid certain arguments. An example is the mass of foundation support for nonproliferation studies, which probably keeps some from noting the deterrent benefit of nuclear weapons or emphasizing the dangers of militarized effort to slow their spread. And while prominent foundations are less tied to primacy than government agencies, their employees, like those of think tanks, have professional reasons to avoid straying too far from Washington's intellectual conventions. That affects what they will fund.

Some think tanks receive funds from foreign governments or entities tied to them.[101] This might seem to induce disloyalty or at least views that deviate from those of the US foreign policy establishment, but it is more likely another reason to support primacy. Most of the funding nations want the aid and protection that primacy justifies.

Professional ambition is a second reason analysts adopt an operational mind-set. Because most think tank scholars aspire to government appointments, they avoid offending the dominant foreign policy views in the party they hope to serve. Because both parties embrace primacy, ambitious analysts on both sides steer clear of attacking it. Ambition also recommends caution even when it comes to trumpeting some goals of potential patrons. Political winds may shift, and other patrons with different views may beckon. In the case of the recent Iraq War, Democratic leaders mostly supported it initially and mostly regretted that later. Hillary Clinton's loss to Barack Obama in the 2008 Democratic presidential primaries demonstrates this risk. Cagey analysts avoided clear stances on the war, keeping their focus on issues like how to coordinate the interagency process to manage the state-building campaign.[102]

The third driver of the operational mind-set is relevance. Donors typically fund think tanks not just because of what they say but also for their seeming ability to convince policy makers. That requires relevance, meaning the attention of administration officials, congressional staff, and the like. Relevance generates media attention and boosts egos. Analysts

that tell policy makers things they do not want to hear, like criticism of primacy's goals, are liable to lose relevance.

Tangled in with relevance is a fourth cause: socialization. Because primacy has become an operational code of the foreign policy establishment, analysts may avoid criticizing it to avoid the social discomfort of being at odds with their peers. This factor should be less important in think tanks housed outside Washington, DC, especially those that are linked to universities. Even Leslie Gelb, as president of the Council on Foreign Relations, was not immune to such pressures. He attributed his support for the Iraq War, which he'd come to regret, to "unfortunate tendencies within the [Washington] foreign policy community, namely the disposition and incentives to support wars to retain political and professional credibility."[103] The credibility Gelb speaks of is probably an amalgam of professional and social factors that induce intellectual conformity. Accepting or at least keeping quiet about a flawed strategic consensus is the price of membership in the foreign policy establishment.

Another example showing the confluence of these pressures is RAND's research on the Vietnam War. RAND never produced a broad assessment of US policy in Vietnam. Starting in 1961, its analysts worked on government-funded studies of narrower issuers like enemy morale and the efficacy of the strategic hamlets program. RAND's historiography on its involvement in Southeast Asia during this period identifies "a general pattern that was to prevail throughout the Vietnam War: When RAND's research conclusions contradicted official thinking, they usually elicited strong objection and were ignored, or were dismissed outright."[104] In this circumstance, analysts eager to be relevant to the client, get a government appointment, or maintain funding are liable to emphasize findings that clients find useful and to avoid questioning the war's wisdom.[105] Honesty in what one writes is compatible with self-censorship.

If academics seek grants, appointments, and access at Washington's foreign policy institutions, they confront some of the same incentives think tank analysts do.[106] The result is academic writing friendlier to primacy and more prone to operational thinking than would otherwise be the case. Still, the academy's professional incentives leave its scholars overall far less susceptible than think tank analysts to the operational mindset. Tenure insulates against political pressures. And by rewarding novel theory and bold conclusions, political science creates incentive to find flaws in key theories underlying popular foreign policies and grand strategies.

Prospects for Grand Strategy Debate

Washington lacks a grand strategy debate, despite a vibrant debate in the academic security studies community on the subject. Something is wrong either in Washington or in the security studies community. We blame Washington, where US national security politics discourages debate about strategy and drives analysts to adopt an operational mindset. The US foreign policy establishment will continue to avoid debating grand strategy until politics changes. Others blame analysis, especially the academic kind. Many Washington policy hands and academics worry that Washington ignores academia because of its irrelevance. More than 20 years after Alexander George advocated "bridging the gap" between policy and academia, a number of initiatives are attempting to do so.[107] Better questions and writing, in this view, would produce better policy. Stephen Walt, for example, refers to an academic "cult of irrelevance," meaning esoteric research questions irrelevant to policy and quantitative and formal model research methods.[108]

Relevance and accessibility are worthy goals. But they are unlikely to bridge the gap that keeps policy makers from embracing international relations scholarship. That prescription follows from a misdiagnosis of the problem. Today, Washington ignores all sorts of relevant, well-written, qualitative political science scholarship—including Walt's. The biggest reason policy makers fail to heed such work is that it does not say what they want to hear. The tendency to blame analysis for bad policy results from the belief that everyone would agree on policy with the right information and theories. But democratic politics is a competition for power, where disagreement results from conflicts of interest and ideas are weapons the combatants wield.

A standard reaction to this notion that politics often wants science to serve rather than guide it is to propose emancipation, schemes to liberate analysis from political influence. That means keeping campuses and think tanks free of political ambition and government funds or somehow protecting "the policy process" from "self-interested individuals and groups."[109] But it is neither possible nor desirable to purge policy debates of self-interest. Washington's marketplace of policy ideas is flawed—but democratic. Were it possible to purge it of self-interest, the market would be barren and silent but for the few failing merchants proudly disdainful of customers that never arrive. Think tanks totally divorced from political interests would wither or die, leaving their job

to entities that respond to political demand. The solution to bad policy is better politics, meaning more productive conflict that demands new ideas, not quixotic attempts to empower Platonic guardians by quieting interested parties.

Willingness to Challenge the Status Quo

Given that the operational mind-set results from consensus, what may improve debate about grand strategy is conflict in the establishment, either between parties or some other set of important groups. If political leaders demanded strategic alternatives, think tanks would provide them. The operational mind-set would diminish. A precedent exists in the interservice fights of the late 1950s, which produced strategic debate about nuclear doctrine.[110] But that seems unlikely at present, primarily because the conditions that produced primacy's dominance appear durable.

Both critics and backers of primacy predicted that the Afghanistan and Iraq wars' unpopularity, recession, and deficits would restrain US grand strategy or at least shift debate that way.[111] Concern about the deficit produced the 2011 Budget Control Act's budget caps, which restrained Pentagon spending. Antiwar sentiment made it difficult for US leaders to propose the use of ground forces in new conflicts.[112] These shifts were not without effect, but the establishment consensus favoring primacy held. No other major defense policy changes have occurred, despite military spending cuts. Were a political constituency rejecting primacy likely to arise from these forces, it should have arrived already. If we are right, few think tanks will push for a reevaluation of US grand strategy. Only the academy can sustain a critique of primacy. That creates a special responsibility to do so. This need not entail a rush to the partisan barricades or prescriptive writing extending beyond what research supports. It means questioning the assumptions that underlie policy—pointing to the tradeoffs and faulty assumptions politics avoids acknowledging.[113] While immediate results are unlikely, policy ideas often matter a lot eventually, but they are not self-ratifying. They get adopted when a shock, like a lost war, or crisis provokes widespread demand for change.[114] Because it is nearly impossible to predict when this may happen, academics should continue producing ideas about strategy so they are on the bookshelf when politics goes in search of new ideas.

Efforts to move the political ground beneath leaders have greater promise. Academics can consider not just the wisdom of grand strategies but the basis of their support, which generates insight about how to alter them. Institutional reforms might fracture support for primacy.[115] For instance, more aggressive spending caps requiring more painful cuts from powerful constituencies might have produced a real push to reevaluate primacy, possibly creating lasting change in the establishment's ideological landscape. Similarly, a law requiring taxes to pay for wars would concentrate some of primacy's costs and, given sufficient expense, likely split primacy's support base. Another means to provoke strategic debate is increasing competition among military services for budgets and relevance. That might induce the services to promote strategic alternatives.

Beyond this, scholars who care about changing US grand strategy should continue their work but lower their expectations. Permissive international and domestic environments allowed Washington's variously warring tribes to agree on a remarkably ambitious grand strategy. The market for alternatives is small, at best, so most politically relevant analysts stay operationally focused. Those of us bothered by that situation can take solace in the national good fortune that produced it. Only the richest, safest nations can persist in a foolish grand strategy without bothering to debate it. SSQ

Notes

1. Other authors address this dynamic in different terms. Henry A. Kissinger, "The Policymaker and the Intellectual," *The Reporter*, 5 March 1959, 30–35; Aaron Wildavsky, "Rescuing Policy Analysis from PPBS," *Public Administration Review* 29, no. 2 (March/April 1969): 189–202, http://www.jstor.org/stable/973700; and Harvey M. Sapolsky, "The Science and Politics of Defense Analysis," in *The Social Sciences Go to Washington*, ed. Ham Cravens (New Brunswick, NJ: Rutgers University Press, 2003), 67–78.

2. Stephen M. Walt, "Rigor or Rigor Mortis? Rational Choice and Security Studies," *International Security* 23, no. 4 (Spring 1999): 46, http://www.jstor.org/stable/2539293. Don K. Price long ago identified a similar academic tendency, which he calls "the retreat toward abstraction," and attributes it to professionalization and the prescriptive modesty it encourages. Don K. Price, *The Scientific Estate* (Cambridge, MA:, Harvard University Press, 1965), 112–19; and Hans J. Morgenthau, "The Purpose of Political Science," in James Clyde Charlesworth, *A Design for Political Science: Scope, Objectives, and Methods* (Philadelphia: American Academy of Political and Social Sciences, 1966), 63–79.

3. On this absence of debate, see John A. Gans Jr., "Can't We All Just Not Get Along? Why a Decade of War Hasn't Provoked a Real Debate about America's Role in the World," *Foreign Policy*, 24 October 2012, http://foreignpolicy.com/2012/10/24/cant-we-all-just-not

-get-along/; and Barry R. Posen, *Restraint: A New Foundation for U.S. Grand Strategy* (Ithaca, NY: Cornell University Press, 2014), 5–16.

4. Major examples are the Center for American Progress and the Center for New American Security.

5. The year 2011 was the latest year for which we could get sufficient data. Totals were calculated using public tax records and James McGann's list of major think tanks, excluding those without foreign policy components, those housed within universities, and those that are primarily grant-making organizations. Those lists are here: http://repository.upenn.edu/think_tanks/.

6. Modern exponents of this view, classically articulated by John Stuart Mill in his essay *On Liberty*, tend to see it as a normative goal that political forces disrupt. Chaim Kaufmann, "Threat Inflation and the Failure of the Marketplace of Ideas: The Selling of the Iraq War," *International Security* 29, no. 1 (Summer 2004): 5–48, http://www.jstor.org/stable/4137546; and Stephen M. Walt, "Where Do Bad Ideas Come From? And Why Won't They Go Away?," *foreignpolicy.com*, 3 January 2011, http://foreignpolicy.com/2011/01/03/where-do-bad-ideas-come-from/.

7. Charles A. Kupchan and Peter L. Trubowitz, "Dead Center: The Demise of Liberal Internationalism in the United States," *International Security* 32, no. 2 (Fall 2007): 7–44, http://www.jstor.org/stable/30133874.

8. We do not necessarily mean operational or operations research, the discipline of using advanced analytical methods to improve organizations' decision making and improve their efficiency. On the development of operational research in Great Britain and the United States during World War II, see Stephen Budiansky, *Blackett's War: The Men Who Defeated the Nazi U-Boats and Brought Science to the Art of Warfare* (New York: Knopf, 2013). On operations research and the birth of systems analysis, see J. A. Stockfish, *The Intellectual Foundations of Systems Analysis,* RAND Publication no. P-7401 (Santa Monica, CA: Rand Corp, 1987).

9. The Brookings Institution, for example, in 1948 helped the Truman State Department plan the administration of the Marshall Plan in a way that satisfied its key congressional sponsor, Sen. Arthur Vandenberg, and succeeded substantively. On this effort, see Hadley Arkes, *Bureaucracy, the Marshall Plan, and the National Interest* (Princeton, NJ: Princeton University Press, 1972), 84–114.

10. Stephen Van Evera, "Why States Believe Foolish Ideas," in *Perspectives on Structural Realism*, ed. Andrew K. Hanami (New York: Palgrave, 2003), 163–98.

11. The "operational code" terminology is from Nathan Leites, *The Operational Code of the Politburo* (New York: McGraw-Hill, 1951).

12. For discussions of these grand strategies and their evolution, see Barry R. Posen and Andrew L. Ross, "Competing Visions for US Grand Strategy," *International Security* 21, no. 3 (Winter 1996/97): 5–53, doi:10.2307/2539272; and Posen, *Restraint: A New Foundation*, 1–23.

13. This term is used to refer to an updated version of primacy in Posen, *Restraint: A New Foundation*. A recent article making the case for primacy calls it "deep engagement." Stephen G. Brooks, G. John Ikenberry, and William C. Wohlforth, "Don't Come Home, America: The Case against Retrenchment," *International Security* 37, no. 3 (Winter 2012/13): 7–51, http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00107.

14. See for example G. John Ikenberry, *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order* (Princeton, NJ: Princeton University Press, 2011), 9, 31, 36, 82, 191, 193, 310–12, 332, 359.

15. Ibid., 1–32, 159–220.

16. Brooks, Ikenberry, and Wohlforth, "Don't Come Home, America," 34. On the security dilemma, see Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214, http://dx.doi.org/10.2307/2009958.

17. See for example James B. Steinberg and Philip H. Gordon, "NATO Enlargement: Moving Forward; Expanding the Alliance and Completing Europe's Integration," Brookings Institution Policy Brief 90 (November 2001), http://www.brookings.edu/research/papers/2001/11/globalgovernance-gordon.

18. Brooks, Ikenberry, and Wohlforth, "Don't Come Home, America," 37. Theoretically, this follows from the fact the nuclear weapons make rivals less responsive to the hegemon's threats or allies less dependent on its protection. Primacists, however, typically offer other rationales for military efforts to stem proliferation.

19. Nuno Monteiro, "Unrest Assured: Why Unipolarity Is Not Peaceful," *International Security* 36, no. 3 (Winter 2011/12): 9–40, doi:10.1162/ISEC_a_00064.

20. Kaufmann, "Threat Inflation," 9–29; and John Prados and Christopher Ames, "The Iraq War—Part II: Was There Even a Decision? U.S. and British Documents Give No Indication Alternatives Were Seriously Considered," National Security Archive Electronic Briefing Book No. 328, 1 October 2010, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB328/index.htm.

21. This is rare point of partial agreement between neoconservatives and realists, who are generally skeptical of international institutions' virtues. John J. Mearsheimer, "The False Promise of International Institutions," *International Security* 19, no. 3 (Winter 1994/95): 5–49, http://mearsheimer.uchicago.edu/pdfs/A0021.pdf.

22. Liberal internationalists are not sticklers for international law so much as for seeming compliance with it or replacing that compliance with multilateral support. See for example Lee Feinstein and Anne-Marie Slaughter, "A Duty to Prevent," *Foreign Affairs* 83, no. 1 (January/February 2004): 136–50, doi:10.2307/20033835.

23. With the exception of an odd scholar here and there, that includes the American Enterprise Institute, Atlantic Council, Brookings Institution, Center for American Progress, Center for New American Security, Center for Strategic and Budgetary Assessments, Center for Strategic and International Studies, Council on Foreign Relations, Heritage Foundation, Hoover Institution, Hudson Institute, Manhattan Institute, New America Foundation, RAND Corporation, and the Third Way. Cato, where one of the authors works and the other worked, is an exception because it is libertarian. Other small liberal and libertarian think tanks also defy the consensus to varying degrees.

24. For the House and Senate, respectively, see https://www.govtrack.us/congress/votes/107-2002/s237 and https://www.govtrack.us/congress/votes/107-2002/h455. On the war debate, see Jane Kellet Cramer, "Militarized Patriotism: Why the US Marketplace of Ideas Failed before the Iraq War," *Security Studies* 16, no. 3 (July/September 2007): 489–524, http://dx.doi.org/10.1080/09636410701547949.

25. Even CIA Director George Tenet's famous "It's a slam dunk!" exclamation was about marketing. Tenet's remark came in response to President George W. Bush's concern that his administration's public argument that Iraq had weapons of mass destruction was insufficiently convincing, as opposed to concern about the claim's substance. Bob Woodward, *Plan of Attack* (New York: Simon & Schuster, 2004), 249–50.

26. A good source on this is Prados and Ames, "The Iraq War — Part II."

27. Woodward, *Plan of Attack*, 149–53.

28. Paul R. Pillar, "Intelligence, Policy, and the War in Iraq," *Foreign Affairs* 85, no. 2 (March/April 2006): 15–27, doi:10.2307/20031908.

29. Russ Hoyle, *Going to War: How Misinformation, Disinformation and Arrogance Led America to War in Iraq* (New York: St. Martin's, 2008), 228–33. For Scowcroft's take at the time, see Brent Scowcroft, "Don't Attack Saddam," *Wall Street Journal*, 15 August 2002, http://www.wsj.com/articles/SB1029371773228069195.

30. Fairness and Accuracy in Reporting, "In Iraq Crisis, Networks Are Megaphones for Official Views," 18 March 2003, http://fair.org/article/in-iraq-crisis-networks-are-megaphones-for-official-views/.

31. Quoted in Danny Postel, "Realistpolitik," *American Prospect*, 16 April 2004, http://prospect.org/article/realistpolitik.

32. On the impact of the wars' unpopularity, see John Mueller, "The Iraq Syndrome Revisited: U.S. Intervention, from Kosovo to Libya," *Foreign Affairs* (website), 28 March 2011, http://www.foreignaffairs.com/articles/67681/john-mueller/the-iraq-syndrome-revisited. On how debt and resulting spending caps contribute to this tendency, see Benjamin H. Friedman and Justin Logan, "Why the U.S. Military Budget Is 'Foolish and Sustainable,' " *Orbis* 56, no. 2 (Spring 2012): 177–91, http://dx.doi.org/10.1016/j.orbis.2012.01.003.

33. A brief critical review of these arguments around when they were made is Benjamin H. Friedman, "Six Bad Arguments for Bombing Libya," Cato-at-Liberty (blog), 29 March 2011, http://www.cato.org/blog/six-bad-arguments-bombing-libya.

34. An argument against the humanitarian rationale for the bombing campaign written as it occurred is: Alan J. Kuperman, "False Pretense for War in Libya?," *Boston Globe*, 14 April 2011, http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2011/04/14/false_pretense_for_war_in_libya/. A subsequent academic take by the same author is Alan J. Kuperman, "A Model Humanitarian Intervention? Reassessing NATO's Libya Campaign," *International Security* 38, no. 1 (Summer 2013): 105–36, doi:10.1162/ISEC_a_00126.

35. A short discussion of some relevant political science is Stephen M. Walt, "Social Science and the Libyan Adventure," foreignpolicy.com, 24 March 2011, http://foreignpolicy.com/2011/03/24/social-science-and-the-libyan-adventure/. See also Alexander B. Downes and Jonathan Monten, "Forced to Be Free: Why Foreign-Imposed Regime Change Rarely Leads to Democratization," *International Security* 37, no. 4 (Spring 2013): 90–131, doi:10.1162/ISEC_a_00117.

36. Ivo H. Daalder and James G. Stavridis, "NATO's Victory in Libya: The Right Way to Run an Intervention," *Foreign Affairs* 91, no. 2 (March/April 2012): 2–7, http://www.jstor.org/stable/23217215; Anne-Marie Slaughter, "Why Libya Skeptics Were Proved Badly Wrong," *Financial Times*, 24 August 2011, http://www.ft.com/cms/s/0/18cb7f14-ce3c-11e0-99ec-00144feabdc0.html; and Anne-Marie Slaughter, "Syrian Intervention Is Justifiable, and Just," *Washington Post*, 8 June 2012, https://www.washingtonpost.com/opinions/syrian-intervention-is-justifiable-and-just/2012/06/08/gJQARHGjOV_story.html?utm_term=.b78cef5cb099.

37. Dick Cheney and Liz Cheney, *Exceptional: Why the World Needs a Powerful America* (New York: Simon & Schuster, 2015), 231–55.

38. Obama criticized the foreign policy establishment focus on credibility in a recent interview. Jeffrey Goldberg, "The Obama Doctrine," *The Atlantic*, April 2016, http://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/.

39. On neoconservatives, see for example James Carden, "Donald Trump Is Alienating Neoconservatives—and Antiwar Democrats Should Worry," *The Nation*, 7 March 2016, http://www.thenation.com/article/donald-trump-is-alienating-neoconservatives-and-anti-war-democrats-should-worry/; and Brianna Gurciullo, "Graham Rips Trump's 'Nonsensical' Foreign Policy Speech," *Politico*, 27 April 2016, http://www.politico.com/blogs/2016-gop-primary-live-updates-and-results/2016/04/lindsey-graham-donald-trump-foreign-policy-222549.

An example of a liberal internationalist denunciation is Thomas Wright, "Trump's 19th Century Foreign Policy," *Politico Magazine*, 20 January 2016, http://www.politico.com/magazine/story/2016/01/donald-trump-foreign-policy-213546. For an argument that Trump's views are less abnormal than Wright contends, see Joshua Shrifrinson, "Trump's Foreign Policy Views Are Actually Pretty Mainstream," *Washington Post*, 4 February 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/02/04/the-secret-behind-donald-trumps-antiquated-foreign-policy-views-theyre-pretty-mainstream/.

40. Joshua W. Busby and Jonathan Monten, "Republican Elites and Foreign Policy Attitudes," *Political Science Quarterly* 127, no. 1 (Spring 2012): 105–42, doi:10.1002/j.1538-165X.2012.tb00722.x.

41. Quoted in Michael A. Cohen, "Can't We All Just Not Get Along? Why the Push for Bipartisan Consensus in Foreign Policy is a Dumb Idea" *Foreign Policy*, 22 June 2012, http://foreignpolicy.com/2012/06/22/cant-we-all-just-not-get-along-2/.

42. On balancing, see Jack S. Levy, "What do Great Powers Balance against and When?," in *Balance of Power Theory in the 21st Century*. ed. T.V. Paul, James J. Wirtz, and Michel Fortman (Stanford: Stanford University Press, 2004), 19–51; Stephen M. Walt, *The Origins of Alliances* (Ithaca, NY: Cornell University Press, 1987), 17–49; and Randall L. Schweller, "Unanswered Threats: A Neoclassical Realist Theory of Underbalancing," *International Security* 29, no. 2 (Fall 2004): 159–201, doi:10.1162/0162288042879913. On the stability of balances of power, see Dan Reiter, "Exploding the Power Keg Myth: Preemptive Wars Almost Never Happen," *International Security* 20, no. 2 (Fall 1995): 5–34, doi:10.2307/2539227; Randall Schweller, "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies* 5, no. 3 (Spring 1996): 90–121, http://dx.doi.org/10.1080/09636419608429277; Robert S. Ross, "The Geography of the Peace: East Asia in the Twenty-first Century," *International Security* 23, no. 4 (Spring 1999): 81–118, doi:10.1162/isec.23.4.81; and Marc Trachtenberg, "The Question of Realism," *Security Studies* 13, no. 1 (Fall 2003): 156–94, http://dx.doi.org/10.1080/09636410490493877. On the limited danger most wars pose to the United States, see Eugene Gholz and Daryl G. Press, "The Effects of Wars on Neutral Countries: Why It Doesn't Pay to Preserve the Peace," *Security Studies* 10, no. 4 (Summer 2001): 1–57, http://dx.doi.org/10.1080/09636410108429444.

43. Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989); and Kenneth N. Waltz, "Nuclear Myths and Political Realities," *American Political Science Review* 84, no. 3 (September 1990): 731–45, doi:10.2307/1962764.

44. On the robustness of trade, see Gholz and Press, "Effects of Wars," 5–15.

45. See for example Donald Kagan, Gary James Schmitt, and Thomas Donnelly, *Rebuilding America's Defenses, Strategy, Forces and Resources For a New Century* (Washington, DC: Project for the New American Century, 2000), 1–14.

46. For competing explanations, see John Mueller, *Retreat from Doomsday: The Obsolescence of Major War* (New York: Basic Books, 1989); Carl Kaysen, "Is War Obsolete? A Review Essay," *International Security* 4, no. 14 (Spring 1990): 42–64, doi:10.2307/2538750; and Stephen Van Evera, "Primed for Peace: Europe after the Cold War," *International Security* 15, no. 3 (Winter 1990/91): 7–57, doi:10.2307/2538906. A good survey of theories predicting peace is Steven Pinker, *The Better Angels of Our Nature: Why Violence Has Declined* (New York: Penguin, 2011), 267–94.

47. On the capitalist peace, see Erik Gartzke, "The Capitalist Peace," *American Journal of Political Science* 51, no. 1 (2007): 166–91, http://www.jstor.org/stable/4122913; and Patrick J. McDonald, *The Invisible Hand of Peace: Capitalism, The War Machine, and International Re-*

lations Theory (Cambridge, UK: Cambridge University Press, 2009). One source of academic support for primacy, which its Washington supporters typically ignore, is hegemonic stability theory. See for example Robert Keohane, *After Hegemony: Cooperation and Discord in the World* (Princeton, NJ: Princeton University Press, 1984).

48. Jeffrey Pickering and Mark Peceny, "Forging Democracy at Gunpoint," *International Studies Quarterly* 50, no. 3 (Fall 2006): 539–60, http://www.jstor.org/stable/4092792; and Bruce Bueno de Mesquita and George W. Downs, "Intervention and Democracy," *International Organization* 60, no. 3 (Summer 2006): 627–49, http://www.jstor.org/stable/3877822.

49. See for example Paul Huth and Bruce Russett, "What Makes Deterrence Work? Cases from 1900 to 1980," *World Politics* 36, no. 4 (July 1984): 496–526, doi:10.2307/2010184; Daryl G. Press, *Calculating Credibility: How Leaders Evaluate Military Threats* (Ithaca, NY: Cornell University Press, 2005); and Jonathan Mercer, *Reputation and International Politics* (Ithaca, NY: Cornell University Press, 2010).

50. Justin Logan and Christopher Preble, "Fixing Failed States: A Dissenting View," in *The Handbook on the Political Economy of War*, ed. Christopher J. Coyne and Rachel L. Mathers (Cheltenham, UK: Edward Elgar, 2011), 379–96; Stewart Patrick, " 'Failed' States and Global Security: Empirical Questions and Policy Dilemmas," *International Studies Review* 9, no. 4 (Winter 2007): 644–62, http://www.jstor.org/stable/4621865; and Jennifer Keister, "The Illusion of Chaos: Why Ungoverned Spaces Aren't Ungoverned, and Why That Matters," Cato Policy Analysis 766 (December 2014), http://object.cato.org/sites/cato.org/files/pubs/pdf/pa766_1.pdf.

51. Posen, *Restraint: A New Foundation*, 50–54.

52. Brooks, Ikenberry, and Wohlforth, "Don't Come Home, America." Our response is Campbell Craig, Benjamin H. Friedman, Brendan Rittenhouse Green, Justin Logan, Stephen G. Brooks, G. John Ikenberry, and William C. Wohlforth, "Debating American Engagement: The Future of US Grand Strategy," *International Security* 38, no. 2 (Fall 2013): 183–92, doi:10.1162/ISEC_c_00140.

53. According to a recent article by three academics that support primacy, "most scholars who write on the future of US grand strategy" oppose primacy. See Brooks, Ikenberry, and Wohlforth, "Don't Come Home, America," 7.

54. Daniel Maliniak, Amy Oakes, Susan Peterson, and Michael J. Tierney, "The View from the Ivory Tower: TRIP Survey of International Relations Faculty in the United States and Canada" (Williamsburg, VA: College of William and Mary, February 2007), https://www.wm.edu/offices/itpir/_documents/trip/ivory_tower_view_2007.pdf.

55. Quoted in Dylan Matthews, "Scholarly Critique," *CampusProgress.org*, 4 November 2009, http://www.campusprogress.org/fieldreport/4769/scholarly-critique.

56. Susan Peterson, Michael J. Tierney, and Daniel Maliniak, "Teaching and Research Practices, Views on the Discipline, and Policy Attitudes of International Relations Faculty at U.S. Colleges and Universities" (Williamsburg, VA: College of William and Mary, August 2005), https://www.wm.edu/offices/itpir/_documents/trip/trip_summary2005.pdf.

57. Richard Jordan, Daniel Maliniak, Amy Oakes, Susan Peterson, and Michael J. Tierney, "One Discipline or Many? TRIP Survey of International Relations Faculty in Ten Countries" (Williamsburg, VA: College of William and Mary, February 2009), 88, http://www.wm.edu/offices/itpir/_documents/trip/final_trip_report_2009.pdf.

58. Office of Management and Budget, *US Budget for Fiscal Year 2011*, Table 6.1, http://www.gpoaccess.gov/usbudget/fy11/sheets/hist06z1.xls.

59. Prominent examples are Charles Krauthammer, "The Unipolar Moment," *Foreign Affairs* 70, no. 1 (Winter 1990/91): 23–33, doi:10.2307/20044692; William Kristol and Robert Kagan, "Toward a Neo-Reaganite Foreign Policy," *Foreign Affairs* 75, no. 4 (July/August 1996):

18–32, doi:10.2307/20047656; and Kurt M. Campbell and Michelle A. Flournoy, *The Inheritance and the Way Forward* (Washington, DC: Center for New American Security, 2007), 26–27.

60. Brooks, Ikenberry, and Wohlforth, "Don't Come Home, America"; Samuel P. Huntington, "Why International Primacy Matters," *International Security* 17, no. 4 (Spring 1993): 68–83, doi:10.2307/2539022.

61. Christopher DeMuth, until recently the head of the American Enterprise Institute, now a senior fellow at the Hudson Institute, remarked that "at the think tank we are working without the simplifying assumptions and the explanatory parsimoniousness that are the hallmarks of academic research." This comment is emblematic of views pundits and Washington analysts who claim to avoid theory. One can form opinions about foreign policy with good or bad theory, implicit or explicit theory, but not with none. See remarks of Christopher DeMuth at "Are Think Tanks Becoming Too Political?," Hudson Institute Forum, 16 February 2012, https://www.c-span.org/video/?304465-1/role-think-tanks-public-policy, http://www.hudson.org/events/922-are-think-tanks-becoming-too-political-22012.

62. The elites are "leaders" the pollsters identified and polled in various fields. The authors describe these results as follows: "Large majorities of leaders and the public say that strong US leadership in the world is at least somewhat desirable. But there is a great difference between leaders and the public in degree or emphasis. At least six in ten leaders (57% of Independent leaders, 70% of Democratic leaders, and 90% of Republican leaders) say it is 'very desirable' for the United States to exert strong leadership in world affairs, compared to just over one-third of the public (37%). Similarly, a much larger portion of leaders (94% Republicans, 97% Democrats, and 92% Independents) than of the public (58%) thinks it will be best for the future of the country if the United States takes an active part in world affairs." Dina Smeltz, Joshua Busby, Gregory Holyk, Craig Kafura, Jonathan Monten, and Jordan Tama, *United in Goals, Divided on Means: Opinion Leaders Survey Results and Partisan Breakdowns from the 2014 Chicago Survey of American Opinion on U.S. Foreign Policy* (Chicago: Chicago Council on Global Affairs, 2015), 6, http://www.thechicagocouncil.org/sites/default/files/2014%20Chicago%20Council%20Opinion%20Leaders%20Survey%20Report_FINAL.pdf.

63. Ibid., 8, 22.

64. An example is Marshall M. Bouton and Benjamin J. Page, *The Foreign Policy Disconnect: What Americans Want from Our Leaders but Don't Get* (Chicago: University of Chicago Press, 2006).

65. Pew Survey of the General Public, 28 October–9 November 2009. Question: "Over the next year, do you think the number of U.S. troops in Afghanistan should be—kept the same increased, decreased, or as it is now?," http://www.people-press.org/files/legacy-pdf/569.pdf.

66. Pew Survey of Council on Foreign Relations (CFR) Members, 2 October–16 November 2009. Question: "Over the next year, do you think the number of U.S. troops in Afghanistan should be—kept the same increased, decreased, or as it is now?," http://www.people-press.org/files/legacy-pdf/569.pdf. The poll does show, on the other hand, a public more willing than CFR members to bomb Iran should it acquire nuclear weapons.

67. Smeltz, Busby, Holyk, Kafura, Monten, and Tama, "United in Goals," 12.

68. John Mueller, "Syria: It Wasn't Isolationism," *The National Interest*, 14 October 2013, http://nationalinterest.org/commentary/syria-it-wasnt-isolationism-9231; and Smeltz, Busby, Holyk, Kafura, Monten, and Tama, "United in Goals," 14.

69. Adam J. Berinsky, "Assuming the Costs of War: Events, Elites, and American Public Support for Military Conflict," *Journal of Politics* 69, no. 4 (November 2007): 975–97, doi:10.1111/j.1468-2508.2007.00602.x; and Daniel W. Drezner, "The Realist Tradition

in US Public Opinion," *Perspectives on Politics* 6, no. 1 (March 2008): 51–70, doi:10.1111/j.1468-2508.2007.00602.x.

70. Anthony Downs, *An Economic Theory of Democracy* (New York: Harper and Row, 1957), 244–6, 298.

71. Bouten and Page, *The Foreign Policy Disconnect*, 171–73, 243–4; and Thomas Knecht, *Paying Attention to Foreign Affairs: How Public Opinion Affects Presidential Decision Making* (University Park, PA: Pennsylvania University Press, 2010), 9–36.

72. On how conscription decreases war support, see Michael C. Horowitz and Matthew C. Levendusky, "Drafting Support for War: Conscription and Mass Support for Warfare," *Journal of Politics* 73, no. 2 (April 2011): 524–34, doi:10.1017/s0022381611000119; and Robert S. Erikson and Laura Stoker, "Caught in the Draft: The Effects of Vietnam Draft Lottery Status on Political Attitudes," *American Political Science Review* 105, no. 2 (May 2011): 221–37, http://www.jstor.org/stable/41495063.

73. This argument is consistent with realism. Realism sees rival power, or appreciation of its possibility, as the source of restraint in both domestic and international politics. For a classic and modern example, see Hans Morgenthau, *Politics among Nations* (New York: Knopf, 1971), 219; and Robert Jervis, "Unipolarity: A Structural Perspective," *World Politics* 61, no. 1 (January 2009): 188–213, muse.jhu.edu/article/260516/pdf.

74. Barry Posen, "Command of the Commons: The Military Foundations of US Hegemony," *International Security* 28, no. 1 (Summer 2003): 5–46, http://www.jstor.org/stable/4137574.

75. Richard K. Betts, "The Political Support System for American Primacy," *International Affairs* 81, no. 1 (January 2005): 1–14, http://www.jstor.org/stable/3569185.

76. Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge, MA: Harvard University Press, 1971), 132–67; and Robert Dahl, *A Preface to Democratic Theory* (Chicago: University of Chicago Press, 1956), 124–51.

77. John Mueller, "The Iraq Syndrome," *Foreign Affairs* 84, no. 6 (November/December 2005): 44–54, doi:10.2307/20031775. A discussion of these dynamics is in Benjamin H. Friedman, "Alarums and Excursions: Explaining Threat Inflation in US Foreign Policy," in *A Dangerous World? Threat Perception in US National Security*, ed. Christopher A. Preble and John Mueller (Washington, DC: Cato Institute, 2014), 281–303. On how liberal democracy's checks and balances improve foreign policies, see Kenneth Waltz, *Foreign Policy and Democratic Politics: The American and British Experience* (Boston: Little, Brown, 1967), 267–311.

78. This alignment of interests is like the log-rolling described in Jack Snyder, *Myths of Empire: Domestic Politics and International Ambition* (Ithaca, NY: Cornell University Press, 1991), 17–19, 43–54.

79. Steven P. Rosen, "Testing the Theory of the Military-Industrial Complex," in *Testing the Theory of the Military Industrial Complex*, ed. Steven P. Rosen (Lexington, MA: Lexington Books, 1973), 23–24.

80. Gordon Adams, *The Politics of Defense Contracting: The Iron Triangle* (New York: Council on Economic Priorities, 1981), 17–45. On sectional economic interests in US foreign policy making, see Peter Trubowitz, *Defining the National Interest: Conflict and Change in American Foreign Policy* (Chicago: University of Chicago Press, 1998), 1–30.

81. Warner Schilling, "The Defense Budget of 1950," in *Strategy, Politics, and Defense: Budgets*, ed. Warner Schilling, Paul Y. Hammond, and Glenn H. Snyder, (New York and London: Columbia University Press, 1962), 19–27.

82. Louis Fisher, "Presidential Power in National Security," in *Understanding the Presidency*, 6th ed., ed. James P. Pfiffner and Roger H. Davidson (Boston: Pearson, 2011), 379–93.

83. Arnold Wolfers, *Discord and Collaboration: Essays on International Politics* (Baltimore: Johns Hopkins University Press, 1962), 13–15; Posen, *Sources of Military Doctrine*, 59–80; and Robert Jervis, "US Grand Strategy: Mission Impossible," *Naval War College Review* 51, No. 3 (Summer 1998): 22–34, http://search.proquest.com/openview/ca96e436d2a1d7b7ecc8113780f5ed24/1?pq-origsite=gscholar.

84. Richard E. Neustadt, *Presidential Power and the Modern: The Politics of Leadership from Roosevelt to Reagan*, Revised Edition (New York: New York Free Press, 1991), 29–49.

85. Benjamin H. Friedman, "Austerity and US Grand Strategy Reform: Not Enough of a Bad Thing" (paper presented at the International Studies Association Conference, New Orleans, February 2015).

86. Christopher Layne, *Peace of Illusions, American Grand Strategy from 1940 to the Present* (Ithaca, NY: Cornell University Press, 2007), 51–70.

87. On this dynamic in another context see Cass Sunstein, *Risk and Reason: Safety, Law, and the Environment* (Cambridge, UK: Cambridge University Press, 2004), 78–99.

88. Donald E. Abelson, *Do Think Tanks Matter? Assessing the Impact of Public Policy Institutes* (Montreal: McGill-Queens University Press, 2002), 60.

89. These functions might be further divided to include help with agenda setting, evaluation of options, enactment, implementation, and monitoring of policies. Andrew Rich, *Think Tanks, Public Policy, and the Politics of Expertise* (Cambridge, UK: Cambridge University Press, 2004), 107–8.

90. Jeremy Shapiro, "Who Influences Whom? Reflections on US Government Outreach to Think Tanks," Brookings Institution, 4 June 2014, http://www.brookings.edu/blogs/up-front/posts/2014/06/04-us-government-outreach-think-tanks-shapiro.

91. John W. Kingdon, *Agendas, Alternatives, and Public Policies*, 2nd ed. (New York: Longman, 1995), 145–64; and Jeffrey W. Legro, *Rethinking the World: Great Power Strategies and International Order* (Ithaca, NY: Cornell University Press, 2005), 13–38.

92. It is cognitively easier to respond to disconfirming evidence by rejecting the evidence than updating one's belief. Robert Jervis, "Bridges, Barriers, and Gaps: Research and Policy," *Political Psychology* 29, no. 4 (August 2008): 587, http://www.jstor.org/stable/20447145.

93. Theodore Lowi, *The End of Liberalism*, 40th Anniversary Ed. (New York: W. W. Norton, 2009), 127–63.

94. Thomas Medvetz, *Think Tanks in America* (Chicago: University of Chicago Press, 2012), 130–80.

95. Senator Olympia Snowe, quoted in Ezra Klein, "Unpopular Mandate: Why Do Politicians Reverse Their Positions?" *New Yorker*, 25 June 2012, http://www.newyorker.com/magazine/2012/06/25/unpopular-mandate.

96. Emily Stokes, "Lunch with the Financial Times: Rory Stewart," *Financial Times*, 1 August 2009, http://www.ft.com/cms/s/0/c7414148-7d60-11de-b8ee-00144feabdc0.html#axzz2RBy5pMdZ. Bernard Brodie had something similar in mind when he wrote: "If there is one practically unvarying principle about the use within the government of outside experts as consultants, it is that they must be known to be friendly to that policy on which they are being consulted. They may be critical of details or of the current execution of that policy, but not of the fundamentals." Bernard Brodie, *War and Politics* (New York: Macmillan Publishing Co., 1973), 214. Likewise, Aaron Wildavsky writes, "The first requirement of effective policy analysis is that top management wants it." Wildavksy, "Rescuing Policy Analysis from PPBS." 197.

97. On the formation of FFRDCs, see Harvey M. Sapolsky, "Inventing Systems Integration," in *The Business of Systems Management*, ed. Andrea Prencipe and Andrew Davies, (Oxford, UK: Oxford University Press, 2003), 15–34.

98. Ken Silverstein, "The Bipartisan Lobbying Center: How a Washington Think Tank Advocates for Political Unity—and its Top Donors," Edmund J. Safra Center for Ethics, Harvard University, http://ethics.harvard.edu/blog/bipartisan-lobbying-center; and Ken Silverstein, "The Secret Donors behind the Center for American Progress and Other Think Tanks," *The Nation*, 21 May 2013, http://www.thenation.com/article/secret-donors-behind-center-american-progress-and-other-think-tanks-updated-524.

99. A recent article on the topic is Eric Lipton and Brooke Williams, "How Think Tanks Amplify Corporate America's Influence, *New York Times*, 7 August 2016, http://www.nytimes.com/2016/08/08/us/politics/think-tanks-research-and-corporate-lobbying.html. See also Lee Fang, "Emails Show Close Ties between Heritage Foundation and Lockheed Martin," *The Intercept*, 15 September 2015, https://theintercept.com/2015/09/15/heritage-foundation/.

100. Aaron Wildavsky, "The Self-Evaluating Organization," *Public Administration Review* 32, no. 5 (September/October 1972): 509–20, doi:10.2307/975158.

101. Eric Lipton, Brooke Williams, and Nicholas Confessore, "Foreign Powers Buy Influence at Think Tanks," *New York Times*, 6 September 2014, http://www.nytimes.com/2014/09/07/us/politics/foreign-powers-buy-influence-at-think-tanks.html.

102. A critique of such focus is in Benjamin H. Friedman, Harvey M. Sapolsky, and Christopher Preble, "Learning the Right Lessons from Iraq," Cato Institute Policy Analysis 610, (February 2008), http://object.cato.org/sites/cato.org/files/pubs/pdf/pa-610.pdf.

103. Leslie H. Gelb with Jeanne-Paloma Zelmati, "Mission Not Accomplished," *Democracy*, no. 13 (Summer 2009): 24, http://democracyjournal.org/magazine/13/mission-not-accomplished/.

104. Mai Elliott, *RAND in Southeast Asia: A History of the Vietnam War Era* (Santa Monica, CA: RAND Corporation, 2010), 28, http://www.rand.org/pubs/corporate_pubs/CP564.html.

105. Two prominent exceptions who were associated with RAND, Daniel Ellsberg and Bernard Brodie, turned against the war as their ambitions of serving in high government office ebbed (a formulation deliberately free of causality). Fred Kaplan, *The Wizards of Armageddon* (Stanford, CA: Stanford University Press, 1983), 337–42.

106. Morgenthau, "The Purpose of Political Science," 73–79.

107. Programs with this aim include the "Bridging the Gap" program cosponsored by American University, UC-Berkeley, and Duke University, funded by the Carnegie Corporation of New York, and the Tobin Project.

108. Walt, "Rigor or Rigor Mortis?," 46; Joseph S. Nye Jr., "Scholars on the Sidelines," *Washington Post*, 13 April 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/04/12/AR2009041202260.html; Paul Avey and Michael Desch, "What Do Policymakers Want From Us? Results of a Survey of Current and Former Senior National Security Decision-makers," *International Studies Quarterly* 58, no. 4 (December 2014): 227–46, http://dx.doi.org/10.1111/isqu.12111; and Michael Desch, "Technique Trumps Relevance: the Professionalization of Political Science and the Marginalization of Security Studies," *Perspectives on Politics* 13, no. 2 (June 2015): 377–93, http://dx.doi.org/10.1017/S1537592714004022.

109. Walt, "Where do Bad Ideas Come From?"

110. Owen R. Cote Jr., "The Politics of Innovative Military Doctrine: The US Navy and Fleet Ballistic Missiles" (PhD diss., Massachusetts Institute of Technology, 1996), 166–243, http://hdl.handle.net/1721.1/11217.

111. Michael Desch, "Is a Grand Strategy of Restraint Politically Viable?" (lecture, Institute of World Politics, Notre Dame University, 27 May 2015), http://www.iwp.edu/news_publications/detail/transcript-is-a-grand-strategy-of-restraint-politically-viable-with-michael

-desch; and Lawrence F. Kaplan, "Springtime for Realism," *The New Republic*, 21 June 2004, http://www.newrepublic.com/article/springtime-realism.

112. Friedman and Logan, "Why the U.S. Military Budget Is 'Foolish and Sustainable,' " 89.

113. This is consistent with Weber's idea that science's responsibility is to help frame political choices but not to direct them. Max Weber, "Science as a Vocation," in *From Max Weber: Essays in Sociology*, trans. H. H. Gerth and C. Wright Mills (New York: Oxford University Press, 1946), 129–56.

114. Kingdon, *Agendas, Alternatives*; Legro, *Rethinking the World.*

115. Friedman, "Alarums and Excursions," 302–3.

Liberating Cyber Offense

James E. McGhee

Abstract

Offensive cyber operations are increasingly an important part of our national defense and provide commanders with unique capabilities to thwart enemy attacks. Conducting cyber operations, however, is not as simple as pushing a button on a keyboard. Challenges involving cyber operations frustrate operators and commanders alike. Four specific problem areas exist, but certain recommended changes can assist operators and commanders to more efficiently conduct cyber operations.

* * * * *

The Department of Homeland Security (DHS) runs a national clearinghouse of cyber-threat information known as the US Computer Emergency Readiness Team (US-CERT). Part of its job is to track cyber incidents, which could include unauthorized attempts to access a network, distributed-denial-of-service (DDoS) attacks, or other nefarious behavior. According to data from a 2013 review, US-CERT received almost 12,000 cyber incident reports in 2007. By 2009 that number had more than doubled—and it quadrupled by 2012.[1] According to the Pentagon's Cybersecurity Culture and Compliance Initiative memo, between September 2014 and June 2015, Department of Defense (DOD) networks experienced 30 million known malicious cyber intrusions. That translates to 3 million attacks per month or 100,000 per day.[2] While these statistics are stunning, they are not news. Most articles discussing cyber incidents sound the klaxon regarding US ability to prevent a cyber Pearl Harbor but do not discuss the difficulty of executing cyber operations. Other articles that discuss cyber operations talk about cyber attack as any garden-variety cyber operation, even those that are not actual attacks. Such articles conflate incidents below the use-of-force threshold

---

James E. McGhee is currently the legal advisor for Special Operations Command North. He graduated from the University of Pittsburgh School of Law in 2000 and served eight years as an Army JAG officer before becoming the Assistant US Attorney in Tucson, Arizona. McGhee previously served as operational law attorney for the Twenty-Fourth Air Force.

with actual use-of-force operations considered an armed attack. Their authors believe every cyber incident is a cyber attack and say things such as, "We're dropping cyber bombs."[3] Those articles also presume cyber operations are easy to do, perhaps too easy. The authors seem to gloss over the "how to," making it appear as if the DOD can simply "launch" a cyber capability whenever it chooses. The current reality is that offensive cyber operations are difficult; adding to the problem are unnecessary restrictions, limitations, and ambiguity. The United States can reach a point where conducting offensive cyber operations becomes easy and quick, but only if there are fewer restrictions and constraints. This article presents some of the challenges that create hardships in offensive cyber operations and offers recommendations to liberate the cyber offense.

Several questionable restrictions regarding offensive cyber operations decrease effectiveness and efficacy of cyber capabilities. First, offensive cyber operations require high-level (presidential or secretary of defense in most cases) approval authority before they can be used. This is true even in emergency defensive situations when existing, approved defenses against cyber threats will not suffice. Even so, such an emergency response still requires multiagency coordination to make such a determination in the first place. Second, it is generally impractical to use offensive cyber operations because, contrary to the speed at which they are carried out, planning these operations generally takes more time than planning conventional, kinetic operations. Third, even though we mistakenly conflate cyber operations with kinetic operations and place more restrictions on cyber offense, clearly cyber has different effects. We also use different cyber definitions throughout the government to describe the same things. These terms are ambiguous and lead to misunderstandings about the efficacy of cyber offense. Finally, confusion remains regarding who is actually in charge of the response in the event of a cyber "attack" against the United States.

Despite each of these issues, cyber offensive operations can be liberated and become quite useful with certain changes and recommendations.

High-Level Approvals

In accordance with the 2015 DOD Cyber Strategy, the DOD has three primary cyber missions. First, the DOD must defend its own networks, systems, and information. Second, the DOD must be prepared to defend the United States and its interests against cyber attacks of

significant consequence. To this end, "if directed by the president or the secretary of defense, the US military may conduct cyber operations to counter an imminent or on-going attack against the US homeland or US interests in cyberspace." Third, if directed by the president or the secretary of defense, the DOD must be able to provide integrated cyber capabilities to support military operations and contingency plans.[4]

The approval authority for any cyber operation that goes outside of a DOD network is very high. Corresponding approval authorities for kinetic operations is much lower. For instance, if a joint force commander wanted to disrupt the power in a large area, he could attack a power plant being used by the enemy in several ways, such as sending in a team to sabotage it, calling in an airstrike, firing a missile, or asking for a cyber operation. The first three courses of action are quick and relatively easy. The commander can likely take those actions at his or her level. The cyber operation, however, can only be used if an execute order (EXORD) authorized cyber operations, that particular power plant was already on a cyber targeting list, the cyber operators already performed appropriate operational preparation of the environment (OPE) on the power plant's network, and interagency and possibly international deconfliction had taken place.

Absent an EXORD authorizing offensive cyber operations, agencies must request specific use of cyber capabilities through the review and approval process for cyber operations (RAPCO).[5] RAPCO applies to cyberspace operations requiring presidential or secretary of defense approval for deployment and initial or ongoing employment. This process takes time, and, due to the interagency nature, it often gets bogged down—ultimately resulting in the request being overcome by events or bypassed in lieu of kinetic operations. While kinetic operations also require an EXORD, additional authorizations are much easier and faster to obtain, as are delegations of authority, if need be.

Offensive cyber operations are difficult even with an EXORD or RAPCO approval. They still require OPE time, coordination, and deconfliction, and there is no guarantee the deconfliction will go smoothly. One of the partners can object, shuttering the whole process. Additionally, planners run into an attribution problem. Perhaps we can discern that the cyber intrusion is emanating from country X, but that does not tell us whether country X is behind the act or whether it is a criminal or

rogue element. Perhaps the best one can hope for is to sever the command and control to stop the event.

Long Planning Times

Preparing and using offensive cyber operations is not a static process. The careful planning required can be lengthy and detailed in nature. Even if an EXORD and valid rules of engagement exist, authorizing cyber operations, target approval, and deconfliction must still be accomplished, which takes more time than conventional kinetic operations. For instance, some examples of preparatory cyber operations may include "reconnaissance (e.g., mapping a network), seizure of supporting positions (e.g., securing access to key network systems or nodes), and pre-emplacement of capabilities or weapons (e.g., implanting cyber access tools or malicious code)."[6] While we may have some number of cyber capabilities "on the shelf," their operational use requires much more than simply loading them and sending them on their way. Our operators must first know and understand the target network, node, router, server, and switch before using any cyber capability against them. However, to conduct such preparatory work still requires operators being told to do so in the first place.

Cyber planners must also consider collateral second- and third-order effects, outlining not only what the capability will do against the target but also what may happen further down the chain, to comply with the principle of distinction. However, the cyber-targeting analysis is different for the principle of proportionality.[7] In assessing incidental injury or damage, remote harms and lesser forms of harm—such as mere inconveniences or temporary losses—need not be considered in applying the proportionality rule. In the case of a power plant supporting civilian infrastructure, this can mean outlining effects against unintended targets, including hospitals, religious sites, orphanages, or other places that might be on a restricted or no-strike target list. This can require weeks or months of accessing, probing, and mapping. While some OPE is also required for kinetic weapons, the time frame for such conventional targeting is reduced to hours or days and in some circumstances mere minutes. Static targets, targeted via kinetic strikes, normally do not change. Once on a targeting list, they are likely to stay on the list. The same is not necessarily true for cyber targets. Networks, servers, routers, and so forth change all the time; they are updated and patched to keep

up with security threats—and sometimes are simply turned off. Moreover, their use can change, too, from strictly military to civilian, resulting in heightened potential for collateral damage. This requires constant OPE to make any required changes to the offensive cyber operation. It is somewhat ironic, then, that offensive cyber operations, which move at the speed of light, require such long prep times and lead some commanders to balk at using cyber operations.

Restrictive Cyber Rules

Equating offensive cyber operations with kinetic operations, in theory, should make use easier. On the one hand, we tend to treat them the same and apply the same rules to their use, but on the other hand, we treat cyber differently, making it harder to actually use it. If they are truly the same and the same rules apply, then why the vast differences in their actual use? This is especially true if we accept that cyber operations are merely one tool among many, including kinetic tools, which a commander may legally use against valid targets. To be sure, "cyber operations, many military experts and scholars have said, will likely be used as a tool in conjunction with larger, more conventional military efforts in future conflicts."[8] Moreover, using cyber operations in lieu of kinetic options is likely cleaner and more apt to comply with the laws of war (LOW), which should in fact call for greater use. The DOD *LOW Manual* states

> In some cases, cyber operations that result in non-kinetic or reversible effects can offer options that help minimize unnecessary harm to civilians. In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effect at all.[9]

Using the previous example, if the commander decides to blow up the power plant via a kinetic operation, it is likely completely destroyed. If he chooses the cyber option, it can merely be turned off or taken off-line without any physical damage or destruction. Additionally, the offensive cyber option may likely be reversible, which makes it much easier to turn the power back on. This is an important consideration, because if previous experiences are any indication, the United States will likely end up replacing the damaged infrastructure and correcting any resulting

damage from second- and third-order effects. A cyber operation actually allows a joint force commander more control to limit effects.

While some of the same old rules may apply equally to both cyber operations and kinetic operations, it is not true that they apply in the same ways. In 2012 Harold Koh, legal advisor to the Department of State, gave a speech at the US Cyber Command (USCYBERCOM) Inter-Agency Legal Conference wherein he ostensibly declared US policy regarding cyber operations and international law. His speech has since become the standard for US cyber operations policy, and much of what he presented has largely been codified in the recently released *LOW Manual.* In that speech, he answered 10 questions regarding cyber operations and international law. Koh said that "cyber activities will sometimes constitute a use of force under Article 2(4) of the UN Charter and customary international law." He then gave several examples, including cyber activities that proximately result in death, injury, or significant destruction, such as operations triggering a nuclear plant meltdown, opening a dam above a populated area causing destruction, and disabling air traffic control, resulting in airplane crashes. In other words, "If the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force." Koh also reaffirmed the proposition that the United States would, "when warranted, respond to hostile acts in cyberspace as we would to any other threat to our country."[10]

Koh also asserted that "there is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality."[11] For instance, "Operations that target an adversary's cyberspace capabilities, but are not achieved in or through cyberspace, would not be considered cyber operations."[12] These include bombing a network hub or jamming wireless communications.[13] In other words, it is more efficient and quicker to just drop a bomb on the adversary's network hub or other target than to disable or disrupt it via a cyber operation. Koh acknowledged, "There are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by 'force.'"[14] Nonetheless, we continue to equate offensive cyber operations with kinetic operations and have yet to engage in a robust discussion of what we mean by *force* regarding those cyber actions that do not have those clear kinetic parallels. Even cyber actions

that do have clear kinetic parallels still have much greater restrictions than kinetic actions. It is also somewhat ironic that a kinetic operation and a cyber operation may result in the exact same overall effect—lack of power, for instance—but the kinetic strike, which causes clear damage, destruction, and probably even death (not just to the enemy but collateral as well), has fewer restrictions than the cyber operation. The result of these added restrictions is that we are essentially forcing a law-of-armed-conflict (LOAC) analysis on cyber operations, falling well below the use-of-force/armed-attack threshold, when none is needed. This forces planners and operators to seek unnecessary authorizations and to consider unnecessary factors.

Ambiguous Definitions and Misunderstandings

Ambiguous definitions that lead to a lack of understanding of cyber utility exacerbate the disconnect between offensive cyber operations and kinetic operations. Within the DOD we have a common set of definitions regarding cyber operations, which are found in Joint Publication (JP) 3-12, *Cyberspace Operations*. We do not necessarily understand what those definitions mean, because they are not well defined. Outside of the DOD there is another set of definitions, which are contained in Presidential Policy Directive 20 (PPD 20). Those definitions, too, are not well defined or easily understood. While the definitions are similar, they differ enough to cause confusion between the DOD and interagency elements. Nonetheless, the DOD must comply with the requirements in PPD 20, which creates problems when trying to define cyber operations using DOD terms and definitions.

Moreover, none of these definitions are helpful in determining what a cyber use of force or cyber armed attack is under the United Nations Charter and the LOW. To date, there is no international consensus defining either a cyber use of force or cyber armed attack. While some attempts have been made—for example, the Schmitt Analysis and the *Tallinn Manual*—they have not been accepted throughout the international community. The United States has provided several examples of what it would consider a cyber use of force or armed attack, but those examples equate cyber effects to kinetic effects. This adds to the mistrust of cyber operations from a misunderstanding of what they can and cannot do. There seems to be a generalized fear that if we use a cyber operation to take down a server, it is more serious than if we had bombed

the same server—that somehow the offended nation will be more upset. Both are a violation of state sovereignty, but a bomb is clearly open and hostile, while a cyber operation is stealthier. This lack of understanding and the very nature of cyber operations give one pause. Most nations would agree that if the physical consequences of a cyber attack produce the same kind of physical damage as dropping a bomb or firing a missile, that attack should be equally considered a use of force. However, we use terms such as "significant consequences" and "disrupt, deny, degrade, negate, impair, and destroy" to describe a cyber attack worthy of a response even without physical consequences.

We are not only concerned strictly about government systems, such as the DOD or the DHS, but also about critical infrastructure. *Critical infrastructure* is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, economic security, public health and safety, or any combination of these matters."[15] Much of this critical infrastructure is privately owned, adding to the confusion about how to handle any such cyber threats. Some examples include common supervisory control and data acquisition (SCADA) systems, including manufacturing, power generation, and water treatment. Other examples of critical infrastructure include the financial industry. It does not include Target, Home Depot, or Sony. We know our adversaries have probed SCADA systems, but what, exactly, are significant consequences? What, exactly, does it mean to disrupt or negate these systems? Even if such systems are disrupted or negated, does that then equate to a cyber use of force/armed attack?

The cyber event that targeted Sony was clearly not a cyber attack. It was, at best, a cybercrime perpetrated by a nation. (Despite what Hollywood elites think to the contrary, Hollywood is not part of the critical infrastructure either.) Likewise, the cyber event that targeted the Office of Personnel Management (OPM) was not a cyber attack. OPM was simply a legitimate target of cyber espionage, which is not prohibited under international law. Did either event result in significant consequences or disruption, degradation, or impairment? One can arguably answer "yes" to both, but how about actual physical consequences such as loss of life, incapacity, or destruction? Then the answer is clearly "no." However, that merely begs some questions: When do the "significant consequences" have to manifest? How extensive must the disruption,

degradation, or impairment be, and for how long? It is puzzling that the terms *disrupt*, *degrade*, *negate*, and *impair* are coupled with *destroy*. The first four terms imply some temporary and perhaps even reversible effects, while *destroy* leaves little doubt of permanent effects. Trying to determine exactly what a significant consequence is or whether something has been degraded or disrupted is nothing more than an exercise in futility absent physical damage, personal injury, or death, which typically will not arise as a result of a cyber operation. As an example of how complicated and confusing this made-up lexicon can be, *degrade* is more granularly defined as "to deny access (a function of amount) to, or operation of, a target to a level represented as a percentage of capacity." Likewise, *disrupt* is further defined as "to completely but temporarily deny (a function of time) access to, or operation of, a target for a period represented as a function of time."[16] Thus, we define the terms using other terms in the overall definition.

Clear cultural and language barriers also affect cyber operations. When Col William Hartman, commander of the Army's first offensive cyber operations brigade, joined the 25th Infantry Division for an exercise, the commanding general told Hartman that his "cyber operators talked in unintelligible 'dolphin speak.'"[17] Others acknowledge that "cyber is too important to leave to the cyber geeks. 'This is a commander's business, ultimately. He's the one responsible for integrating all these capabilities.'"[18] However, to integrate fully requires more than merely participating in exercises. "Cyber experts must start educating commanders on the art of the possible so they can drive requirements. There aren't enough requirements out there, because people don't know what to ask for and they don't believe they'll ever get to use it."[19] Without a coherent lexicon, common across the DOD, the intelligence community, and the legal profession, cyber language often means nothing to the commanders who make decisions. If they do not understand what cyber operations are or what they are capable of doing, they certainly will not ask for them—thus, the lack of requirements.

While some cyber operations may have the capacity to cause damage and destruction similar to kinetic strikes, the vast majority cannot reach that level. That is not what cyber operations are about. They are not designed to attack people but rather networks, network architecture, components, and equipment—generally resulting in an inability to communicate on time or correctly. Shutting down a power plant via a

cyber operation is clearly not the same as dropping a bomb on the power plant. One is clearly a use of force/armed attack, while the other may not be.[20] Unfortunately, far too many people have a basic misunderstanding about cyber operations. One recent example of this appears in a *Nextgov* article, "Pentagon Contractors Developing Lethal Cyber Weapons," in which the writer, Aliya Sternstein, asserts, "Under a forthcoming nearly half-billion-dollar military contract, computer code capable of killing adversaries is expected to be developed and deployed if necessary."[21] She continues, "Digital arms designed to kill are sanctioned under Pentagon Doctrine [referring to the DOD *LOW Manual*]. . . . The manual lays out three sample actions the Pentagon deems uses of force in cyberspace: 'trigger a nuclear plant meltdown; open a dam above a populated area, causing destruction; or disable air traffic control services, resulting in airplane crashes.'"[22] Sternstein totally misses the point, making it appear as if the United States is currently designing cyber capabilities that would have these intended effects. However, those who know and understand cyber operations and the LOW recognize the three examples as clear violations of the LOW—namely, specifically attacking civilian populations. Instead, what the *LOW Manual* suggests is that if any of those actions happened inside the United States, the government would clearly consider them a use of force/armed attack against the United States under the UN Charter and respond accordingly. There is a distinct difference in contracting for offensive cyber capabilities that we can use against an adversary (that is, their networks, command and control, communications, and so forth) and contracting for offensive cyber capabilities that can actually directly kill our adversaries. While second- and third-order effects of cyber operations may harm people, it is hard to fathom a realistic scenario wherein a cyber operation directly kills anyone.

The misunderstandings regarding cyber operations permeate the highest levels of US decision making, not only military commanders but also top civilian political leaders. Robert Work, deputy secretary of defense, recently stated, in response to activity against ISIS [the Islamic State in Iraq and Syria], "We are dropping cyber bombs. We have never done that before."[23] However, as a recent *Defense One* article states,

> Cyber options are adjunct powers, utilized in conjunction with other more traditional forms of coercion. Analogizing cyber operations as a kinetic weapon renders us cognitive misers, cheating our way through a difficult test. It is better to see cyber operations for what they are: changing lines in spreadsheets, intercepting email, jamming communication, and deception. We ought to be

careful when talking about cyber bombs because if we really think we are dropping cyber bombs, then these "bombs" are all landing with a resounding thud.[24]

Others, however, appear more sensitive about the topic. In a recent interview in Colorado Springs in which she was asked about Work's "cyber bombs" comment, National Security Advisor Susan Rice said, "It should not be taken out of proportion; it is not the only tool."[25] Some of Work's colleagues admitted to wincing when he said it, because lawyers for the government have worked diligently to narrowly limit cyber attacks to highly precise operations with as little collateral damage as possible.[26]

Who's in Charge?

A recent Government Accountability Office (GAO) report states that the Pentagon does "not clearly define its roles and responsibilities for cyber incidents."[27] There is confusion regarding who would be the supported command and have primary responsibility for supporting civil authorities. US Northern Command's (USNORTHCOM) defense support of civil authorities (DSCA) response concept plan states that USNORTHCOM would be the supporting command for a DSCA mission that may include cyber-domain incidents and activities. Other guidance directs that US Cyber Command (USCYBERCOM) would be responsible. Another problem is that key DSCA guidance documents do not identify the role of the dual-status commander, the commander who has authority over federal military and National Guard forces.[28] Some believe the DHS would have the lead, along with the Federal Bureau of Investigation and other agencies. Then there is also the newly created National Mission Forces, which are charged with defending the nation against "cyber attacks of significant consequence."[29]

It seems clear that, regardless who actually gets the initial approval, USCYBERCOM should be the supported command, simply because it has the capacity and capabilities to handle such incidents whereas USNORTHCOM and the DHS may not. To be sure, it is generally assumed that USNORTHCOM or the DHS would likely call upon USCYBERCOM for help. In recent comments, RADM Dwight Shepherd, director of cyberspace operations for USNORTHCOM and North American Aerospace Defense Command (NORAD), said, "From a cyber standpoint, we would have to coordinate with DHS because DHS or FEMA [Federal Emergency Management Agency] may be the leading federal agencies and we'd have to coordinate obviously with the states

that are affected."[30] But Shepherd conceded that USNORTHCOM is not best suited for the cyber component in national incidents. "I can tell you from a NORAD/NORTHCOM perspective we're really good at hurricanes [and] tornados but we're not capable, truthfully, to tackle a cyber event. So we, in my mind, would be supporting of CYBERCOM or JFHQ-DoDIN [joint forces headquarters-Department of Defense information network] along with coordinating with DHS or FEMA or the states." He said, "The real cyber expertise comes from CYBERCOM and the JFHQ-DoDIN."[31]

Liberating Cyber Offense

Offensive cyber operations seem to scare people who are unfamiliar with their conduct (and even some who are familiar with them). A general fear is that some super cyber weapon will be released and "escape" into the wild, taking down the entire Internet or inadvertently taking down the financial sector or SCADA systems. However, if one looks at Stuxnet as a real-world example of a cyber operation, it is clear that it is possible to specifically design a cyber capability with the LOW in mind. While it did spread throughout the world, it only affected what it was specifically designed to affect—Iranian nuclear components—thus complying with the principles of distinction and proportionality. Another general fear is that using offensive cyber operations will eventually lead to a cyber arms race and possibly a tit-for-tat escalation leading to all-out war. While this is a legitimate concern, it is overblown. An offensive cyber operation is usually a one-off, meaning that once used it probably cannot be used again, because the adversary has seen it, is aware of it, and quite likely knows how to mitigate the vulnerability or the effects. This is also known as *fragility*, that is, "the possibility that once used an adversary may be able to devise defenses that will render a cyber tool ineffective in the future."[32] As a result, escalation is limited because it takes so much time to not only develop such high-level cyber capabilities but also to conduct appropriate OPE to employ them. The idea that any cyber capability may be a one-off also leads commanders to hold onto them until absolutely needed, often ultimately rendering them useless through passage of time. Nonetheless, while the DOD struggles to get its cyber game in order, others are already doing so. Gen Keith Alexander, US Army, retired, discussing cyber operations at a recent Association of the United States Army conference, stated, "It's like

the recon/counter-recon fight. It's not the only fight: it's the first fight. If we win that, we'll still be in the second fight. What we can't afford to do is have our nation crippled in the cyber fight so it's fighting blind in the clashes that follow. In fact, China's already put out a strategy like that."[33] China, however, is not the only country to worry about. Maj Gen Stephen Fogarty, head of the Army's newly created Cyber Center at Fort Gordon, Georgia, believes Russia is also better at the cyber game. In an interview, he stated, "Russian activities in Ukraine . . . really are a case study in the potential for [what Army doctrine calls] CEMA, cyber-electromagnetic activities. It's not just cyber, it's not just electronic warfare, it's not just intelligence, but it's really effective integration of all these capabilities with kinetic measures [that is, bullets and bombs, drones and tanks] to actually create the effect that their commanders want to achieve."[34] The interviewer concludes, "That Russian-style integration of cyber/electronic warfare, drones, and old-fashioned high explosive is frankly impressive. It's also something US troops don't want to be on the receiving end of, ever. The only way to ensure we aren't is to get better at integrating cyber into traditional operations ourselves."[35]

Integrating offensive cyber operations into traditional operations requires commanders understanding what cyber can provide. It requires commanders comprehending the timing and tempo of cyber operations, particularly OPE. Other nations, such as Russia, China, and Iran, clearly do not restrict their cyber operators as does the United States. In fact, they partner with nongovernment hackers to broaden their reach and also to be able to assert plausible deniability and mask their identity. Adm Michael Rogers, former commander of USCYBERCOM and former director of the National Security Agency (NSA), warned that "nation states with advanced cyber warfare capabilities are taking steps to mask their cyber attacks by cooperating with nongovernmental hackers."[36] James Lewis, a cyber expert at the Center for Strategic and International Studies, agrees that "the Russians are so good we don't usually see them. The FSB [Russian Federal Security Service] hackers do classic political espionage, and it's a tribute to their success that they got into State, DOD and White House networks last year. The frightening thing about those incidents is that it may have been practice events for new teams. They really are [our] peers in cyberspace."[37] Russian capabilities may equal ours, and they are obviously using them. Their operators are enabled, while the United States lags behind, always on the defense,

reacting instead of being proactive. The DOD is currently building a cyber force of 6,200, while Russia and China have tens of thousands doing the same kind of work. While the DOD struggles to find and retain cyber operators, other nations seem resilient.

Highlighting the complex and confusing nature of cyber operations, Admiral Rogers said, "It literally probably took us two years to generate an internal consensus as to who was going to do what. . . . We've moved beyond a discussion of who ought to do what to OK, now we have clearly identified who has what responsibilities. Now let's roll up our sleeves and focus on how we're going to make this work."[38] We can make this work only if we remove the barriers that make offensive cyber operations too difficult.

First, the United States needs to reduce the approval authorities for offensive cyber operations to those commanders who are employing them, just as we do for kinetic operations. Offensive cyber operations are tools, just like kinetic options, that a commander may choose to use. To make this easier, perhaps the president or secretary of defense should preapprove a list of certain cyber capabilities to be used at the discretion of lower-level commanders and also expand the countries and areas in which they may be used. Those that fall outside of preapproved actions would still require approval, but we can speed up the request process. The United States should reconsider streamlining the RAPCO process to reduce the number of individuals involved, especially when many lack a comprehensive understanding of cyberspace. This will greatly speed up cyber operations, making them much more useful to commanders when needed. Cyberspace operations cannot continue to be held hostage to a slow, cumbersome, interagency process within which any agency that does not understand cyberspace operations can stop an operation supporting a joint force commander.

Despite the good work the NSA does, it sometimes forgets it is a DOD support agency and, as a result, does not like to collaborate and share with others, especially those who may disrupt their intelligence gathering or even appear to do so. The intelligence gain/loss is a concern, but it should not stop or hinder cyber operations. To be sure,

> Initial demands from the White House regarding cyber operations against ISIS, generated some resistance. The NSA has spent years penetrating foreign networks, placing thousands of implants in them. Those implants can also be used to manipulate data or to shut down a network. That frequently leads to a battle between the NSA civilians—who know that to make use of an implant is to

> blow its cover—and the military operators who want to strike back. NSA officials complained that once the implants were used to attack, the Islamic State militants would stop the use of a communication channel and perhaps start one that was harder to find, penetrate or de-encrypt.[39]

The nation must allow better sharing of data between agencies regarding access and mapping data of adversary networks. This would drastically reduce the time it takes to conduct OPE. We also need to educate combatant commanders and their planners about cyber operations so they understand the timeframes of cyber. It is relatively quick and easy for a joint force commander or other commanders to call for a kinetic strike, but not so for cyber. Without OPE, which takes some amount of time, cyber operations will not achieve the intended effects. Cyber operations cannot be on-call, on-demand, or on stand-by without appropriate OPE times taken into account. Cyber operations must be baked into the overall operation and planning with a clear understanding of the preparatory times required. If done correctly, offensive cyber operations can operate faster than kinetic operations either as stand-alone or preparatory to kinetic follow-on operations.

The DOD needs to pinpoint clear differences between cyber operations and kinetic operations where clear differences exist. This will avoid the clumsy and confusing misunderstanding that results with conflating them. We cannot simply treat them the same since the effects of each are different and affect different targets. The same rules can apply, but we cannot continue to apply them the same way for both cyber and kinetic operations. Most, if not all, of what the United States does in cyber falls well below the use of force/armed attack threshold, while kinetic operations are all but certain to be use of force/armed attack. Nonetheless, we continue to talk in terms of use of force and armed attack when dealing with cyber operations. It will be the rare cyber operation that actually crosses this threshold. Instead of worrying about when a cyber operation will cross that line, we should instead focus on the vast majority that do not and find ways to discuss and use them accordingly without having to engage in a LOAC analysis.

We need to delineate between true offensive cyber operations, OPE, and cyber surveillance and reconnaissance (SR) and those cyber capabilities that fall below the use of force/armed attack. Even those cyber operations that qualify as truly offensive cyber may not meet the international law definition of use of force/armed attack. We need a vigorous

dialogue regarding OPE and the authorities and approvals for conducting OPE and, more recently, cyber SR. These are not true offensive cyber operations. They are access tools and mapping tools. The DOD must have a robust discussion regarding countermeasures taken in response to cyber incidents. Countermeasures are generally considered "part of the subject of reprisals not associated with armed conflict."[40] In other words, they are used against actions that fall below use of force/armed attack and are themselves below that threshold—namely, exactly what most of our adversaries are engaged in.

We must consolidate working cyber operations definitions that come from the cyber operators, cyber commanders, and their cyber lawyers, those who truly know and understand cyber operations. There are profound differences among cybercrime, cyber espionage, and cyber attack. Likewise, there are profound differences between cyber tools, cyber capabilities, and cyber weapons. It is imperative that organizations understand these differences before having a serious discussion. The type or kind of cyber intrusion dictates who responds and how. Calling everything a cyber attack does a disservice to everyone. Having a standard set of commonsense and coherent definitions allows us to more easily explain to those who are not familiar with cyber operations exactly what cyber operations can accomplish.

Finally, we need to issue or update guidance that clarifies DOD roles and responsibilities to support civil authorities in a domestic cyber incident, in accordance with the recommendations of the GAO. It is imperative in an emergency situation that we have clear guidance on who is in control and that we work through the issues in an exercise environment prior to real-world events forcing us to fumble through.

If we fail to take these actions, alternative avenues will be pursued and leave offensive cyber operations behind. In fact, this is already happening as frustrated commanders rely on relatively simple and quick kinetic solutions. Agencies are also using different authorities to accomplish the same results without having to battle the same restrictions. If faced with a choice—destroy it now via a kinetic strike or wait some days, weeks, or perhaps even months for a cyber operation to potentially achieve the same effects—it seems clear which choice commanders will make. It does not have to be this way. If the proposals discussed above are implemented, offensive cyber operations can actually begin to move at the speed of light and benefit the commanders who most need them. SSQ

Notes

1. Brian Fung, "How Many Cyberattacks Hit The United States Last Year," *Nextgov*, 8 March 2013, http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/.
2. Department of Defense Cybersecurity Culture and Compliance Initiative memorandum, 30 September 2015.
3. David Sanger, "US Cyberattacks Target ISIS in a New Line of Combat," *New York Times*, 24 April 2016, http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.
4. Department of Defense, *DOD Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. The purpose of this document is to guide the development of the DOD's cyber forces and strengthen our cyber defense and cyber deterrence posture.
5. Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3139.01, *Review and Approval Process*, 22 October 2013, 3–4.
6. Office of General Counsel, Department of Defense, *Department of Defense Law of War (LOW) Manual*, June 2015, 16.1.2.1, http://www.dod.mil/dodgc/images/law_war_manual15.pdf.
7. Ibid., 16.5.1.1.
8. Mark Pomerleau, "Cyber Operations Come Out of the Shadows," *Cyber Defense* (web site), 5 May 2016, https://defensesystems.com/articles/2016/05/05/us-cyber-war-isis.aspx.
9. *LOW Manual*, 16.5.3.1.
10. Harold Hongju Koh, legal advisor, US Department of State (address, USCYBERCOM Inter-Agency Legal Conference, Fort Meade, MD, 18 September 2012).
11. Ibid.
12. *LOW Manual*, 16.1.2.2.
13. Ibid., 16.1.2.2.
14. Koh, USCYBERCOM Inter-Agency Legal Conference.
15. Title 42, United States Code, Section 5 195c(e).
16. Joint Publication 3-12, *Cyberspace Operations*, 5 February 2013, 11-6.
17. Sydney J. Freedberg Jr., "Army Fights Culture Gap between Cyber and Ops: 'Dolphin Speak,'" *Breaking Defense*, 10 November 2015, http://breakingdefense.com/2015/11/army-fights-culture-gap-between-cyber-ops-dolphin-speak/.
18. Ibid.
19. Ibid.
20. For the purposes of this paper, I have combined use of force and armed attack, because the United States does not acknowledge a distinction between the two.
21. Aliya Sternstein, "Pentagon Contractors Developing Lethal Cyber Weapons," *Nextgov*, 4 November 2015, http://www.nextgov.com/cybersecurity/2015/11/lethal-virtual-weapons-real/123417/.
22. Ibid.
23. Sanger, "US Cyberattacks Target ISIS."
24. Brandon Valeriano, Heather Roff, and Sean Lawson, "Stop Saying We're Dropping 'Cyber Bombs' on ISIS," *Defense One*, 24 May 2016, http://www.defenseone.com/ideas/2016/05/stop-saying-were-dropping-cyber-bombs-isis/128581/?oref=d-river.
25. Ibid.
26. Ibid.

27. US Government Accountability Office, Report to Congressional Committees, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, GAO-16-332 (Washington, DC: Government Accountability Office, April 2016), http://purl.fdlp.gov/GPO/gpo68065.

28. Ibid.

29. DOD Cyber Strategy, 2015.

30. Mark Pomerleau, "DOD Says It's Prepared to Support Civilian Response to a Cyber attack," *Defense Systems* (web site), 25 April 2016, https://defensesystems.com/articles/2016/04/25/dod-support-response-to-domestic-cyber-attack.aspx.

31. Ibid.

32. *LOW Manual*, 16.5.3.1.

33. Freedberg, "Army Fights Culture Gap."

34. Quoted in ibid.

35. Ibid.

36. Bill Gertz, "China Continuing Cyber Attacks on U.S. Networks," *Washington Free Beacon*, 18 March 2016, http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/.

37. Ibid.

38. Andrew Tilghman, "Cyber Force Grows, along with Retention Concerns," *Military Times*, 16 March 2015, http://www.militarytimes.com/story/military/careers/2015/03/14/cyber-growing/70210162/.

39. Sanger, "US Cyberattacks Target ISIS."

40. *LOW Manual*, 18.18.1.1.

Does China Have a Monroe Doctrine? Evidence for Regional Exclusion

Steven F. Jackson

Abstract

Chinese confrontational behavior in the East and South China Seas has led observers to assert that it has a "Monroe Doctrine." These discussions, however, have been vague as to what a Chinese Monroe Doctrine might actually be. This article will examine evidence for the degree to which China's current behavior actually constitutes a regional exclusion doctrine, rather than the more commonly used term "Monroe Doctrine." China specifically denies the analogy and denies excluding other countries from the region. However, recent leadership statements and declarations of an air defense identification zone in the East China Sea (and possibly in the South China Sea), point to the incremental development of just such a doctrine. Additional Chinese discussions of the "security belts" and "island chains" as strategic zones, moreover, would seem to point in that direction. The apparent lack of a formal exclusionary doctrine remains curious, and alternative explanations for this exist.

* * * * *

China's territorial claim in the South China Sea, recently upended by the Permanent Court of Arbitration in The Hague on 12 July 2016, is often cited as part of a broad Chinese effort to dominate East Asia.[1] This and other recent Chinese behavior toward its neighbors in Northeast and Southeast Asia have led some analysts to ask: Does China have a "Monroe Doctrine"? This question has been cropping up with increasing frequency in the popular and academic media while many of these analysts discuss it as if it were a fact.[2] The purpose of this article is to examine the evidence concerning this significant issue. Whether or not China is claiming exclusive rights to all or to parts of East Asia cuts to

---

Steven F. Jackson is professor of political science at Indiana University of Pennsylvania. Having lived and taught in China from 1981–83 and 2014, he specializes in Chinese foreign relations and comparative foreign policy of regionally dominant states. He holds an AB in international relations from Stanford University and a PhD in political science from the University of Michigan.

the core of US–China relations, the international relations of East Asia, and the future of the twenty-first century. Given China's assertions of ownership to the South China Sea, the Senkaku/Diaoyu Islands administered by Japan, and a "Belt-and-Road Initiative" opening economic ties to South and Central Asia, the question of China's official views on the region is very timely.

This article begins by defining exactly what a Monroe Doctrine or regional exclusion doctrine is, both in historical and comparative terms. Although primarily associated with early nineteenth-century US policy in the Western Hemisphere, in fact most regionally dominant powers have announced such doctrines. Next, the article examines recent Chinese policies to see if they match the doctrinal type, both in explicit announcements and in marginal behavior. Finally, the article explores potential reasons why China has not explicitly proclaimed such a doctrine and what signals may indicate changes for the future.

Regional Exclusion Doctrines Defined

Pres. James Monroe announced in 1823 that the United States viewed any new European colonization in the Western Hemisphere to be a "manifestation of an unfriendly disposition toward the United States."[3] The statement, dubbed "the Monroe Doctrine" in 1850, has since been conflated with the term *regional exclusion doctrine*, meaning a generic term for the formally articulated policy of a state to exclude other powers from an area, which it regards as its exclusive area of ownership, or influence. However, this is not the original intent. Today, many regional powers have regional exclusion doctrines, and many of them specifically reference President Monroe's address. It is important, however, to regard the issue with precision and not to conflate regional exclusion doctrine with other contemporary policies.

A regional exclusion doctrine is best summarized as "hands-off": an explicit and unilateral foreign-policy announcement by the regional hegemon that powers external to the region are not welcome. Unlike spheres of influence, regional exclusion doctrines must be openly and clearly articulated; a "Keep Out" sign does no good if it is hidden. They are also unilateral. Regional exclusion doctrines usually involve a specific region or sometimes a functional grouping of states or colonies. These are most frequently the immediate neighbors of the regional hegemon and an area beyond. The limits of the regional exclusion doctrine's zone

depend on a variety of factors, geography being the most important; some regions have clear terminal geographic boundaries that are both objectively and subjectively recognized. Other zones are more difficult to define precisely and "blend off" into other regions and other zones. The Eurasian continent is perhaps the best example of this.

The most pertinent aspect of a regional exclusion doctrine is the self-asserted rights adhering to the hegemon. The most prominent of these is the right to determine the foreign relations of member states within the zone. These span a wide degree of control by the regional hegemon, from "suggesting" that states within the region of exclusion consult with the hegemon to placing treaty controls on the regional states' third-party foreign relations. Of the third parties, extra-regional great powers are the most concerning to the regional hegemons. Formal military alliances with extra-regional powers, purchase or acquisition of arms beyond a hegemon-defined "maximum," and diplomatic recognition of governments hostile to the hegemon are all examples of foreign policies which regional exclusion doctrines seek to deny, mitigate, or veto. The introduction or reintroduction of external great powers into the affairs of a region that is dominated by a hegemon can often be the most provocative. As international relations scholar John Mearsheimer summarized in a 2015 *New York Times* editorial, "Great powers react harshly when distant rivals project military power into their neighborhood, much less attempt to make a country on their border an ally. This is why the United States has the Monroe Doctrine, and today no American leader would ever tolerate Canada or Mexico joining a military alliance headed by another great power."[4] Although the United States is one of the few countries to achieve complete regional hegemony according to Mearsheimer, other powers have sought to do so and have developed doctrines that seek to exclude others from their area.[5] The Soviet Union aggressively sought to exclude US influence in Eastern Europe through the "Doctrine of Limited Sovereignty." India under Nehru and Indira Gandhi sought to set South Asia off as a region of Indian dominance, specifically citing the Monroe Doctrine; this effort eventually was dubbed the "Indira Doctrine." Nigeria has periodically invoked a "Doctrine of Continental Jurisdiction" over sub-Saharan Africa.

Another very closely related doctrine that is usually subsumed under a regional exclusion doctrine is one which justifies direct intervention in the domestic affairs of regional states. The two are technically distinct,

but the latter is so frequently found with the former that the two will be included in this analysis. The United States doctrine of Caribbean intervention was dubbed the "Roosevelt Corollary" to the Monroe Doctrine after Pres. Theodore Roosevelt, and the Brezhnev Doctrine of 1968 formally articulated the Soviet Union's "internationalist duty" to intervene in socialist states' affairs when they deviated from socialism (read: Soviet-directed policy).[6]

Finally, a regional exclusion doctrine is distinct from the idea of spheres of influence. The latter tended to be much less formal than a regional exclusion doctrine and in the pre-twentieth-century world were secret divisions of a region or country between two great powers, with the quiet or tacit understanding that if an area were to be formally annexed, a particular power had the first rights to it.[7] To the extent that a sphere of influence area is not explicit, exclusion of other great powers' activity is seen as "devious" and does not bind third parties legally but does often lead to formal annexation. The most recent academic definition is a "definite region within which a single external power exerts a predominant influence, which limits the independence or freedom of action of states within it."[8] After World War I, the principle of self-determination of nations conflicted with the idea of great powers' spheres of influence, although the Soviet Union in particular was (secretly) in favor of them, evidenced by the secret protocols to the Nazi-Soviet Pact of 23 August 1939.[9] Post–World War II international norms and the United Nations made formal spheres of influence even more difficult to explicitly announce, and although the term is often used, it is not legally defined.

A Monroe Doctrine per se is not a desire for territorial aggrandizement or conquest, just as "Manifest Destiny" was not the same idea as the Monroe Doctrine in early nineteenth-century United States. Conquering or annexing land to the regional power or hegemon's formal control may be part of a regional exclusion doctrine, but in all of the doctrines examined above, most state members of the regional or functional system over which the regional hegemon is claiming exclusivity retain at least nominal sovereignty; it is domination, not annexation. Thus, this article is not discussing the broad range of twenty-first-century Chinese behavior in East Asia, only a very specific and important part of its foreign policy. It seeks to explore the ideational basis of Chinese behavior.[10] The South China Sea is part of the story, but in fact, the question of a Chinese regional exclusion doctrine in East Asia is much

more expansive than that contested area. All of this adds up to the expectation that a regional hegemon such as China would likely follow the pattern of other such states and formally announce a regional exclusion doctrine. To date, it has not.

China's Doctrine Denial

Other regional hegemons develop and articulate regional exclusion doctrines; has China done so? The direct answer is no, though the evidence is mixed and some trends that may point in that direction. First, Chinese officials themselves specifically and emphatically deny that China has a Monroe Doctrine (*Menluo zhuyi* 门罗主义, literally "Monroe-ism"). State Councilor Dai Bingguo was the top-level leader with responsibility for foreign affairs under Pres. Hu Jintao. His speech in December 2010, "Adhere to the Path of Peaceful Development," was considered by Chinese and outsiders as a major statement on China's outlook and is particularly worth examining precisely because it engages issues of neighboring relations and doctrines of exclusion directly.

Dai's statement is quite pacific, which is not terribly surprising: "China's strategic intention can be defined in two words: peaceful development, i.e., harmony and development at home and peace and cooperation abroad."[11] What is particularly important is his denial: "We do not seek hegemony and will never compete with other countries for leadership in our region, seek so-called 'joint hegemony' or follow so-called 'Monroe Doctrine.' . . . The bilateral and multilateral agreements we have signed with Asian countries do not have a single article that is exclusive."[12] Dai repeated this statement as a retired senior official as recently as 5 July 2016 in anticipation of the Permanent Court of Arbitration's award: "It would be nothing but baseless speculation to assert that China wants to make the South China Sea an Asian Caribbean Sea and impose the Monroe Doctrine to exclude the US from Asia or that China is trying to compete with the US for dominance in the South China Sea, Asia and even the world."[13] Chinese scholars have also delved into the Monroe Doctrine with extensive analyses as to why China's policies are not similar to the Monroe Doctrine.[14] Official Chinese sources have stressed that the policies of China do not seek to exclude external actors from the region: "China consistently stressed that Asia is open and welcomes a positive and constructive role from non-regional members, a stance that is essentially different from the Monroe Doctrine. China

. . . has never pursued a sphere of influence."[15] This statement has been repeated by the Foreign Ministry as well. The most logical target of such a policy, the United States, has been specifically mentioned as a state that China does not seek to exclude. Wang Yiwei, director of the Institute of International Affairs at Renmin University, writing in the usually provocative *Global Times* (*Huanqiu Shibao* 环球时报), also made this point clear: "Beijing has stated on many occasions it welcomes Washington to play a positive and constructive role in Asia and it is therefore unnecessary and impossible to exclude the world's greatest power."[16] Jin Canrong and Duan Haowen of the School of International Studies at Renmin University, the former a frequent commentator on China's East Asian relations, called for "Open Regionalism" as China's policy: "We must adhere to the principle of open regionalism. As the Asia-Pacific has become the biggest engine of the world economy, external powers are all eager to participate in Asia-Pacific economic activities in order to obtain reasonable rights and interests. China, whether out of consideration for its own relationships with other major powers or Asia-Pacific economic growth, should adhere to the principle of open regional cooperation."[17]

Senior researchers at the China Institutes of Contemporary International Relations (CICIR), an influential think-tank in Beijing, authored an article explicitly titled "The Pacific Ocean is Wide Enough for All" in 2014 and wrote that Chinese foreign policy initiatives in 2014 were "not . . . intended to squeeze Washington out of the region."[18] The point is reinforced by Han Caizhen and Shi Yinhong, writing in the same forum: "China's rapid rise is misunderstood as a bid by China to expand its regional power and to exclude the U.S. This is in spite of the fact that China has repeatedly said it welcomes a constructive role of the U.S. in East Asia."[19] Thus, at least at the level of officially articulated policy, China has not engaged in the construction of a regional exclusion doctrine seen in other regional hegemons' behavior. There is no explicit "Keep Out" sign. There have been hints, however.

Regional Exclusion Doctrine by Other Names

The treatment of American activities in East Asia is one of the key indicators that Chinese leaders may be seeking to exclude outside powers from the region. The US role in aggravating China's diplomatic problems with its Southeast Asian neighbors has been a recurring theme of Chinese foreign policy statements at least since 2004. These state-

ments have at times approached the point of calling for the exclusion of American forces and influence in the region. Chen Xiangyang, the deputy director of the influential China Institutes of Contemporary International Relations, wrote of the problem in 2004. He pointed out that US relations with the Philippines, India, and Japan create a hegemonic presence in the region to "clearly not allow Asian countries to manage Asian affairs."[20] This has the effect of making China's "Good Neighbor Policy" much more problematic. Specifically on the South China Sea issue, China regularly criticizes the United States for its "kibitzing" in the region, regularly calls for the United States to be "impartial" in the dispute, and very specifically notes that the United States is a nonparty to the dispute.[21] The *Global Times* opined, "The fundamental reason for the sudden prominence of the South China Sea issue and the Diaoyu Islands dispute has been the US. Seeing the 'pivot' to Asia, the US has fomented surrounding countries into confronting China over territorial disputes, so as to disturb and check China's rise."[22] Feng Zhongping of the CICIR wrote that, "It is generally believed at home and abroad that the U.S. has largely been responsible for worsening relations between China and some of its neighbors over the past two years. For example, some believe Japan has grown tough with China because it has Washington's backing."[23]

Pivot, Rebalance

The evolution of this idea may be linked to the US "pivot" to Asia, but evidence shows it began earlier. America's focus in the first decade of the twenty-first century was firmly on the Middle East and Afghanistan. The focus of American leadership was also on the domestic front from 2008 to 2009 because of the US presidential election and the financial crisis. Though some remain in Afghanistan, US combat forces were withdrawn from Iraq at the end of 2011, when then-Secretary of State Hillary Clinton wrote a provocative article, "America's Pacific Century," in which she advocated the United States pivoting its power to the Asia–Pacific region (the Chinese translation is usually *chongfan YaTai* 重返亚太).[24] Almost immediately the term "pivot" was substituted with "rebalance" (*zai pingheng* 再平衡), though *pivot* is still commonly used in Chinese and English.

As Mearsheimer claims, the introduction of a new great power into the regional hegemon's space is likely to result in a conflictive relationship between the native power and the "intruder." How does China's

reaction compare? The initial, official reaction of the Chinese foreign ministry in 2011 was muted:

> The US took high-profile steps to deepen its involvement in Asia-Pacific affairs. After 10 years of combating terrorism, the United States was seeking to withdraw its troops from Afghanistan and at the same time increased input in the Asia-Pacific. The United States strengthened ties with its allies including Japan, the ROK and the Philippines, promoted relations with such regional emerging countries as India and Indonesia, expanded engagement in regional multilateral affairs, and pressed ahead with the Trans-Pacific Strategic Economic Partnership. President Obama attended the East Asia Summit for the first time.[25]

In 2012, China's foreign ministry briefly noted the term *rebalancing*. It also noted curtly that, "The United States played an important part in China's disputes with neighboring countries on territorial sovereignty and maritime rights and interests."[26] The following year it continued to note the "strategic rebalance" of the United States in the Asia–Pacific, emphasizing at length US military and strategic cooperation with allies in the region.[27]

Was this a change? China's previous statements about American involvement in East Asia and Sino-American relations in general have evolved during the twenty-first century, gradually becoming cooler. However, it is also interesting to note that the official Chinese foreign policy assessment of the United States in East Asia never characterized America as "absent" from the region prior to the pivot policy. The evolution of Chinese statements on the subject of US policy and presence in Asia is worth exploring in some detail.

Constructive and Cooperative

In 2002, in the wake of 9/11, the Chinese foreign ministry noted that "The US increased its deployment in Eurasia galvanized by the need to fight terrorism. It encouraged NATO to expand further to the east, beefed up its forward troop buildup in Asia-Pacific, set up new footholds in Southeast Asia and solidified its military presence in Central Asia."[28] The overall tone of the Foreign Ministry's characterization was highly positive, remarking, "China-US relations witnessed significant improvement and growth. The two countries maintained close exchanges of high-level visits and strategic dialogue. President Jiang Zemin . . . reached an important common understanding with President Bush on developing a constructive and cooperative relationship between the two countries"

and noting increased understanding and trust, trade, cooperation on terrorism and regional issues, as well as military exchanges.[29] Specifically in Asia, the Chinese Foreign Ministry said, "The United States, proceeding from its practical needs of counter-terrorism, adjusted its national security strategy, paying more attention to its coordination and cooperation with China and Russia. There were growing common interests among major countries in maintaining a peaceful and stable Asia." It also noted "Japan and the US reinforced their military alliance and cooperation."[30] The phrase "constructive and cooperative relations" is noted in 2001.[31]

The 2003 assessment of US foreign policy in the wake of the invasion of Iraq was exceptionally blunt, calling US unilateralism "trigger-happy" and questioning the US role in the world in general.[32] There was a strong sense of fear that the United States policy toward Iraq might be implemented in North Korea: "China and other neighbors of the Peninsula were deeply worried. They did not endorse sanctions and coercion, let alone war, as viable ways to cope with the situation, but wanted a peaceful solution to the crisis. Thanks to many rounds of diplomatic mediation volunteered by China . . . the DPRK and the US expressed readiness for talks."[33] Yet China's foreign ministry nevertheless said, "A stronger constructive and cooperative relationship between China and the US contributed to a healthy trend of development in Asia."[34] "Constructive and cooperative relations between China and the US continued to grow" in 2004, and the "US continued to readjust and strengthen its military posture in the Asia-Pacific region."[35] The "constructive and cooperative" Sino-American relationship tagline was also used in reference to 2005 but with the additional note that "the United States stepped up its presence in Southeast Asia, enhanced relations with its allies, such as the Philippines, Thailand and Singapore, resumed military and security cooperation with Indonesia and improved ties with Vietnam. It followed regional cooperation in Asia with keen interest and increased its involvement in it."[36] Moreover, the same theme can be found in 2006: "The overall US foreign policy remained unchanged, but some adjustments were made. . . . It continued to focus on the greater Middle East region and increased input in the Asia-Pacific region."[37]

In its assessment of US foreign relations in 2007, the Chinese Foreign Ministry emphasized, "The United States became more pragmatic in conducting diplomacy and paid more attention to the role of other powers and multilateral mechanisms. It continued to pursue counter-

terrorism . . . increased engagement in the Middle East, adopted the 'New Strategy in Iraq,' pushed for tougher sanctions on Iran, and hosted the Middle East Peace Conference. . . . It attached greater importance to the Asia-Pacific region, and took an active part in the Asia-Pacific regional cooperation."[38] It further noted that "China and the United States maintained close consultations and increased dialogue and cooperation on issues in Asia" and that "the constructive and cooperative relations between China and the United States continued to grow. The two countries had increasing common interests in upholding regional peace and stability and maintained close consultation and coordination."[39]

Strategic Belts

However, in 2009, the "constructive and cooperative" characterization changed, indicating that "major powers continued their deep involvement in regional affairs and expanded their influence."[40] By 2010, China noted that major powers including the United States, Europe, and Russia increased their attention to an input in Asia" and evoked Secretary Clinton's term of "forward-deployed diplomacy," which "increased its attention to and input in the Asia-Pacific region."[41]

Other evidence that China is beginning to move toward a regional exclusion doctrine can be found in a number of statements by leaders and scholars in China. One of the most important high-level conferences that engaged policy issues about China and its policy toward its neighbors was the October 2013 Peripheral Strategy Conference, one of the highest-level foreign policy leadership meetings in years, and its academic follow-on conference, which may have made some modifications to this approach. One of the more provocative articles from the academic conference was by Li Yonghui, dean at Beijing Foreign Studies University, who explicitly called for China to establish a "strategic peripheral belt" (*zhoubian zhanlüe yituo dai* 周边战略依托带) in the region.[42] Li explicitly pointed to the unsuccessful efforts of prewar Germany and Japan to establish such belts in their regions and the more successful effort of the United States in its "Good Neighbor Policy." Li concludes that "China can set up its strategic belt with its twenty-odd neighbors, of course, but it also can construct a larger strategic belt with the countries of the Middle East, the Pacific Rim, and the Indian Ocean."[43] Still others, most notably the president of the CICIR, Ji Zhiye, have disagreed with this proposal, saying, "History shows how

some big powers turned their neighborhood [*zhoubian* 周边 (although "surrounding area" would be a more precise translation)] into colonies by imposing their systems, laws and even languages on them; others set up spheres of influence around themselves by ignoring the national interests of their neighboring countries; still others sought to establish their hegemony by using alliances or institutions. All of these efforts have met with failure."[44] Ji continues and allows the United States a role in the region, saying, "Since China is blazing a trail in the field of neighboring diplomacy, it will naturally not reject the legitimate interests of the other major powers on her periphery. In this regard, China needs to learn how to co-exist peacefully with other major powers, notably the United States."[45]

Perhaps the most noted hint that China was moving toward a regional exclusion doctrine was Pres. Xi Jinping's statement about "New Asian Diplomacy" to the Fourth Conference on Interaction and Confidence Building Measures in Asia (CICA) in May 2014 in Shanghai, when he stated in a prepared speech that, "In the final analysis, it is for the people of Asia to run the affairs of Asia, solve the problems of Asia and uphold the security of Asia. The people of Asia have the capability and wisdom to achieve peace and stability in the region through enhanced cooperation."[46] Many analysts, both foreign and Chinese, jumped on the (officially translated) phrase "it is for the people of Asia to run the affairs of Asia" as an exclusion of non-Asian powers, and strangely similar to the phrase "Asia for the Asiatics" first used by Konoe Atsumaro in 1898 in contemplating Japan's own version of the Monroe Doctrine.[47] Chinese scholars and policy analysts quickly sought to deny such an interpretation. The official government China Internet Information Center engaged the issue directly:

> The Western media, along with the media in some of China's neighboring countries, have noticed that Chinese leaders tend to use the phrase 'having Asian countries manage Asian affairs' more frequently. They interpreted it as 'China's Monroe Doctrine,' because it shows China's urge for a greater role in Asian affairs, much in the same way the Monroe Doctrine provided the legitimacy for the U.S. management of the affairs in the Western Hemisphere. . . . At the same time, some of China's neighbors have shared the concern that they will be victimized in the contention between China and the United States in seeking regional dominance, in the same way the ongoing Ukrainian crisis worried Ukraine's neighbors.

> But after all, the Monroe Doctrine, a term filled with hegemony, cannot truthfully summarize China's activities in its peripheral regions, nor could the reckless remarks of some Chinese officials during the preparation for the CICA.[48]

It is well worth noting that the next paragraph in Xi's speech denies any effort at exclusion: "Asia is open to the world. While enhancing their own cooperation with each other, countries in Asia must firmly commit themselves to cooperation with countries in other parts of the world, other regions and international organizations. We welcome all parties to play a positive and constructive role in promoting Asia's security and cooperation and work together to achieve win-win outcomes for all."[49]

Xu Qingchao of the Shanghai Academy of Social Sciences, while noting the rise of China and the importance of Xi's "New Asian Diplomacy," also specifically denied it to be a "Chinese Monroe Doctrine."[50] Interestingly, several Chinese commentators also pointed out that "Asian states even including Japan have misgivings about whether the US can provide permanent security for them, Xi's remarks indicate that it is never reliable to bind your own security to another's wagon."[51] This questioning of the US security commitment to Asia has been posed not as an actor to exclude, but rather as a public good which the United States may fail to provide.[52] Other Chinese authors equivocated on the issue of China's potential domination of its neighbors similar to other historical great powers. Writing in *China Daily*, Yan Xuetong said,

> Historically, all global powers rose as regional powers before becoming global powers. In the early stages of its rise, the US implemented the Monroe Doctrine and focused on Latin America; after World War II, the Soviet Union, which was growing in strength, took Europe as the focus. China will be no exception, so it too needs a successful neighborhood policy first. That move can help win friends among its neighbors, because after World War II it is already an established rule that sovereignty and territory should not be violated; both the US and the Soviet Union influenced neighbors' politics but without incorporating territory as they had done in the past."[53]

Core Interests

Another central foreign policy statement that some external analysts have seen as an element of an exclusion doctrine is expansion of China's "Core Interests." The term (*hexin liyi* 核心利益) has been used in discussing issues which China sees as nonnegotiable, such as the status of Taiwan and Tibet as provinces of China beginning in 2003.[54] However,

beginning in 2010 the term was used to describe other areas under a new national security law.[55] Although Japanese media claimed that this had applied to the Senkaku/Diaoyu disputed islets, and other media claimed it was being applied to the South China Sea, Chinese statements are in fact ambiguous about whether these two areas are in fact claimed as "core interests."[56]

In addition to these statements, some analysts have specifically cited some Chinese behavior as showing at least some evidence of exclusion: Chinese activity in the South China Sea claimed by the "Nine-Dashed Line," a self-declared "Air Defense Identification Zone (ADIZ)" in the East China Sea near the Senkaku/Diaoyu Islands in 2013, and the general discussion of the "First Island Chain" and "Second Island Chain" as defense features.

Dashed Lines

The "Nine-Dashed Line" (revised in 2013 to a "Ten-Dashed Line" on official Chinese maps) represents a claim that predates the People's Republic of China. What is ambiguous is whether the dashes on Chinese maps are a simple map-making convention—grouping the many islands, islets, reefs, shoals, and rocks of the South China Sea together for purposes of clarity but not claim—or a full maritime sovereignty claim to the entire South China Sea: water, islands, rocks, and reefs.[57] Although a territorial claim, the Chinese statements concerning the South China Sea are not exactly a regional exclusion doctrine as it has been defined here. First, the area is unpopulated and not exactly a region; all other regional exclusion doctrines have spanned broader identifiable regions, encompassing multiple sovereign countries. Second, the claim is not particularly new, though the construction of artificial islands on top of reefs is new, as is the use of coast guard and naval resources to patrol and enforce Chinese claims. Third, although Chinese documents and announcements regularly reiterate their territorial claims to the South China Sea, there has been no effort to categorically deny entrance or transit to other countries' ships or aircraft in the area, and given its importance to international shipping, such a move would be impossible to enforce. The Chinese foreign ministry stated, "The Chinese side respects and safeguards the freedom of navigation and over-flight in the South China Sea to which all countries are entitled under international law."[58]

In one respect, however, Chinese territorial claims in the South China Sea do resemble a regional exclusion doctrine. The Chinese claim to determine the method of resolution—by strictly bilateral negotiations—on the basis of China's "historical claims," not multilateral negotiations (where China would be only one of five or six claimants at a very publicly observable table) and not by international legal arbitration, as demonstrated by its rejection of the Permanent Court of Arbitration's award. China is seeking to set up the rules of the game in Southeast Asia, just as James Monroe and John Quincy Adams (the actual author of the Monroe Doctrine) unilaterally asserted the rules of the Western Hemisphere.

Chinese statements specifically on the US presence in the South China Sea, moreover, have been contradictory. On the one hand, when the United States announced that Japan might join it in aerial patrols of the region, a Chinese spokesman said in 2015 that the United States and Japan were "not involved in the South China Sea issue" and should not do anything to "complicate the situation," which would imply staying out.[59] Furthermore, Chinese naval units have protested the US "Freedom of Navigation Exercise" within 12 nm of Chinese-occupied reefs.[60] On the other hand, Chinese statements have alluded to future US use of weather stations and search-and-rescue facilities in the South China Sea reefs being reclaimed by China.[61] Thus, there seems to be a fine difference between a sign that says "Keep Out" and one that says "I Own This."

Air Defense Identification Zones

The announcement of an East China Sea Air Defense Identification Zone in the East China Sea near the disputed Senkaku/Diaoyu Islands in November 2013 was seen by some analysts as another assertion of Chinese primacy in the region and at the least the advancement of a territorial claim against Japan.[62] The rhetoric associated with the announcement of the zone was clearly anti-Japanese but did not seem aimed at the United States.[63] Somewhat akin to the position on the South China Sea, China's announcements sought to differentiate civil and non-civil intrusions into "its" sovereign territory: "China's establishment of the zone is aimed at safeguarding national sovereignty and security of territory and territorial airspace. . . . The Chinese government . . . explicitly [points] out that normal flight activities by foreign international airlines within the East China Sea ADIZ will not be affected at all."[64] But at least one Chinese scholar was explicit in linking the zone to a broader idea: "It is

an important measure towards improving geopolitical security structures in the East China Sea and building the 'strategic buffer zone' [*zhanlüe huanchong qu* 战略缓冲区]."[65] Other Chinese authors pointed out that the United States has its own ADIZ, and the rules involving them are substantially similar.[66] US policy makers did not see it that way, and the strong US reaction to the announcement of the zone—sending two B-52 bombers flying through it unannounced—and the negative reaction by other countries such as South Korea—whose claim to a sea structure called Ieodo is overlapped by the Chinese ADIZ—resulted in China stepping back from enforcing its zone.[67]

Island Chains

Finally, Chinese popular and scholarly press have had vague discussions about the "First Island Chain" and "Second Island Chain" that might be interpreted as an effort to set a zone of exclusion. The term "island chain" was first used by John Foster Dulles in 1951 (prior to his stint as secretary of state), and subsequent mentions reference US defense agreements with states occupying a chain of islands from Hokkaido to Okinawa, Taiwan, Luzon, and the Philippine archipelago. The term did not appear again until the 1990s and by the 2000s was increasingly referenced both by US and Chinese strategic analysts.[68] Chinese Admiral Liu Huaqing, sometimes dubbed the "Father of the Chinese Navy," set a goal of being able to defend China's maritime security interests out to the First Island Chain in 2000, to the Second Island Chain (a vague line including the Kuriles, Hokkaido, and Honshu and then south through the Bonin Islands, Guam to the western tip of New Guinea, and possibly including the Straits of Malacca) by 2020.[69] Some western analysts have implied that these discussions amount to an area that China seeks to control, such as a US military analyst's 2001 comment about Chinese naval acquisitions: "It really does have the potential to force the United States back away from that first island chain that they want to declare as their own territorial seas."[70] Other US authors claim that China's discussions of island chains are territorial: "When it comes to the sea, [China] still thinks territorially, like an insecure land power, trying to expand in concentric circles in a manner suggested by [geostrategist Nicholas J.] Spykman. The very terms it uses, 'First Island Chain' and 'Second Island Chain,' are territorial terms, which, in many cases, are seen as archipelagic extensions of the Chinese landmass." That

author also invokes US policy toward the Caribbean at the beginning of the last century: "Much like when the Panama Canal was being dug, and the United States sought domination of the Caribbean to be the preeminent power in the Western Hemisphere, China seeks domination of the South China Sea to be the dominant power in much of the Eastern Hemisphere. . . . Once it becomes clear, a few years or a decade hence, that the United States cannot credibly defend Taiwan, China will be able to redirect its naval energies beyond the first island chain in the Pacific . . . to the second island chain."[71] And Simon Winchester, a popular author writing in an opinion column in the *New York Times*, also made the point concerning the island chains, saying, "Central to the new [Chinese] strategy is the construction of three imagined bastions, chains of disconnected Pacific islands that would, in Beijing's view, comprehensively protect and project its influence."[72]

Chinese discussions, on the other hand, have tended to see the island chains as defensive lines of the United States hemming China in, a "blockade" which the United States and Japan have imposed on China. The *Global Times* characterizes it as a matter of breaking out: "In front of a growing strategic siege by the US and Japan, China will have to intensify efforts in breaking through the first island chain blockade, so as to guarantee its freedom to navigate in the West Pacific including the Sea of Japan."[73] Thus far, there have been no clear, official claims by China that the first or second island chains constitute any sort of sphere of influence or an area subject to the regional exclusion doctrine.

All of this makes it difficult to say that China has a regional exclusion doctrine, but it may be moving toward one. Analysts and policymakers could expect, based upon the behavior of similar regional hegemons in the nineteenth and twentieth centuries, that just such a doctrine would have already been explicitly declared. Why not?

Why No Explicit Doctrine?

Explaining a lack of behavior is, of course, much more difficult than explaining observable behavior, so what follows here is somewhat speculative. The first possible reason why China does not have a Monroe Doctrine is something akin to path dependency: it has explicitly decried any such regional exclusion doctrine in the past and has stated in official terms that it would never adopt such a doctrine. To adopt such a doctrine now or in the near future requires an explicit statement and would

naturally beg the question of why the previous policy had changed. It has occurred in the past, of course, that states have openly repudiated previous policies. Government or regime change is one such instance, but it seems unlikely in the foreseeable future for China.

A second possible reason for the lack of a Chinese Monroe Doctrine is a historical Chinese aversion to regional exclusion doctrines. The first reference to countries other than the United States having their own Monroe Doctrine was the relationship of Imperial Japan to East Asia in the late 1890s and the English during World War I.[74] By the 1930s, Japan's "Greater East Asian Co-Prosperity Sphere" (*Daitōakyōeiken* 大東亜共栄圏 or the "East Asian New Order" (*Tō-A shin chitsujo* 東亜新秩序) was not only a regional exclusion doctrine based upon the slogan of "Asia for the Asians," it was also a thinly veiled justification for rapacious Japanese imperialism. This history is well known in China, and its scholars have written on the subject of "Japan's Monroe Doctrine."[75] Qing dynasty China also had to endure European spheres of influence in its territory during the late nineteenth and early twentieth centuries, as well as formal colonies and leaseholdings. Thus, China's recent historical experiences with regional exclusion are not positive.

A third potential reason for China eschewing a formal regional exclusion doctrine would be the precedent it would set for its relations with South Asia and Central Asia. In both regions, China's economic reach is already intruding into areas which the Indians and the Russians explicitly believe they have primacy and have said so on several occasions. Pres. Xi Jinping's 2013 initiative, the "Silk Road Economic Belt" and the "Maritime Silk Road" ("One Belt, One Road," *Yi Dai, Yi Lu* 带一路) concept expands infrastructure, transportation, and trade links between China, Southeast Asia, South Asia, Central Asia, the Middle East, and all the way to Europe. For China to seek to exclude other powers from East Asia while pushing ahead into Russian and Indian regions would doubtlessly provoke charges of hypocrisy and resistance. China is seeking to expand its influence globally, not to limit it.

Fourth, the original Monroe Doctrine is now officially defunct. In a move that attracted more attention in Latin America and China than the United States, the US Secretary of State John Kerry, in a major speech at the Organization of American States, officially renounced the Monroe Doctrine in November 2013: "The era of the Monroe Doctrine is over. . . . Many years ago, the United States dictated a policy that defined the

hemisphere for many years after. We've moved past that era."[76] Officially, of course, this means nothing to China. In reality, it deprives China of using the same excuse for having a regional exclusion doctrine that so many other regional hegemons have invoked: the United States has one, too. Chinese scholars wrote several articles on the issue, some seeing it primarily as a response to declining US power and an effort to improve Latin American relations. Other scholars looked at it from a broad view of historical development. But it seems likely that Chinese policy makers would have been made aware of the announcement.[77]

The final possibility is, of course, that China's leaders do not think the time is right for such an announcement but that it will be in the future. Paramount leader Deng Xiaoping's famous dictum, *taoguang yanghui,* still has a powerful influence on Chinese strategic thinking. (韬光养晦. Translations vary but often include elements of "lay low," "hide your capabilities, develop some strength," or more fully, "keep a low profile and bide your time, while also getting something accomplished.") Trying to exclude foreign powers from Southeast and Northeast Asia means trying to exclude the United States. And few Chinese authors, scholars, or even bloggers argue that China currently has that capability, and no Chinese leaders or official sources openly advocate that path. At least, not yet.

Conclusions: What to Watch For

Three conclusions and a number of recommendations follow from the above analysis. First, China has not yet developed a regional exclusion doctrine, and journalists, scholars, and policy makers should be very careful in making such an assertion. Second, China's behavior vis-à-vis its neighbors, though often vexing and seemingly aggressive, is actually more moderate than other regional hegemons' behavior; China has not openly intervened in its neighbors' domestic affairs, its use of military force has been limited, and it has not openly declared a regional exclusion doctrine. Compared to the Russian Federation now, or the United States at the beginning of the twentieth century, China appears much more benign. It still might develop a regional exclusion doctrine, and one can find evidence for a "creeping doctrine." Nevertheless, a regional exclusion doctrine needs to be explicit, and once such an announcement is made, the potential effect would be substantial and dangerous. There is little question but that the United States would object to such a move,

possibly forcefully and in conjunction with its friends and allies. A number of additional indicators and cautions should be noted.

Closely Watch the Charge of US "Meddling"

The most important indicator of a Chinese policy shift toward a regional exclusion doctrine doubtlessly focuses on its assessment of America's role in East Asia in general, Southeast Asia in particular, and vis-à-vis those neighbors with whom China has disputes.[78] China's scholars, editorial writers, and, increasingly, official spokespersons have commented in ways that imply that the United States is meddling in the affairs of the region. When such comments begin to use a possessive pronoun "our region" and are not accompanied by the usual disclaimer that China does not seek to exclude other great powers, then Beijing is starting toward its own regional exclusion doctrine.

Focus on China's Views of India and South Asia

China's original rival in East Asia was Japan, but Beijing's power has clearly begun to eclipse that of Tokyo. And the power of the United States, as seen by Chinese scholars, appears to be gradually declining and drawn off to other regions such as the Middle East. But there is another rising power in Southeast Asia: India. In the long term, the relationship of China and India in South and Southeast Asia represents another area in which both powers come into contact and potentially conflict. Indian political leaders see the subcontinent at a minimum to be "their" area and seek to exclude other powers.[79] At the same time, India's navy has already begun to make port visits in Southeast Asia, and the diplomatic competition between China and India in states such as Bangladesh, Myanmar, Sri Lanka, and Nepal could be a manifestation of Chinese willingness to exclude great powers of the future from "its" region.

Monitor Chinese Treatment of Overseas Citizens and Co-Ethnics

Regional hegemons generally dislike other great powers in their neighborhoods; they also usually react quite forcefully when their civilian citizens or co-ethnics suffer harm in other countries, which are often in neighboring states. Such interventions, though ostensibly for civilian protection, have often been used as justification for broader action against smaller states, such as the US interventions in the Caribbean and Central America in the late nineteenth and early twentieth centuries or the

Russian intervention in Ukraine in 2014. During the 1950s, 1960s, and 1970s, China's reaction to the unequal and often harsh treatment of ethnic Chinese in Southeast Asian countries was vehement, but it lacked the means to back up its comments. This has changed. At the same time, the condition of ethnic Chinese in Southeast Asia in this century has generally improved to the point that China has few causes for complaint, since the "overseas Chinese" have gained local citizenship and become prominent and prosperous in their adopted countries. More recently, contract workers and tourists have added to the mix, though China's reaction to the anti-Chinese riots in Vietnam was quite subdued. Future reactions in situations in which China has a motive to "teach them a lesson" may test that restraint.

Watch the Rhetoric

Language matters, and it can be a key indication of disposition and intentions. Terms such as "backyard," "our region," "our neighborhood," and the like indicate a subtle shift in both psychology and policy toward possessiveness. Pan-Asian rhetoric has been largely absent from Chinese foreign policy statements, but most regional exclusion doctrines assert a distinctiveness to the region which the hegemon seeks to lead—hence the attention given to the Xi Jinping's speech at the 2014 CICA summit ("Asian countries managing Asian affairs"). The statement in *China's Foreign Affairs* in 2015 also seems to be leaning in that direction: "[Asian countries'] sense of belonging and identity with Asia continued to grow. The Asia security concept of common, comprehensive, cooperative and sustainable security increasingly gained support of the people. Countries in Asia followed the 'Asian Way' featuring mutual respect, consensus and taking care of all parties' comfort levels."[80] However, terms that imply familial relations, especially "elder brother" terms, are often seen in other regional hegemons' efforts to determine the affairs of the "little brothers" in their region and are a statement of primacy. The language of neighbors can point in the opposite direction of respect and equality. The Chinese "Good Neighbor Policy" (*Mulin Youhao Guanxi* 睦邻友好关系) may invoke the same reaction, while the trends of rhetoric may serve as a useful indicator whether China really is moving toward a regional exclusion doctrine.

In July 2010, then-Chinese Foreign Minister Yang Jiechi, when meeting Association of Southeast Asian Nations (ASEAN) ministers, found

China under significant criticism from Secretary Clinton and others at the meeting. Yang reportedly blurted out, "China is a big country, and other countries are small countries, and that's just a fact," a blunt statement that shocked many in the room, fearing that it revealed China's sense of entitlement over the region broadly. The subsequent statement on China's Foreign Ministry web site was much more measured and indicated that China sought to solve the South China Sea dispute using bilateral diplomacy. It also asserted that the position represented the interests of "fellow Asians."[81] If China believes that it can determine what is in its neighbors' interests by unilateral fiat, then it is well on its way to a regional exclusion doctrine. SSQ

Notes

1. Permanent Court of Arbitration, "PCA Case No 2013–19 In the Matter of the South China Sea Arbitration before An Arbitral Tribunal Constituted Under Annex VII to the 1982 United Nations Convention on the Law of the Sea between The Republic of the Philippines and the People's Republic of China: Award," The Hague, Netherlands, 12 July 2016, https://pca-cpa.org/wp-content/uploads/sites/175/2016/07/PH-CN-20160712-Award.pdf.

2. Lexis-Nexis shows 132 unique hits on the phrase "Chinese Monroe Doctrine" through 18 June 2016. It appears first in print in the *New York Times* article by Jane Perlez on 9 October 2003, quoting Ernest Z. Bower, at the time the president of the US-ASEAN Business Council. A letter to the editor of the *South China Morning Post* in December 2003 also mentions it. A search on CNKI.net, the China Academic Journals Full-Text Database, one of the most prominent Chinese-language databases of scholarly and policy-oriented periodicals, shows 149 hits on the phrase "门罗主义" (as of 7 January 2016). See also Roger Cohen, "Op-Ed: China's Monroe doctrine," *New York Times*, 8 May 2014, http://www.nytimes.com/2014/05/09/opinion/cohen-chinas-monroe-doctrine.html; Stephen M. Walt, "Dealing with a Chinese Monroe Doctrine. Room for Debate Forum: Are We Heading for a Cold War with China?," *New York Times*, 2 May 2012, http://www.nytimes.com/roomfordebate/2012/05/02/are-we-headed-for-a-cold-war-with-china, updated 26 August 2013; Patrick Mendis, "Beijing's Menluo doctrine," *Harvard International Review* 36, no. 1 (2014): 18–21; John Glaser, "China's Monroe doctrine – or escalation in Asia?," *The American Conservative*, 10 December 2013, http://www.theamericanconservative.com/articles/chinas-monroe-doctrine-or-escalation-in-asia/; James R. Holmes, "China's Monroe Doctrine," *The Diplomat*, 22 June 2012, http://thediplomat.com/2012/06/chinas-monroe-doctrine/; Ted Galen Carpenter, "Should Washington consider accepting a Chinese Monroe doctrine?," *China-US Focus*, 21 August 2014, http://www.chinausfocus.com/foreign-policy/should-washington-consider-accepting-a-chinese-monroe-doctrine/; and Bruce Fein, "Stop Opposing China's Monroe Doctrine and Roosevelt Corollary," Huffington Post blog, 4 November 2015, accessed 18 June 2016, http://www.huffingtonpost.com/bruce-fein/stop-opposing-chinas-monr_b_8473588.html. For a very good treatment of the term and its evolution in Chinese, see Li Zhonglin, "*Ping suowei Zhongguo ban 'Menluo zhuyi'* " ["Comment on the so-called 'Chinese Monroe Doctrine' "], *Heping yu fazhan*, no. 4 (2013): 103–15.

3. US National Archives and Records Administration, "Transcript of the Monroe Doctrine (1823)," Ourdocuments.gov, accessed 9 April 2015, http://ourdocuments.gov/doc.php?doc=23. For a more recent scholarly source on the doctrine and its origins, see Mark T. Gilderhus, "The Monroe Doctrine: Meanings and Implications," *Presidential Studies Quarterly* 36, no. 1 (2006): 5–16, http://www.jstor.org/stable/27552742.

4. John J. Mearsheimer, "Op-Ed: Don't Arm Ukraine," *New York Times*, 8 February 2015, http://www.nytimes.com/2015/02/09/opinion/dont-arm-ukraine.html.

5. John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton, 2001), 143.

6. "Theodore Roosevelt's Corollary to the Monroe Doctrine (1905)," US National Archives & Records Administration, accessed 9 April 2015, http://ourdocuments.gov/doc.php?flash=true&doc=56. For a scholarly treatment of the Corollary, see Serge Ricard, "The Roosevelt Corollary," *Presidential Studies Quarterly* 36, no.1 (2006): 17–26, http://www.jstor.org/stable/27552743.

7. Geddes W. Rutherford, "Spheres of Influence: An Aspect of Semi-Suzerainty," *American Journal of International Law* 20, no. 2 (1926): 300–25, http://www.jstor.org/stable/2188919. This is one of the few formal discussions of the international legal nuances of spheres of influence.

8. Paul Keal, "Contemporary Understanding about Spheres of Influence," *Review of International Studies* 9 (July 1983): 156, http://www.jstor.org/stable/20096980.

9. Geoffrey Roberts, "Ideology, Calculation, and Improvisation: Spheres of Influence and Soviet Foreign Policy 1939–1945," *Review of International Studies*, 25 (October 1999): 657, http://www.jstor.org/stable/20097627.

10. For an exploration of the term, see especially Alastair Iain Johnston, "How New and Assertive Is China's New Assertiveness?" *International Security* 37, no. 4 (2013): 7–48, doi:10.1162/ISEC_a_00115.

11. Dai Bingguo, "*Zhongguo guowu weiyuan Dai Bingguo: zhichi zou heping fazhan daolu*" ["State Councilor Dai Bingguo: Adhere to the Path of Peaceful Development"], *Zhonghua Renmin Gongheguo zhongyang renmin zhengfu* [Central People's Government of the People's Republic of China] web site, 6 December 2010, http://www.gov.cn/ldhd/2010-12/06/content_1760381.htm.

12. Ibid.

13. Dai Bingguo, "Speech by Dai Bingguo at China-US Dialogue on South China Sea Between Chinese and US Think Tanks," Ministry of Foreign Affairs, People's Republic of China, 5 July 2016, accessed 20 July 2016, http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1377747.shtml.

14. Li Zhonglin, "*Ping suowei Zhongguo ban 'Menluo zhuyi'* " ["Comment on the so-called 'Chinese Monroe Doctrine' "], *Heping yu fazhan* no. 4 (2013): 103–15; and Yang Cheng, "*Zhōngguó bǎn mén luó zhīyì e cuòwù zhījué*" ["The Misperception of 'China's Monroe Doctrine' "], *Dongfang zaobao*, 19 May 2014, A09.

15. Zheng Xiwen, "No Asian Monroe Doctrine," *China Daily*, 29 September 2014, http://www.chinadaily.com.cn/opinion/2014-09/29/content_18679191.htm.

16. Wang Yiwei. "Outsiders Unreliable as Security Providers," *Global Times* (China), 7 July 2014, http://www.globaltimes.cn/content/869253.shtml.

17. Jin Canrong, and Duan Haowen, "New Features of the Surrounding International Environment and China's Response," *Contemporary International Relations* (English) 23, no. 6 (2013): 30, http://caod.oriprobe.com/articles/40849005/New_Features_of_the_Surrounding_International_Envi.htm.

18. Ji Zhiye, "The Pacific Ocean Is Wide Enough for All: Thoughts on Building a TPSCA," *Contemporary International Relations* 24, no. 6 (2014): 17, http://caod.oriprobe.com/articles/43723600/The_Pacific_Ocean_Is_Wide_Enough_For_All.htm.

19. Han Caizhen and Shi Yinhong, "Bottlenecks in East Asia's Regional Cooperation," *Contemporary International Relations* (English) 24, no. 3 (2014): 30–31, http://caod.oriprobe.com/articles/42219254/Bottlenecks_in_East_Asia_s_Regional_Cooperation.htm.

20. Chen Xiangyang, *Zhongguo mulin waijiao: sixiang, shijian, qianzhang* ["China's Good-Neighbor Diplomacy: Thought, Practice, Prospect"]. (Beijing: Shishi Chubanshe, 2004), 290.

21. Xinhua, "Commentary: America the Kibitzer on South China Sea," Xinhua News Agency, 21 March 2015, http://eng.mod.gov.cn/Opinion/2015-03/21/content_4576041.htm; Xinhua, "China Urges U.S. to Be Impartial in South China Sea," Xinhua News Agency, 22 January 2015, http://news.xinhuanet.com/english/china/2015-01/22/c_133939681.htm.

22. "Clinton Must See China's Territorial Stance," *Global Times* in *People's Daily*, 5 September 2012, http://english.peopledaily.com.cn/90883/7936254.html.

23. Feng Zhongping, "Periphery Strategy Should Focus on Innovative Security Cooperation," *Contemporary International Relations* (English) 23, no. 6 (2013): 53, http://caod.oriprobe.com/articles/40849000/Periphery_Strategy_Should_Focus_on_Innovative_Secu.htm.

24. Hillary Clinton, "America's Pacific Century," *Foreign Policy* 189 (11 October 2011): 56–63, http://www.jstor.org/stable/41353253.

25. *China's Foreign Affairs 2012* (Beijing: Ministry of Foreign Affairs), 4. *China's Foreign Affairs (Zhongguo waijiao* 中国外交) is the official yearbook of China's Foreign Ministry, usually published in March and covering the previous year's events; *China's Foreign Affairs 2015*, for instance, covers 2014. There are English as well as Chinese versions, and they are very close translations.

26. Ibid., *2013*, 4, 309.

27. Ibid., *2014*, 12–14.

28. Ibid., *2003*, 8.

29. Ibid., *2003*, 11.

30. Ibid., *2003*, 13, 15.

31. Ibid., *2002*, 2.

32. Ibid., *2004*, 3.

33. Ibid. *2004*, 4–5.

34. Ibid., *2004*, 8.

35. Ibid., *2005*, 7–8.

36. Ibid., *2006*, 5, 15.

37. Ibid., *2007*, 18.

38. Ibid., *2008*, 1.

39. Ibid., *2008*, 4, 5.

40. Ibid., *2009*, 4.

41. Ibid., *2011*, 4, 18.

42. Li Yonghui, "Constructing a Strategic Peripheral Belt to Support the Wings of China's Rise," *Contemporary International Relations* (English) 23, no. 6 (2013): 66, http://caod.oriprobe.com/articles/40849009/China_s_Neighboring_Diplomacy_Demands_Top_level_De.htm.

43. Ibid., 68–69.

44. Ji Zhiye, "China's Neighboring Diplomacy Demands Top-level Design," *Contemporary International Relations* (English) 23, no. 6 (2013): 4, http://caod.oriprobe.com/articles/40849009/China_s_Neighboring_Diplomacy_Demands_Top_level_De.htm.

45. Ibid., 4.

46. Xi Jinping, "New Asian Security Concept for New Progress in Security Cooperation," 5 May 2014, "Remarks at Fourth Summit of the Conference on Interaction and Confidence Building Measures in Asia," Ministry of Foreign Affairs, People's Republic of China, http://www.fmprc.gov.cn/mfa_eng/ zxxx_662805/t1159951.shtml. CICA was founded in 1999 and encompasses a large number of countries from Egypt and the Middle East, South Asia, Central Asia, and East Asia. The United States and Japan are observers, and South Korea is a member. http://www.s-cica.org.

47. Paula S. Harrell, *Asia for the Asians: China in the Lives of Five Meiji Japanese* (Portland, ME: MerwinAsia, 2012), 21. The Chinese text was *Yazhou guojia zhudao Yazhou shiwu* 亚洲国家主导亚洲事务. The noun should be translated as "Asian countries" and the translated verb could also be "leading," "guiding," or "dominating," while *Yazhou shiwu* 亚洲事务 should be translated as "Asian affairs." Konoe's exact words were, "*Tōyō mondai wa hitori tōyō no mondai ni arazu, sekai no mondainai. . . . Tōyōjin hitori tōyō mondai o kessuru no kenri nakarubekarazu*" 東洋人独り東洋問題を決するの権利なかるべからず ("Orientals alone should solve the Orient's problems."). He then goes on to specifically discuss a Monroe Doctrine for Asia.

48. Cui Heng, "The Strategic Coupling of Sino-Russian Relations," China.org.cn [State Council Information Office], 25 May 2014, http://www.china.org.cn/opinion/2014-05/25/content_32473565.htm.

49. Xi Jinping, "New Asian Security Concept."

50. Xu Qingchao, "*Zhongguo xin Yazhou waijiao bushi Zhongguo ban 'Luomen zhuyi*,' " *Zhongguo shehui kexue bao*, 18 July 2014, A07 (no longer available). Sourced from China Academic Journals Full-Text Database, accessed 16 June 2015, http://oversea.cnki.net.

51. Wang Yiwei, "Outsiders Unreliable as Security Providers."

52. Yang Cheng, "The Misperception of 'China's Monroe Doctrine.' "

53. Yan Xuetong, "Diplomacy Should Focus on Neighbors," *China Daily*, 27 January 2015, http://usa.chinadaily.com.cn/epaper/2015-01/27/content_19419558.htm.

54. Caitlin Campbell, Ethan Meick, Kimberly Hsu, and Craig Murray, *China's "Core Interests" and the East China Sea* (Washington, DC: US-China Economic and Security Review Commission Staff Research Backgrounder, 2013), 2, http://www.uscc.gov/sites/default/files/Research/China%27s%20Core%20Interests%20and%20the%20East%20China%20Sea.pdf.

55. Edward Wong, "Security Law Suggests a Broadening of China's 'Core Interests,' " *New York Times*, 2 July 2015, http://www.nytimes.com/2015/07/03/world/asia/security-law-suggests-a-broadening-of-chinas-core-interests.html.

56. Campbell, Meick, Hsu, and Murray, *China's "Core Interests*," 4.

57. US State Department, Bureau of Oceans and International Environmental and Scientific Affairs, *Limits in the Seas: China: Maritime Claims in the South China Sea*, no. 143 (Washington DC: US State Department, December 2014), http://www.state.gov/documents/organization/234936.pdf; and Liselotte Odgaard, "Op-Ed: China's dangerous ambiguity in the South China Sea," *New York Times*, 10 December 2015, http://www.nytimes.com/2015/12/11/opinion/chinas-dangerous-ambiguity.html.

58. "Foreign Ministry spokesperson Lu Kang's regular press conference on October 27, 2015," Ministry of Foreign Affairs, People's Republic of China, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/ s2510_665401/2535_665405/t1309625.shtml.

59. Nobuhiro Kubo, Tim Kelly, and David Brunnstrom, "Exclusive: Japan Considering Joint U.S. Air Patrols in South China Sea—Sources," Reuters, 29 April 2015, http://www.reuters.com/article/us-usa-japan-southchinasea-idUSKBN0NK15M20150429.

60. "Foreign Ministry Spokesperson Lu Kang's regular press conference on October 27, 2015"; and Yeganeh Torbati, "'Hope to See You Again': China Warship to U.S. Destroyer after South China Sea Patrol," Reuters, 5 November 2015, http://www.reuters.com/article/us-southchinasea-usa-warship-idUSKCN0SV05420151106.

61. Ben Blanchard, "China Says U.S. Welcome to Use Civilian Facilities in South China Sea," Reuters, 30 April 2015, http://www.reuters.com/article/us-china-usa-southchinasea-idUSKBN0NM31620150501.

62. "Crossing a Line in the Sky," *The Economist* (30 November 2013): 44, http://www.economist.com/news/asia/21590926-what-chinas-new-air-defence-zone-over-disputed-islands-says-about-its-foreign-policy-crossing-line; and "Regional Turbulence: the East China Sea," *The Economist* (30 November 2013), 39, http://www.economist.com/blogs/banyan/2013/11/east-china-sea. An Air Defense Identification Zone was a legal concept developed during the Cold War to force nearby aircraft to identify themselves well before they cross into sovereign airspace. Japan has had an ADIZ around it since 1969. These have been self-proclaimed zones since the Cold War, and many other countries have announced them.

63. Jane Perlez and Martin Fackler, "China Patrols Air Zone over Disputed Islands," *New York Times*, 28 November 2013, http://www.nytimes.com/2013/11/29/world/asia/japan-south-korea-fly-military-planes-in-zone-set-by-china.html.

64. "Foreign Ministry Spokesperson Qin Gang's regular press conference on November 25, 2013," http://az.china-embassy.org/eng/fyrth/t1102346.htm.

65. Lin Hongyu, "Sino-Japanese Relations and ADIZ," *Contemporary International Relations* (English) 24, no. 2 (2014): 17, http://caod.oriprobe.com/articles/42280892/Sino_Japanese_Relations_and_ADIZ.htm.

66. Cao Qun, "*ZhongMei fangkong shibiequ guize shi fou cunzai fenqi?*" ["Are there Differences between Chinese and American Rules Governing Air Defense Identification Zones (ADIZ)"], *Dangdai YaTai* [*Journal of Contemporary Asia-Pacific*], no. 2 (2014): 27–53.

67. Jane Perlez, "After Challenges, China Appears to Backpedal on Air Zone," *New York Times*, 27 November 2013, http://www.nytimes.com/2013/11/28/world/asia/china-explains-handling-of-b-52-flight-as-tensions-escalate.html.

68. Toshi Yoshihara, "China's Vision of its Seascape: the First Island Chain and Chinese Seapower," *Asian Politics & Policy* 4, no. 3 (July–September 2012): 294, doi:10.1111/j.1943-0787.2012.01349.x. A Lexis/Nexis search of Xinhua, *People's Daily*, and *Global Times* online showed no hits in the early 1990s and only three hits between 1994 and 2002, but by 2015 there were eleven hits on the phrase "first island chain."

69. Bernard D. Cole, *Asian Maritime Strategies: Navigating Troubled Waters* (Annapolis: Naval Institute Press, 2013), 96–97.

70. Brian Mitchell, "China's Growing Military Power Creating Trouble for U.S. in Pacific," *Investor's Business Daily*, 24 April 2001, http://www.lexisnexis.com.libgateway.susqu.edu/lnacui2api/api/version1/getDocCui?lni=42WN-T6X0-003M-X0VH&csi=270944,270077,11059,8411&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true.

71. Robert D. Kaplan, *The Revenge of Geography: What the Map Tells Us About Coming Conflicts and the Battle Against Fate* (New York: Random House 2013), 215; and Kaplan, "While U.S. Is Distracted, China Develops Sea Power," *Washington Post*, 26 September 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/24/AR2010092404767_pf.html.

72. Simon Winchester, "Op-Ed: China's Pacific Overtures," *New York Times*, 6 November 2015, http://www.nytimes.com/2015/11/07/opinion/chinas-pacific-overtures.html.

73. Li Kaisheng, "Tokyo's Meddling in South China Sea Puts Bilateral Ties, Regional Peace at Risk," *Global Times* (English), 2 December 2015, http://www.globaltimes.cn/content/956216.shtml.

74. Gilbert Reid, "An Imitation Monroe Doctrine," *Journal of Race Development* 6, no. 1 (July 1915): 12–22, doi:10.2307/29738098.

75. Chen Xiuwu, "*Riben de 'Yazhou Menluo zhuyi'* " ["Japan's 'Asia Monroe Doctrine' "], *Waiguo wenti yanjiu* 214, no. 4 (2014): 3–8.

76. John Kerry, "Remarks on U.S. Policy in the Western Hemisphere," US Department of State, 18 November 2013, http://www.state.gov/secretary/remarks/2013/11/217680.htm.

77. Sun Hongbo, "*Meiguo gaobie 'Menluo zhuyi,' de yingxiang ji weilai de MeiLa guanxi*" ["America Bids Farewell to the 'Monroe Doctrine's' Influence and the Future of US-Latin American Relations"], *Dangdai shijie* [*Contemporary World*] no. 3 (2014): 37–40; Zhao Lingmin, "*Meiguo gaobie 'Menluo zhuyi*?' " ["America Says Farewell to the 'Monroe Doctrine?"], *Huaxingbao*, no. 23 (28 November 2013): 1–2; Xing Yue, "*San wen 'Men Luo zhu yi*' " ["Three Questions about the Monroe Doctrine"], *Zhongguo shehui kexue bao* [China Social Sciences], International Edition, B04 (12 February 2014), 1–2; Sun Xihui "*Menluo zhuyi' zhi hui zhongjie ma*?" ["Can the 'Monroe Doctrine' Rally Be Ending?"], *Xin Shijie* [*New Horizons*] 39, no. 1 (2014): 80–81.

78. It should be noted here that although China does use the term "neighbor" (*linguo* 邻国) in reference to adjacent, proximate, and regional states, including states such as the Philippines, Vietnam, and Japan, with which China has territorial disputes, it does not consider Taiwan to be a neighbor since it is not considered an independent state. The Chinese social analogy to Taiwan is that of family.

79. This is a policy that Chinese scholars are well aware of. See Li Zhonglin, "*Indu de Menluo zhuyi pingxi*" ["An Analysis of India's Monroe Doctrine"], *YaFei Zongheng*, no. 4 (2013): 15–21.

80. *China's Foreign Affairs 2015*, 3.

81. John Pomfret, "US Takes a Tougher Tone with China," *Washington Post*, 30 July 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/29/AR2010072906416.html.

Prohibiting Interference with Space-Based Position, Navigation, and Timing

Jonty Kasku-Jackson

Abstract

The United States must lead the way in establishing a norm prohibiting interference with satellites and satellite control segments of space-based position, navigation, and timing (PNT) systems. This norm would not prohibit interference with end user equipment and would be consistent with the just war principles of proportionality and discrimination. Prohibiting interference would address potential escalation concerns. These concerns could also be minimized through certain transparency and confidence-building measures (TCBM), including (1) creating a common set of definitions, (2) expressing a noninterference declaratory policy, and (3) information-sharing agreements.

* * * * *

After the launch of the first satellites by the United States and the Union of Soviet Socialist Republics (USSR) in the late 1950s, numerous foundational, space-related norms of behavior were developed and eventually codified into a series of treaties, the last of which was signed in 1975. Currently it appears unlikely any new space treaties will be agreed upon. This is due to the large number of states with potentially divergent interests and concerns. Among those concerns is the view that retaining the ability to interfere with space capabilities is of greater benefit than retaining access to space capabilities. Even though a new space treaty is unlikely, norms not codified in a treaty still can be useful in favorably shaping behavior in space. Additionally, the strategic environment in which those original norms were established has changed significantly. Instead of two emergent space powers, many states now have a presence in space. Of these, some are full-fledged, established space powers

---

Jonty Kasku-Jackson is a strategy and policy analyst and instructor at the National Security Space Institute (NSSI). She has worked in the space field since 1998, first in Air Force Space Command and then the NSSI. She is a former USAF intelligence officer and earned a juris doctor degree from the New England School of Law in Boston.

with their own organic ability to launch indigenous satellites. Others are emerging space powers with the ability to manufacture and operate their own spacecraft. Finally, numerous aspiring space powers may have space programs but do not yet have the capability to access space services through means other than purchasing them. Significantly, those aspirants are relying on others for space-based position, navigation, and timing (PNT) capabilities. Perhaps more importantly, numerous non-state international and commercial entities also use space-based PNT to pursue their interests. Those interests range from purely commercial economic interests to internationally recognized safety of navigation and safety of life obligations. Non-state entities, as well as established, emerging, and aspiring space powers, are concerned about losing space-based PNT capability during a conflict. In addition, there is great concern that a loss of space-based PNT could lead to an escalated conflict in space or expand from a conflict in space to a terrestrial conflict.

While current space treaties recognize space should be used for "peaceful purposes," the term "peaceful purposes" is not defined.[1] The Outer Space Treaty (OST) does require states to conduct their activities in space with due regard to the interests of other states and to undertake consultations in the event their space activities could potentially interfere with another state's peaceful exploration and use of outer space.[2] However, the OST can be suspended between belligerents during a time of conflict.[3] Additionally, currently no treaties specifically address interference with space-based PNT. This could be an issue since states, non-state international organizations, and commercial entities directly and indirectly rely heavily on space-based PNT capabilities.

Space-based PNT systems consist of satellites, control segments, and end user receivers. Intentional and unintentional interference with the end user receivers has become common enough on military battlefields that the military has developed tactics, techniques, and procedures (TTPs) to specifically address the issue. However, there is increasing concern that the satellites themselves or the control segment could be interfered with, which could have a far-reaching, global impact to all users regardless of whether they are on, or near, a particular battlefield. Interference consists of jamming, spoofing, cyber attack, or physical harm to the satellite or control segments of a space-based PNT system to degrade or disrupt the position or timing signal transmitted.

The United States continues to lead the way in assuring the availability of space-based PNT services. It has clearly recognized the importance of ensuring space-based PNT is available to the rest of the world, both in its policy actions and its space system acquisition actions. In May 2000 the United States discontinued its use of selective availability (SA), which could be used to degrade the PNT signal, and stated it had no intent to ever use SA again.[4] In 2007, the United States went so far as to announce to the world at an International Civil Aviation Organization (ICAO) assembly that it would procure future satellites without SA capability and that GPS III would "deliver signals without any compromise in precision—guaranteed."[5] According to the 2010 US National Space Policy, the United States will "provide continuous worldwide access, for peaceful civil uses, to the Global Positioning System (GPS) and its government-provided augmentations, free of direct user charges."[6]

It is also critical for the United States to retain the ability to use space-based PNT information for its military activities. It makes sense for the United States to lead the way in codifying a norm that prohibits interference with the satellite and control segments of a space-based PNT system during peacetime, crisis, or conflict. Such a proposed norm would not prohibit interference with end user equipment. The norm would be consistent with the long-established just war principles of proportionality and discrimination and would preserve a state's ability to protect itself against precision-guided weapons that rely on space-based PNT. Prohibiting interference with the satellite and control segments of space-based PNT could address potential escalation concerns as well as concerns about significant impacts to international obligations if space-based PNT were unavailable as a result of interference.

This article does not address the localized interference with the end user receivers, which has become almost commonplace and which is confined to a small area rather than a global phenomenon. It first discusses how and by whom space-based PNT is used. Users of space-based PNT vary among military, nonmilitary, and civil and commercial entities in pursuit of an extremely wide variety of interests and activities. Next, it explores the emerging noninterference norm and how it is built on current practices and policies. It also discusses how support for the norm can be extrapolated from norms codified in treaties other than the OST. Finally, it explains how a norm prohibiting interference with the satellite and ground-control segments of space-based PNT, and a norm's

associated transparency and confidence-building measures, are in the best interest of the United States and why they should be incorporated into a considered set of deterrence options.

Space-Based PNT Uses

In the 1950s there were two emergent space powers: the United States and the Soviet Union. Today, there are approximately 60 countries with some sort of presence in space. This presence varies from those such as the United States, Russia, and China, which have a full range of space capabilities, to states like Argentina and Malaysia that are only present in space because of their commercial satellite communications sector. Even the city-states of Singapore and Monaco have a satellite in space. Moreover, a number of non-state players such as commercial consortia and international civil users are also present in space. For example, Intelsat, Eutelsat, SES, and Iridium together own and operate approximately 215 communications satellites; the Regional African Satellite Communications Organization also has a satellite in space. (See appendix for a complete list of states and organizations present in space at the time of this article's writing.)

All these players use space-based PNT capabilities to provide precise orbit determination. Moreover, virtually all states, regardless of whether they own or operate satellites, have some sort of direct reliance on space-based PNT. For example, major communications networks, banking systems, financial markets, and power grids depend heavily on GPS for precise time synchronization. Additionally space-based PNT is used for surveying and mapping, agricultural activities, collecting data regarding the environment, highway and rail transportation, facilitating public safety and disaster relief, and increasing the safety of aviation and marine operations.[7]

Additionally, space-based PNT information is important to international norms regarding safety of life. The *Cosmicheskaya Systyema Poiska Aariyniyich Sudov* (COSPAS)[8] Search and Rescue Satellite Aided Tracking (SARSAT) is an international organization that provides space-based relay of distress signals or alerts from emergency beacons to search and rescue (SAR) authorities internationally.[9] During 2014, close to 2,400 people were rescued during approximately 700 SAR events.[10] SARSAT has been credited with saving 32,000 lives since 1982.[11] Currently 15 percent of the COSPAS-SARSAT locator beacons rely on the US GPS, but future enhancements plan to use two additional space-based PNT

systems: the Russian GLONASS and European Galileo systems.[12] Use of the space-based PNT capabilities is expected to reduce detection and tracking of a beacon to a few minutes rather than a few hours.[13] Additionally, the International Maritime Organization (IMO) has required ships to implement the Global Maritime Distress and Safety System (GMDSS) since 1988, and COSPAS-SARSAT is part of that system.[14] It is important to note participants in COSPAS-SARSAT include both states and non-state international organizations, demonstrating the widespread acceptance of the importance of space-based PNT for safety of life.[15] The inclusion of two additional space-based PNT systems indicates the increasing reliance on those capabilities for the accuracy critical to search and rescue missions.

US Use of Space-Based PNT

With such ubiquitous reliance on space-based PNT, the question of whether interference with the satellite or control segments should be allowed has become urgent. This question is especially germane to the United States. According to Joint Publication 3-14, *Space Operations*, space capabilities in general *enable* the application of the principles of joint operations.[16] However, it also states, "National security objectives and the needs of the supported commander compel the conduct of space operations,"[17] thus indicating the reliance of the United States on space capabilities when conducting military operations. When considering the space capabilities that enable joint operations, space-based PNT assets in particular provide a foundation for a number of other space force enhancement capabilities. While the positional capability is often the capability that comes to mind when considering PNT, it is the precision-timing aspect of PNT that provides the capability to synchronize operations, enable communications capabilities, and enable network and cryptologic synchronization. Space-based PNT also enables precision attack from standoff distances, which reduces collateral damage and US losses.[18] The substantial reliance the United States places on space-based PNT for military operations is reflected in JP 3-14, asserting the necessity to assure friendly use of PNT information and prevent adversary use through deliberate defensive and offensive actions.[19]

Arguably, the United States has an asymmetric advantage in counter-space capabilities, which it might be reluctant to give up. However, that advantage appears to be eroding as Russia and China increase their

counter-space capabilities and indicate their willingness to interfere with satellites.[20] As potential adversaries continue to make progress and US advantage diminishes, it is even more important to assure the integrity of the control and satellite segments of US space-based PNT to ensure the United States can continue to conduct activities at the times and places of its choosing. If interfering with the satellite and control segments of space-based PNT is prohibited, then space-based PNT information should remain available outside a particular battlefield, even though the United States might face localized interference with the end user receivers on that battlefield.

With such a global use of space-based PNT capabilities, one might assume there would be well-established norms of behaviors concerning use of and interference with the use of those capabilities. That assumption would be reinforced by the fact there are organizations dedicated specifically to space-based PNT. For example, The International Committee on Global Navigation Satellite Systems (ICG) was established in 2005 to promote voluntary cooperation on matters of mutual interest to civil space-based PNT.[21] It encourages coordination among providers of space-based PNT, regional systems, and augmentations to ensure greater compatibility, interoperability, and transparency.[22] However, neither the charter of the ICG or other organizations nor the ways in which space-based PNT is used currently explicitly identify any norms about whether interference is prohibited. In the absence of explicit norms, it could be argued that a norm prohibiting interference could actually be emerging since the expectation seems to be that space-based PNT is, and will continue to be, freely available to all users at all times. Since the United States has continually led the way in providing space-based PNT to the world, it is in a particularly good position to lead an effort to codify that expectation into a norm that prohibits interference with the satellite and control satellite segments of space-based PNT.

Development of Noninterference with a Space-Based PNT Norm

In order to understand the rationale behind prohibiting interference with space-based PNT, it is necessary to understand specifically what norms are and how they develop. Norms are commonly understood to be agreed-upon rules for acceptable behavior or conduct.[23] They are internalized and socialized as universal principles guiding international be-

havior. They set standards, encourage good behavior, and discourage bad behavior. They are developed to protect a state's national security and its economic and societal interests in context of the surrounding strategic environment. A norm will only be adopted if it is beneficial (or at least not harmful) to the parties involved. The incredibly widespread use of space-based PNT capabilities, the multitude of uses for space-based PNT, and the fact that space-based PNT capabilities facilitate other capabilities have created an international geopolitical situation in which the availability of space-based PNT is not only desired but is also expected. Arguably, a norm prohibiting interference with space-based PNT is emerging.

The Outer Space Treaty (OST), the primary, overarching space treaty, reflects the broad foundational norms created around fear of nuclear conflict. The numerous space-related norms of behavior that developed during the dawn of the space age were codified in a series of space treaties.[24] Due to the strategic environment of the time, they focused in large part on the prevention of a nuclear war in or from space as an extension of deterrence of terrestrial nuclear war. The space treaties addressed national security, protection of personnel, safety of space activities, and protection of the space environment. Prior to the signature of the OST, nonbinding United Nations General Assembly (UNGA) resolutions reflected those concerns and emerging norms of behavior. The OST cites two UNGA resolutions in addition to the Declaration of Principles for the use of outer space.[25] The resolution relevant to this discussion called on states to refrain from placing nuclear weapons or weapons of mass destruction into orbit or on celestial bodies.[26]

Those norms developed because the Soviet Union and the United States were the only two space powers and could impose order on their respective blocks. No others had any kind of presence in space and effectively had little influence in developing the space norms that were eventually codified in treaties. Since the greatest fear of the United States and Soviet Union at the time was that weapons placed in orbit or on the moon would be destabilizing, it is not surprising that norms about weapons of mass destruction were codified in the OST. However, the concerns of those with a presence in space today are not the same. Those present in space are concerned with being able to use space capabilities to pursue their security, economic, and societal development interests. In particular, they are concerned with being able to use space-based PNT to do so. Those actors are now in the position of shaping an emerging noninterference norm.

Norms are applicable in times of peace, crisis, and conflict. Peacetime norms developed to maintain peace, facilitate commerce, and protect safety of life and navigation. The IMO requires all ships to be fitted with certain search and rescue equipment. One such type of equipment is an emergency position-indicating radio beacon designed to specifically work with COSPAS-SARSAT. Using the space-based PNT portion of COSPAS-SARSAT increases the accuracy of location data to approximately 20 meters from five kilometers.[27] Additionally, space-based PNT has become the primary means of navigation in many maritime applications.[28] The International Civil Aviation Organization also requires aircraft to install emergency locator transmitters.[29] Clearly, space-based PNT capabilities are critical to meeting international obligations regarding protecting the safety of life and navigation. The noninterference norm for peacetime is, in effect, already being established.

Norms for crises and conflict have developed to reduce misperceptions, misunderstanding, and mistrust and to avoid conflict or prevent escalation of a conflict but are not yet formally established. Although a norm may be widely accepted, states may differ in their interpretation of the norm or the actions they can take to implement it. One indication a norm has been widely adopted is its codification in official, binding international treaties as has occurred with the OST. As previously mentioned, an explicit norm for noninterference with the satellite and control segments of space-based PNT has not yet occurred but may be emerging. Norms also may be inferred from the provisions and terms of binding international treaties or from nonbinding instruments such as UNGA resolutions and codes of conduct.

How Are Norms Developed?

Traditionally, norm development has been the purview of state actors. Norms were developed when (1) leading states proposed a new norm, (2) a majority of states followed the proposal, and (3) the norms then were internalized and socialized as universal principles.[30] Norms are typically developed when a large number of states agree on acceptable standards of behavior and conduct their actions accordingly. However, as ever more non-state entities increasingly rely on space-based PNT capabilities to pursue both economic and national security interests, they also are helping to develop a new space norm. Specifically, the development and implementation of agreed-upon standards, practices, and procedure

have become a key factor. This type of norm development, where a large number of entities determines agreed-upon behavior, may also draw on UNGA resolutions and reports. While a resolution is not binding, it does reflect the beliefs of those who sign it. It has been common for this type of norm, developed in this way, to eventually be codified in a binding multilateral treaty much like the 1958 Geneva Conventions on the Law of the Sea codified norms already being practiced.[31] However, it should be noted that there have been no post–World War II examples of norms in general emerging in this manner. Arguably, the norm against using nuclear weapons emerged in this manner and was codified in the numerous bilateral arms control agreements between the United States and Soviet Union. However, that norm was relevant only to those two nuclear powers. Certainly no space-related norms have emerged in this way.

Alternatively, norms may develop when relatively few players with a large interest in the area of concern determine acceptable behavior. This is essentially the model by which the OST came into being. Another good example is found in international civil aviation law. In 1944, only 52 countries signed the Chicago Convention, and for the most part they were those with established or emerging air capabilities.[32] As of 2013, 191 nations had signed the Chicago Convention. Arguably, noninterference with space-based PNT is becoming, or has become, a norm in a similar manner. Since the mid-1990s, only four states and the European Union have developed a space-based PNT capability, and no non-state players have done so. Virtually all states and numerous commercial and international civil entities rely on space-based PNT provided by one of those five states to some extent as they pursue their security and economic interests. For instance, the Chinese Beidou Satellite Navigation System, used by the Chinese government and military, also has been offering navigation services to customers in the Asia–Pacific region since December 2012.[33] Additionally, the Chinese system has been approved for use in maritime operations by the Maritime Safety Committee of the IMO.[34] In another example, the Russian GLONASS services have been freely available to civilian users since May 2007, and Russia has been actively promoting civil use of GLONASS.[35] Finally, the United States has issued a number of statements establishing cooperation relationships with other states with space-based PNT capabilities, as well as those without indigenous space-based capabilities.[36]

These same countries plus India, Japan, and the European Space Agency (ESA) also participate in a number of other international organizations regarding space-based PNT issues.[37] The ICG encourages coordination among providers of space-based PNT systems regional systems and augmentations to ensure greater compatibility, interoperability, and transparency.[38] The ICG serves as a focal point for information exchange on space-based PNT. It has 10 state members (to include the European Union) plus the ESA. It has 11 associate members (to include non-state and commercial organizations) and eight observers.[39] It also promotes the introduction and utilization of space-based PNT in developing countries.[40] Another international organization, United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER), also comprises non-state entities as well as state entities. UN-SPIDER ensures all states, international organizations, and regional organization have access to, and develop the capacity to use, all types of space-based information to support the full disaster-management cycle.[41] This information includes space-based PNT as well as remote sensing and satellite communications information. Both of these organizations are composed of non-state entities, states with no indigenous space capabilities, and states that provide space-based PNT.

This widespread dependency on a very small number of states for space-based PNT and the willingness by those states to ensure space-based PNT is globally available are key factors in the emergence of a noninterference norm. The combination of a relatively few, heavily vested players with a large number of dependent users has effectively established the expectation that space-based PNT will always be available for use by all who wish. This expectation arguably was set by the United States itself in 1983 when the Soviet Union shot down Korean Airlines Flight 007, which the Soviet Union claimed had intruded into Soviet airspace. The incident was so horrendous it was widely denounced by the world. Recognizing the critical need for civilian aircraft to know their precise position, Pres. Ronald Reagan immediately declared the United States would provide three-dimensional positional information to civilian airliners when its GPS came online. The United States reinforced the expectation of availability by its actions in 2000 and 2007. Expectation of space-based PNT's continued availability was also strengthened internationally beginning in 1999 when the Third United Nations Conference on the Exploration and Peaceful Uses of Outer Space (UNISPACE III) adopted a strategy

to address global challenges of the future by using space capabilities. One action of that strategy was to "improve the efficiency and security of transport, search and rescue, geodesy and such by promoting universal access to space based PNT."[42]

Expectation regarding ever-present availability of space-based PNT has been further reinforced by the existence of organizations such as the previously mentioned ICG and UN-SPIDER. In addition to illustrating the emerging expectation and potential obligation to ensure the availability of space-based PNT, participation in these organizations also provides formal institutional structures to monitor compliance, adjudicate disputes, and provide a forum for regular discussion of space-based PNT issues. The structures provide known processes and organizations so that all parties are familiar with expectations associated with the emergent norms.

A New Norm for Space-Based PNT

The next step in defining and codifying an emerging norm prohibiting interference with space-based PNT is to understand current norms and the rationales behind those norms and associated transparency and confidence-building measures (TCBM). A large part of international maritime, aviation, and land law developed in response to codifying the norm of promoting or maintaining peace. UNGA resolutions and international treaties clearly reflect the importance of maintaining peace and stability between the United States and the Soviet Union. Agreements that codified that norm and its associated TCBMs included bilateral, nonbinding arms control agreements as well as multilateral aviation, naval, and environmental-modification agreements. Unlike the space treaties, each treaty contained language specifically reflecting the desire to avoid conflict. It is possible language found in those treaties could be useful in defining specific language for a norm prohibiting interference with the satellite and control segments of space-based PNT. For example, the United Nations Convention on the Law of the Sea (UNCLOS) states it is "aware of the historic significance of this Convention as an important contribution to the maintenance of peace, justice and progress for all peoples of the world."[43] The Convention of Civil Aviation (Chicago Convention) declares "it is desirable to avoid friction and to promote that cooperation between nations and peoples upon which the peace of the world depends."[44] Article 1 of the United Nations Charter states the UN's purpose is to "maintain international peace and security."[45] Even the

Environmental Modification Convention explicitly states it is "guided by the interest of consolidating peace, and wishes to contribute to the cause of halting the arms race, and of bringing about general and complete disarmament under strict and effective international control, and of saving mankind from the danger of using new means of warfare."[46]

A norm that prohibits interference with the satellite and control segments of space-based PNT, but that retains the right to interfere with the end user equipment, should likewise be grounded in the concept of promoting or maintaining peace. The use of space-based PNT is essential to both maritime and aviation safety of life activities and also essential for disaster mitigation and state capacity building. Language defining the noninterference norm should reflect this. Such language should also act to move the issue outside the space law arena, which is narrowly defined, less mature, and often viewed as insular from other areas of international law. Similar to the UNCLOS language, noninterference language should explicitly recognize that space-based PNT is an important contributor to the preservation of peace and progress for all peoples of the world. It should also promote cooperation as the Chicago Convention does. Finally, it should explicitly state that it is desirable to prevent conflict in outer space.

The challenge to defining a noninterference norm is balancing ongoing expectations and acceptable practices with other established norms. According to the foundational norms codified in the space treaties, space is to be used for peaceful purposes. Article I of the OST states, "Activities in outer space . . . are to be conducted for peaceful purposes"[47] and Article IX of the OST specifies that states are to conduct space operations "with due regard" to the corresponding interest of all other state parties to the treaty.[48] Adding to the tension, the OST says, "States shall carry out activities in outer space . . . in accordance with international law to include the United Nations Charter."[49] Article 51 of the UN charter, which allows for self-defense in the event of "armed attack," therefore applies. States may, and do, interpret armed attack and self-defense differently. Interfering with space-based PNT might or might not be interpreted as an armed attack that requires a response—a response that might be escalatory either in space or on earth. Additionally, those states that rely heavily on space-based PNT for military operations might be so concerned about possibility of interference they might attempt to preemptively disable an adversary's capability. Since states cannot agree on the interpretation of "peaceful purposes" or "armed

attack" it is extremely difficult to determine acceptable behavior or conduct regarding interference with space-based PNT.

Currently, discussions seem to center around how much interference is necessary before a response is appropriate. A norm prohibiting any interference whatsoever with the satellite and control segments of space-based PNT would eliminate that debate. Since the United States relies more on space-based PNT than its potential adversaries, it is vital that it retain access to space-based PNT information. It might even be argued that it is more important the United States retain its own access to uncorrupted space-based PNT information than it is to deny an adversary access to space-based PNT information. Additionally, interference with the satellite or control segment could be more likely to create effects outside a single battlefield, thereby impinging on the United States' ability to conduct other activities outside a particular battlefield. Appropriate TCBMs would clarify the interpretation of the norm and establish the consequences for failure to adhere to the norm.

Preserving the long-established self-defense norm must be balanced against safety of life and safety of navigation. Space-based PNT capabilities are critical to the safety of navigation and safety of life across the world. Norms regarding safety of navigation and safety of life have been codified in both international maritime and aviation law and may be extrapolated to apply to space-based PNT. The Safety of Life at Sea Treaty (SOLAS) has a set of associated standards that require on-board electronic navigation systems. While the United States GPS is not the mandated system, it is used overwhelmingly, although the Chinese Beidou system has recently joined the list of systems that meet the standards.[50] Both the 1958 Convention of the High Seas and the UNCLOS codify an obligation to render assistance to those in danger of being lost at sea. According to the Chicago Convention, "every State must refrain from resorting to the use of weapons against civil aircraft in flight and that, in case of interception, the lives of persons on board and the safety of aircraft must not be endangered."[51]

Aviation and maritime laws and the Laws of Armed Conflict (LOAC) provide a useful basis for determining the legitimacy and desirability of targeting the space portion of space-based PNT capabilities. Although the Chicago Convention requires states to refrain from use of weapons against civilian aircraft, it goes on to say the Convention "shall not be interpreted as modifying in any way the rights and obligations of States set

forth in the Charter of the United Nations."[52] States may take actions consistent with the UN Charter self-defense provisions. However, there is a precedent for limiting or constraining targets during times of conflict. In space, it is an established norm that National Technical Means (NTM) are not to be interfered with since such interference is likely to quickly escalate a crisis between states with significant destructive capabilities. This prohibition on interfering with NTMs was contained in every major arms control agreement between the United States and Soviet Union. Additionally, the Agreement to Reduce the Risk of Outbreak of Nuclear War required the United States and Soviet Union to notify each other in the event of signs of interference with the NTMs.[53] But no established norm exists regarding interfering with non-NTM satellites. Since many states use space capabilities in military and national security activities, they are understandably reluctant to establish a norm that impinges on their ability to neutralize any advantage an adversary gains from using satellites. Moreover, no major space actor will accept constraints on its actions unless it can independently verify compliance with the norm either by use of its own NTMs or other forms of intelligence, surveillance, or reconnaissance under its control or that of trusted partners.[54] However, establishing a noninterference norm could neutralize any relative advantage an adversary could gain by interfering with space-based PNT preemptively to a conflict or during a conflict.

JP 3-14's section on Navigation Warfare (NAVWAR) specifically states the United States will conduct both defensive and offensive actions to assure friendly use of PNT information and deny adversary use of PNT information.[55] It is important to note GPS does more than simply enable land, maritime, and air location and navigation and precision weapons delivery. It also provides exact positioning to other satellites, precise timing to communications satellites, precise timing for cyberspace operations, and positioning information to launch vehicles.[56] Clearly, the United States considers retention of space-based PNT critical. Additionally, space-based PNT also enables more precise attacks, which reduces collateral damage and increases the ability to comply with LOAC.

The Law of Armed Conflict and Space-Based PNT

Under the LOAC proportionality principle, military action must not cause collateral damage that is excessive in light of the expected military advantage. The relative advantages provided by space-based PNT

for military activities have decreased since the 1990s when the United States and Soviet Union had the only space-based PNT systems. China, Europe, and India have now developed their own space-based PNT systems. Japan has developed a space-based PNT augmentation system and just recently changed its laws to allow the use of space for security purposes. States have realized their reliance on space-based PNT has become a great vulnerability and are pursuing non-space-based alternatives.[57] Additionally, relatively little benefit would be gained by interfering with space-based PNT since many space powers have the ability to use more than a single space-based PNT system or are pursuing non-space-based PNT options, thus minimizing any strategic or tactical military advantage. Receivers that use multiple space-based PNT constellations are being developed, eliminating the benefit gained from targeting an adversary's satellites.[58] US national space policy also specifically recognizes foreign PNT services may be used to augment and strengthen the resiliency of GPS.[59] Furthermore, the above states' space-based PNT systems are dual use, which creates a very high level of entanglement with nonmilitary activities and users. The United States recognizes in its own national space policy that space-based PNT is inherently dual use and accordingly will provide continuous worldwide access to its GPS for "peaceful civil uses."[60] With such an entangled situation it is clearly not in the interests of any entity to lose access to space-based PNT.

Since most, if not all, satellites can be used for a military purpose and can also be used by nonmilitary users, a satellite could become a legitimate military objective and subject to attack by an adversary, depending on its use. Because space-based PNT capabilities could be denied to an adversary via narrowly scoped, temporary, and reversible means, space-based PNT would at first glance seem to be a legitimate target under the LOAC principle of proportionality. However, the number of providers that can provide PNT information for users is extremely limited and the impact on some of those users could be literally life-threatening. This could make targeting PNT systems highly unpalatable and might arguably make targeting more difficult under the proportionality provisions of LOAC. Targeting the satellite or control segment of a space-based PNT system could create global impacts to literally billions of users and could be considered to be not proportionate.

Retaining Use of Space-Based PNT

The desire to retain use of space-based PNT by giving up the right to interfere with the satellite and control segments of space-based PNT systems must be balanced with the desire to prevent adversary use of space-based PNT by retaining the right to interfere. Arguably, that balance would seem to weigh in favor of retaining the capability for the United States and other states and international civil and commercial entities. Although militaries have developed tactics, techniques, and procedures for dealing with jamming end user receivers, nonmilitary users have done little if anything. For example, on 31 March 2016, North Korea used radio waves to jam GPS receivers in South Korea. Over 50 airliners and hundreds of South Korean fishing boats were affected, but the US-South Korean military exercises under way were not affected.[61] The 2 April 2014 failure of all 24 of the Russian GLONASS satellites was felt throughout the world, as GLONASS was unavailable for "tractor automation for farming, machine control and robotics in mining and heavy industry, and in the national infrastructure used by surveyors and industry across many countries."[62] Codifying a norm that prohibits interfering with the satellite and control segments of space-based PNT, while preserving the option of disrupting end user equipment, could protect the interests of the United States and others better than denying the use of space-based PNT to an adversary. Such a norm would preserve the use of the space-based PNT capability by all and allow them to meet their security, economic, and societal needs. Ships and aircraft could continue to safely navigate. Search and rescue operations could be swiftly and accurately carried out. Satellite communications and cyberspace activities would continue. Spacecraft and launch vehicles would be able to more safely operate. Finally, military operations could be enabled in such a way as to better meet LOAC obligations. This noninterference norm would protect US interests by ensuring the space-based PNT information it relies on would be preserved.

Given states' general reluctance to give up any strategic advantage, it seems unlikely any would be amenable to a prohibition on interfering with the end receiver segment of space-based PNT as a means of pursuing their security interests. However, this article suggests a constraint on interfering with the satellite and control segments of space-based PNT systems. Moreover, precedence has been set to constrain activities that could be legitimately conducted under LOAC. Protocol IV to the

Convention on the Prohibition or Restrictions of the Use of Certain Conventional Weapons prohibits use of specific weapons (blinding lasers) as a matter of policy. Nations participating in the negotiation of the Convention did not conclude that blinding or a blinding laser weapon caused unnecessary suffering but decided for policy reasons to prohibit their use.[63] Similarly, as a matter of policy, targeting the satellite and control segments of space-based PNT systems during peacetime, crisis, or conflict could be prohibited out of concern for the global consequences gained for a limited, decreasing military advantage.

TCBMs for the Norm

To effectively establish this proposed noninterference norm, appropriate TCBMs need to be created to ensure a common interpretation of the prohibition of targeting the satellite or control segments of space-based PNT, to establish a recognized framework in which players must act regarding space-based PNT, and to provide a means by which "bad actors" may be identified and, if necessary, sanctioned. Successful transparency measures provide ways for parties to practice communication and reduce misperceptions, misunderstanding, and mistrust. Successful measures would decrease the likelihood of escalation of a crisis in space or the expansion of a space conflict to a terrestrial conflict.

Established space powers are understandably reluctant to agree to anything that limits their ability to access and use space in pursuit of their security or economic interests. They are also unlikely to agree to anything that even appears to have the capability to force them to conduct, or refrain from, particular activities. However, emerging and aspiring space powers seem more willing to seek agreements to regulate behavior in space to preserve access to space and protect the domain for equitable use by all. The common objective among all players is to assure access to space and use space in pursuit of their interests. Attempts by the Committee on Peaceful Uses of Outer Space and the UN Conference on Disarmament to address issues such as the use of antisatellite weapons and a potential arms race in space have been largely unsuccessful since they focus on reducing capabilities rather than focusing on the legitimacy of potential targets of those capabilities.

As the United States and others develop counter-space capabilities, they seem to be making threats of retaliation for undesired actions in space more explicit.[64] It is therefore critical that de-escalatory TCBMs

associated with a noninterference norm support a set of coherent deterrence options. TCBMs must address the requirements of each party and must be something each party agrees to follow. A norm prohibiting targeting of the satellite or control segments of space-based PNT is relatively straightforward. However, effective associated TCBMs may be much more difficult to develop.

Transparency measures are necessary to provide states sufficient information to more accurately assess another state's intent. Arguably, transparency measures would only be between states since only states have the capability to interfere with the satellite or control segments of space-based PNT. However, transparency measures could also include non-state actors in a manner similar to the US Space Situational Awareness (SSA) information-sharing agreements. Confidence-building measures should facilitate small, incremental actions that build trust on each side and reassure the other state that actions taken by the first state are not a prelude to an armed attack. However, that level of transparency could cause anxiety on the part of states concerned that the information gained via TCBMs could be used preemptively against them. TCBMs also provide a known framework of acceptable behavior. It becomes easier to identify bad actors as they refuse to adhere to accepted norms and follow accepted TCBMs. Those bad actors may then be more closely watched by the international community, which may exert pressure on them to comply with the norms and TCBMs. Failure to adhere to widely adopted norms and TCBMs could also subject a bad actor to isolation from the rest of the community. For instance, a bad actor might not receive the technical assistance or the resources it needs to conduct its space program. Importantly, the technical assistance in question might not be in the same area as the violated norm. In the case of interference with PNT, it might be possible to renegotiate the SSA data-sharing agreements, spacecraft launch agreements, personnel exchanges, or other partnership agreements as a part of the cost-benefit calculations to deter that bad actor.

Models for TCBMs

It seems best to model new space norms and associated TCBMs on bilateral, rather than multilateral, agreements. Bilateral agreements are easier to negotiate as they focus on the concerns of only two parties. Previous experience during the Cold War recognized the importance

TCBMs played in avoiding escalation into full nuclear war—and those TCBMs were bilateral and narrowly focused. For example, the 1971 US/USSR Agreement to Reduce the Risk or Outbreak of Nuclear War required the United States and Soviet Union to notify each other in the event of an accidental or unauthorized incident that might lead to a nuclear war.[65] An agreement regarding noninterference with the satellite and control segments of space-based PNT could be similarly based on parties informing each other of accidental or unauthorized events that could escalate into conflict. Specifics might include activities that interfere with any of the frequencies used by any of the five space-based PNT providers. Or they might include instances in which a party's space-based PNT system would be unavailable in such ways as to appear as if a state was protecting its system in preparation for other aggressive actions.

In another example, the Agreement Between the United States and Soviet Union to Prevent Incidents on the High Seas was a confidence-building measure intended (and apparently successfully implemented) to prevent actions that could increase tension and the possibility of conflict. It is important to note neither of these two agreements directly affected size, weaponry, or force structure of the two parties.[66] That made both parties more willing to sign the agreements. Similarly, focusing on actual *occurrence* of interference with PNT, versus the *capabilities* to interfere with space-based PNT, would be more palatable to those involved since capabilities would not be impacted. Elements of this type of an agreement could include things such as geographic limitations beyond which localized jamming of user segments is no longer considered local and could be considered a "bad action."

Three additional TCBMs might help create a common interpretation and accepted set of behaviors regarding a noninterference norm. First, states could negotiate an agreement defining nomenclatures. Even if unsuccessful, the communications among those involved in the attempt would be extremely valuable as a way to define expectations. A definition of terms also could lead to better transparency as parties find a common understanding on how a potential adversary might act in a given situation. Any agreements reached also could be provided to broader international organizations as evidence of acceptance of the interpretation of the norm. For example, the ICG holds regional workshops on applications of space-based PNT and provides a publication on current and planned global and regional space-based PNT systems and programs.[67]

In addition to providing information for dissemination as evidence of a norm, negotiations could build on information already discussed in organizations such as the ICGs in order to develop the norm.

Second, each state should develop declaratory policy that it will not interfere with the satellite or control segments of space-based PNT in peacetime, crisis, or conflict. That declaratory policy should actively identify expectations of behavior—particularly, currently unstated expectations. This proposed TCBM is already partially implemented. According to the US National Space Policy, the United States will provide continuous worldwide access to its GPS for peaceful civil uses, and it will provide that access without degrading the signals.[68] Note that the policy states the access is for peaceful civil uses and, furthermore, does not indicate the United States would not interfere with end user receivers as is consistent with the inherent right of self-defense. The US National Space Policy also specifically states foreign PNT services may be used to augment and strengthen the resiliency of GPS.[69] Both of these statements indicate recognition of the importance of space-based PNT and at least a small move toward codifying an expectation the satellite and control segments will not be interfered with. In addition to the official national space policies, speeches, interviews, social media, and testimonies of different organizations are also studied by non-US entities for policy statements and should also be considered. An official declaratory policy loses credibility if governmental organizations are making statements counter to it. A comprehensive strategic communication plan that effectively communicates a declaratory policy against interfering with the satellite and control segments of space-based PNT could decrease uncertainty by sending a consistent message. At the very least, a cohesive strategic communication plan would lessen chances of inconsistent messaging as all players should at least consider how their message could conflict with another agency's message. Inconsistent and confusing messages create potentially dangerous mistrust and uncertainty that could lead to escalation of a conflict in space or expansion of a conflict in space to a terrestrial conflict.

Third, states should develop and implement information-sharing agreements that actively define how the noninterference norm is to be interpreted and the framework for acceptable behaviors. Two different types of agreements could be useful in developing such information-sharing agreements. In the commercial sector, the Space Data Association

(SDA) created agreements in which satellite companies share information to supplement data previously provided by states. It provides a legal and technical framework that states could leverage when developing information-sharing agreements.[70] States could also leverage the SDA itself to conduct what has been called "open" verification that leverages the increasing transparency of space to private observers.[71] In the governmental sector, the notification agreements between the United States and Soviet Union during the Cold War could also serve as a model. Under those agreements, parties explicitly required notification in the event of accidental or unauthorized activities. Similarly, information-sharing agreements associated with a noninterference norm could require parties to notify each other of accidental or unauthorized activities that pose a danger of interference with the satellite or control segments space-based PNT. Depending on the agreement, the notification could be via either formal or informal channels. In general, information-sharing agreements for a noninterference norm should probably be bilateral. Bilateral agreements allow the parties to tailor measures that address each party's concerns. Moreover, bilateral agreements preclude states outside the agreement from negatively influencing the effectiveness of the agreed-upon measures. Although space powers with counter-space capabilities may consider the desires of new or aspiring space powers, bilateral agreements would prevent those entities from having undue influence and could prevent delay in developing and implementing the agreements.

Although it seems to be an appropriate time to develop a noninterference norm with associated TCBMs, monitoring to ensure compliance with the norm is complicated by the fact that current space situational awareness capabilities are not at a level where they may be relied on as a sole source of verification. However, established, new, and aspiring space powers and international commercial entities have entered into space situational awareness information-sharing agreements. These agreements, used primarily to predict potential collisions between space objects, could be leveraged to create more able monitoring capabilities.

Successful transparency measures could lead to successful confidence-building measures as states are able to assure themselves the other states are acting in accordance with agreed-upon TCBMs. That, in turn, helps develop trust or decrease distrust. However, successful confidence-building measures are incremental, iterative actions. Ideally, confidence-building measures will help a state more correctly assess the intentions

of other states as their confidence in each other builds. Each state must believe the other intends to abide by the proposed measure. Declarations by a state that it intends to follow the confidence-building measure may not be believed unless it takes concrete actions to implement the measure. Although United States space policy clearly indicates the importance of GPS, additional steps are necessary to develop an effective TCBM. Fortunately, those steps may have already begun as states with space-based PNT capabilities are beginning to work together to create technical commonalities between the space-based portions of the PNT systems as well as the end user equipment. However, the success of confidence-building measures can only be determined over time.

The Noninterference Norm's Contribution to Deterrence

Successful TCBMs associated with a noninterference norm could contribute to a cohesive set of deterrence options. There are two types of deterrence that should be considered. First, there is "general deterrence," which is based on power relationships and attempts to prevent an adversary from seriously considering *any kind* of military challenge because of expected adverse consequences.[72] General deterrence in the space domain attempts to prevent *any type* of interference by *any actor* against *any type* of space systems. General deterrence is insufficient for the current strategic environment due to the large number of both state and non-state players present in space, the difficulty in attributing interference to a particular actor, and its reliance on adverse consequences. It is essential to note that deterrence has been developed as a way to prevent undesired action between states, not individual citizens or corporations within the state.

In contrast to general deterrence, there is "immediate deterrence," which is specific. Immediate deterrence attempts to forestall an anticipated challenge to a *well-defined* and publicized commitment.[73] It is practiced when general deterrence is thought to be failing.[74] Immediate deterrence would seem to have a higher likelihood of success than general deterrence in the space domain as it is more narrowly focused on particular actors and their actions. Deterring any entity that has any kind of offensive counter-space capability from conducting any kind of interference against any kind of satellite is daunting at best. Additionally, attribution of interference to a particular party can be problematic. On the other hand, deterring interference with the satellite and control segments of space-based PNT ca-

pabilities specifically might be accomplished via immediate deterrence. Although immediate deterrence can be considered less complex since it focuses on a single target, it could also be more complex as deterrence actions must be tailored for specific rather than broad actions and must be tailored for each adversary to be deterred. Additionally, a state must consider not only what an opposing state believes but must consider allies and partners in its calculations, too.[75] Any coherent set of immediate deterrence actions designed to prevent interference with the satellite and control segments of space-based PNT would certainly have to address these factors. Calculations could be further complicated by the presence of non-state international and commercial entities.

Whether considering general deterrence or immediate deterrence, opportunities abound for complications and misunderstandings. Space-based PNT capabilities are dual use and are essential to both military and nonmilitary activities. From a military point of view, it is critical for deterrence measures to succeed because the military relies so heavily on space-based PNT to conduct military operations. From a nonmilitary point of view, it is critical for deterrence measures to succeed since non-space powers and international and commercial entities rely heavily on space-based PNT as they pursue their own economic, security, and development interests. As defined in this article, intentional interference with space-based PNT is escalatory. It represents vertical escalation since it expands terrestrial conflict into another domain, and, if not limited in ways suggested by the proposed norm, attacking the space or control segment represents horizontal escalation affecting many other users not party to the conflict, in contravention of other established principles such as LOAC. It is therefore extremely important to explicitly codify the non-interference norm and the associated TCBMs necessary to deter actions that could escalate conflict in space or expand a conflict in space to a terrestrial conflict. Additionally, a codified norm prohibiting interference with the satellite and control segments of space-based PNT capabilities and effective associated TCBMs is a means by which the United States might preserve its access to the capability during all phases of a conflict.

A codified norm prohibiting intentional interference with satellite and control segments of space-based PNT could inhibit escalation, since there would be no option to interfere with the capability in order to gain the upper hand in a military action. Clearly delineated TCBMs such as well-defined nomenclature could lead to a decrease in misun-

derstandings regarding the interpretation of the noninterference norm. Declaratory policies and information-sharing agreements could reduce misunderstandings and mistrust between the states, which could lead to greater stability as states feel less of a need to preemptively interfere with a space-based PNT system.

Conclusion

It has been six decades since the first satellites were launched and the foundational norms concerning peaceful purposes of space were codified. Yet, there is no agreed-upon definition of peaceful purposes or the threshold for an armed attack, so uncertainty lingers regarding how interference with space capabilities should be addressed. Such uncertainty is destabilizing, and any interference with a space capability has the possibility of escalating a conflict in space or expanding a space conflict into a terrestrial conflict. A wide variety of entities ranging from states to non-state international organizations and commercial organizations use space-based PNT capabilities. Usages may support military operations, economic interests, societal development, or safety of life and navigation activities. The potential impact to the world if intentional interference with satellite or control segments caused worldwide loss of PNT information would be devastating. An expectation that space-based PNT is available and will continue to be available has recently emerged. A general understanding is emerging that the capability will always be available and that interference with the capability is not acceptable.

Those expectations, and the current restraint from interfering with the space and control segments of space-based PNT systems, are proceeding toward a norm that actively prohibits interference. However, that norm and associated TCBMs must be codified in order to create a common interpretation of the norm and define an acceptable framework of behaviors. The language of the norm should explicitly recognize that space-based PNT is an important contributor to the preservation of peace and progress for all peoples of the world. It should also promote cooperation among space-based PNT providers and users. Finally, it should explicitly state that it is desirable to prevent conflict in outer space that could escalate or expand into a terrestrial conflict.

There are at least three potential TCBMs to associate with the noninterference norm. First, a common set of nomenclatures should be created. The negotiation process itself would help define a common interpreta-

tion of, and expectations regarding, the norm. It might also help provide insight on how a potential adversary might respond to a given situation. Second, states should declare that they will not interfere with the satellite and control segments of space-based PNT capabilities. The United States has already implemented this TCBM to some degree through its national space policy, which states it will provide GPS for peaceful civil purposes. Third, states should develop and implement information-sharing agreements whereby they inform each other in the event of accidental or unauthorized activities that could lead to interference with the satellite and control segments of space-based PNT capabilities.

A codified norm prohibiting intentional interference with the satellite and control segments of space-based PNT could inhibit escalation. Clearly delineated TCBMs, such as a well-defined nomenclature, could lead to a decrease in misunderstandings regarding the interpretation of the noninterference norm. Declaratory policies and information-sharing agreements could reduce misunderstandings and mistrust between the states, which could lead to greater stability as states feel less of a need to preemptively interfere with a space-based PNT system. As a matter of security and as a matter of policy, targeting the satellite and control segments of space-based PNT systems during peacetime, crisis, or conflict could be prohibited out of concern for the global consequences gained for a limited, decreasing military advantage. SSQ

Appendix. States and organizations with a presence in space

Country/ Consortium	*Capabilities*	*Users Government/Military/Civil/ Commercial*
Algeria	Earth observation	Government
Argentina	Communications Technology development	Commercial Civil/Commercial
Australia	Communications	Military/Commercial
Austria	Space science Technology development	Civil Civil
Azerbaijan	Communications	Government
Belarus	Earth observation	Government
Belgium	Earth observation Space science	Government/Military/Commercial Civil
Bolivia	Communications	Government

Country/ Consortium	*Capabilities*	*Users Government/Military/Civil/ Commercial*
Brazil	Communications Earth observation Technology development	Commercial Government Civil
Canada	Communications Space science Space observation Technology development	Commercial Government/Civil Government/Military/Commercial Civil
Chile	Earth observation	Government/Military
China	Communications Earth observation PNT Space science Technology development	Government/Civil/Military/Commercial Government/Military/Commercial Military Government/Civil Government/Military/Civil/Commercial
Denmark	Communications Earth observation Technology development	Civil Government Commercial
Egypt	Communications	Government
France	Communications Earth observation Space science Technology development	Military/Commercial Government/Military/Commercial Government Military
Germany	Communications Earth observation Space science Technology development	Government/Military/Civil Government/Military/Civil/Commercial Government/Civil Government/Civil/Commercial
Greece	Communications Earth observation	Commercial Military
India	Communications Earth observation PNT Space science Technology development	Government/Military/Commercial Government/Military/Civil Government Government Government/Civil
Indonesia	Communications Earth observation Technology development	Commercial Government Government
Iran	Communications	Government/Military/Civil/Commercial
Iraq	Earth observation	Civil
Israel	Communications Earth observation	Government/Military/Civil Military/Commercial
Italy	Communications Earth observation Space science	Government/Military/Commercial Government/Military/Civil Government
Japan	Communications Earth observation PNT Space science Technology development	Commercial Government/Civil/Commercial Government Government/Civil/Commercial Government/Civil/Commercial
Kazakhstan	Communications Earth observation	Commercial Government
Laos	Communications	Government

Country/ Consortium	*Capabilities*	*Users Government/Military/Civil/ Commercial*
Luxembourg	Communications	Commercial
Malaysia	Communications	Commercial
Mexico	Communications	Government/Military/Commercial
Monaco	Communications	Government/Commercial
Morocco	Technology development	Government
The Netherlands	Communications Technology development	Civil/Commercial Civil
Nigeria	Communications Earth observation Technology development	Commercial Government Government
Norway	Communications	Government/Commercial
Pakistan	Communications	Government/Commercial
Peru	Technology development	Civil
Philippines	Communications	Commercial
Poland	Space science	Government
Russia	Communications Earth observation PNT Space science Technology development	Government/Military/Civil/Commercial Government/Military/Commercial Military/Commercial Government Military/Civil
Saudi Arabia	Communications Earth observation Space science Technology development	Government/Commercial Government Government Commercial
Singapore	Communications Earth observation Technology development	Commercial Government/Civil/Commercial Civil/Commercial
South Africa	Earth observation Technology development	Military Civil
South Korea	Communications Earth observation Technology development	Government/Military/Commercial Government/Commercial Government
Spain	Communications Earth observation Technology development	Government/Military/Commercial Government/Military Government/Civil
Sri Lanka	Communications	Government
Sweden	Communications Earth observation	Commercial Government/Commercial
Switzerland	Technology development	Civil
Taiwan	Communications Earth observation	Commercial Government/Military/Civil
Thailand	Communications Earth observation	Commercial Government
Turkey	Communications Earth observation Technology development	Commercial Government/Military Civil

Country/ Consortium	*Capabilities*	*Users Government/Military/Civil/ Commercial*
Turkmenistan	Communications	Government/Commercial
Ukraine	Technology development	Civil
United Arab Emirates	Communications Earth observation	Military/Commercial Government
United Kingdom	Communications Earth observation Space science Technology development	Government/Military/Commercial Government/Commercial Government Government/Commercial
United States of America	Communications Earth observation PNT Space observation Space science Technology development	Government /Military/Civil/Commercial Government/ Military/Commercial Military/Commercial Military Government/Military/Civil Government/Military/Civil/Commercial
Uruguay	Technology development	Civil
Venezuela	Communications Earth observation	Government Government
Vietnam	Communications Earth observation	Government Government
European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)	Earth observation	Government/Civil
European Space Agency (ESA)	Communications Earth observation PNT Space science Technology development	Government/Commercial Government/Civil Commercial Government Government/Commercial
Regional African Satellite Communications Organization (RASCOM)	Communications	Commercial

Information in this table is derived from the Union of Concerned Scientists Satellite Database, http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.VwK-xbwYNFI.

Notes

1. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (hereafter, Outer Space Treaty), 27 January 1967, 18 UST 2410, TIAS 6347, 6610 UNTS 205, http://disarmament.un.org/treaties/t/outer_space/text; Preamble, Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, 22 April 1968, 19 UST 7570, TIAS 6599, 672 UNTS 119, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introrescueagreement.html; Preamble, Convention on the International Liability of Damage Caused by Space Objects, 29 March 1972, 24 UST 2389, TIAS 7762, 961 UNTS 187, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html; Preamble, Convention on the Registration of Objects Launched into Outer Space, 12 November 1974, 28 UST 695, TIAS 8480,1023 UNTS 15, http://www.unoosa.org/oosa/en/ourwork

/spacelaw/treaties/introregistration-convention.html; and Preamble, Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, 18 ILM1434, 1363 UNTS 3, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/intromoon-agreement.html. Note: Only 11 states have signed the OST. The United States has not signed this this treaty.

2. Outer Space Treaty, Article IX.

3. Lucius Caflisch, *Articles on the Effects of Armed Conflict on Treaties*, United Nations Audiovisual Library of International Law, 2016, 2, http://legal.un.org/avl/pdf/ha/aeact/aeact_e.pdf.

4. "Selective Availability," National Coordination Office for Space-Based Positioning, Navigation, and Timing, accessed 31 March 2016, http://www.gps.gov/systems/gps/modernization/sa/.

5. The Honorable Mary Peters, US secretary of transportation (remarks, 36th ICAO Assembly, Montreal, Canada, 18 September 2007), http://www.gps.gov/systems/gps/modernization/sa/peters/.

6. Presidential Policy Directive 4, "National Space Policy of the United States of America," 28 June 2010, Intersector Guidelines, 5, http://permanent.access.gpo.gov/lps124681/national_space_policy_6-28-10.pdf.

7. "Applications," National Coordination Office for Space-Based Positioning, Navigation, and Timing, accessed 15 January 2016, http://www.gps.gov/applications.

8. *Cosmicheskaya Systyema Poiska Aariyniyich Sudov* loosely translates to "Space System for the Search of Vessels in Distress," http://www.sarsat.noaa.gov/SARSAT%20101%20Brief%20PDF.pdf.

9. NOAA Search and Rescue Satellite Aided Tracking, "Frequently Asked Questions," National Oceanic and Atmospheric Agency, accessed 7 April 2015, http://www.sarsat.noaa.gov/faq%202.html. The governments of Canada, France, Russia, and the United States (the Parties) have signed an agreement to provide for the long-term operation of the system and to support the objectives of the International Maritime Organization (IMO) and the International Civil Aviation Organization (ICAO) concerning search and rescue. In addition to the four Parties and the two Participating Organizations (IMO and ICAO), COSPAS-SARSAT international participation includes 26 ground segment providers and 11 user states. Over 32,000 people have been rescued since the COSPAS-SARSAT creation in 1982. http://www.sarsat.noaa.gov/SARSAT%20101%20Brief%20PDF.pdf.

10. "SAR Statistics," COSPAS-SARSAT International Satellite System for Search and Rescue, accessed 15 March 2016, https://www.cospas-sarsat.int/en/sar-statistics.

11. "Search and Rescue Satellite Aided Tracking (SARSAT)," NOAA, accessed 4 April 2016, http://www.sarsat.noaa.gov/SARSAT%20101%20Brief%20PDF.pdf.

12. Ibid.

13. "Honeywell Tracking Passes Test for Galileo Search and Rescue," *GPS World*, 13 April 2015, http://gpsworld.com/honeywell-tracking-passes-test-for-galileo-search-and-rescue/; "McMurdo Opens Emergency Response Experience Center," *GPS World*, 13 May 2015, http://gpsworld.com/mcmurdo-opens-emergency-response-experience-center/.

14. "Global Maritime Distress and Safety System," *Wikipedia*, accessed 9 August 2016, https://en.wikipedia.org/wiki/Global_Maritime_Distress_and_Safety_System. In 1988, IMO amended the Safety of Life at Sea (SOLAS) Convention, requiring ships subject to it to install Global Maritime Distress and Safety System equipment.

15. NOAA SARSAT, accessed 7 April 2015, http://www.sarsat.noaa.gov/faq%202.html.

16. Joint Publication 3-14, *Space Operations*, 29 May 2013, I-3.

17. Ibid., ix.

18. Ibid., II-6.

19. Ibid.

20. James R. Clapper, director of national intelligence, Statement for the Record before the 113th Congress, "Worldwide Threat Assessment of the US Intelligence Community," Senate, *Select Committee on Intelligence*, 29 January 2014, 7, https://www.dni.gov/index.php/newsroom/testimonies/203-congressional-testimonies-2014/1005-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

21. Mission Statement of the International Committee on Global Navigation Satellite Systems (ICG), accessed 12 December 2015, http://www.unoosa.org/oosa/en/SAP/gnss/icg.html.

22. International Committee on Global Navigation Satellite Systems, accessed 23 April 2015, http://www.unoosa.org/oosa/en/SAP/gnss/icg.html. Members: Ten states plus the European Space Agency. Associate members: Eleven nongovernment organizations.

23. Richard A. Clarke, "Securing Cyberspace Through International Norms, Recommendations for Policymakers and the Private Sector," accessed 23 June 2016, 4, www.goodharbor.net/media/pdfs/SecuringCyberspace_web.pdf; and Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (Autumn 1998): 891, http://www.jstor.org/stable/2601361.

24. Ibid.; Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, 22 April 1968, 19 UST 7570, TIAS 6599; 672 UNTS 119, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introrescueagreement.html; Convention on the International Liability of Damage Caused by Space Objects, 29 March 1972, 24 UST 2389, TIAS 7762, 961 UNTS 187, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html; and Convention on the Registration of Objects Launched into Outer Space, 12 November 1974, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introregistration-convention.html.

25. UN General Assembly, Resolution 1962 (XVIII) "Declaration of Legal Principles Governing the Activities of Space in the Exploration and Use of Outer Space." 13 December 1963, http://www.un-documents.net/a18r1962.htm.

26. Ibid.

27. "Global Maritime Distress," *Wikipedia*, https://en.wikipedia.org/wiki/Global_Maritime_Distress_and_Safety_System.

28. Nick Ward, George Shaw, Paul Williams, and Alan Grant, General Lighthouse Authorities, Research & Radio Navigation Directorate, "The Role of GNSS in E-Navigation and the Need for Resilience," www.gla-rrnav.org/file.html?file=13d83ef7a17a5002eb55389905230b2c.

29. International Civil Aviation Organization, Standards, Recommended Practices and Procedures, Annex 6, Part II, International General Aviation-Aeroplanes, code7700.com/pdfs/icao_annex_6_part_ii.pdf.

30. Finnemore and Sikkink, "International Norm Dynamics," 895.

31. See the Audiovisual Library of International Law at http://legal.un.org/avl/ha/gclos/gclos.html for the history of the Convention and a list of the preparatory documents.

32. The predecessor to the International Civil Aviation Organization (ICAO) was the International Commission for Air Navigation. When it met for the first time in 1903, only eight countries attended; in 1906, 27 states attended.

33. "China's Beidou GPS-substitute opens to public in Asia," BBC, 27 December 2012, http://www.bbc.co.uk/news/technology-20852150.

34. Bree Feng, "A Step Forward for Beidou, China's Satellite Navigation System," Sinosphere, 4 December 2014, http://sinosphere.blogs.nytimes.com/2014/12/04/a-step-forward-for-beidou-chinas-satellite-navigation-system/?_r=0.

35. Briefing, Prof. Dr. Grigory Stupak, GLONASS Status and Development Plans, 5th Meeting of the International Committee on GNSS, Turin, Italy, 2010, http://www.unoosa.org/pdf/icg/2010/ICG5/18october/03.pdf.

36. National Coordination Office, "International Cooperation," accessed 20 January 2016, http://www.gps.gov/policy/cooperation/#content. The United States has agreements with Australia, China, the European Union, India, Japan, Russia, and the United Kingdom.

37. Ibid. The United States works with the following: International Civil Aviation Organization, International Maritime Organization, International Telecommunication Union, UN Committee on the Peaceful Uses of Outer Space, Asia-Pacific Economic Cooperation, North Atlantic Treaty Organization, and the World Trade Organization.

38. "International Committee on Global Navigation Satellite Systems Mission Statement," UN Office for Outer Space Affairs, accessed 23 April 2015, http://www.unoosa.org/oosa/en/SAP/gnss/icg.html.

39. "ICG Members, Associate Members and Observers," www.unoosa.org, accessed 23 April 2015, http://www.unoosa.org/oosa/en/SAP/gnss/icg/members/index.html.

40. ICG Mission Statement, accessed 12 August 2016, http://www.unoosa.org/oosa/en/ourwork/icg/icg.html.

41. "About UN-SPIDER," UN Office of Outer Space Affairs, accessed 25 April 2015, http://www.unoosa.org/oosa/en/unspider/index.html.

42. United Nations General Assembly, *Report on the United Nations/United States of America International Meeting on the Use and Applications of Global Navigation Satellite Systems*, Committee on the Peaceful Uses of Outer Space, Vienna, A/AC.105/846, 13–17 December 2004, http://www.unoosa.org/pdf/reports/ac105/AC105_846E.pdf.

43. United Nations Convention on the Law of the Sea, 10 December 1982, at preamble, http://www.un.org/Depts/los/convention_agreements/texts/unclos/UNCLOS-TOC.htm.

44. Convention on International Civil Aviation, 7 December 1944, 61 Stat. 1180, T.I.A.S. 1591, 15 U.N.T.S. 295, www.icao.int/publications/Pages/doc7300.aspx.

45. United Nations Charter, 26 June 1945. The purpose of the United Nations is "to maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace."

46. Bureau of International Security and Nonproliferation, Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, 18 May 1977, http://www.state.gov/t/isn/4783.htm.

47. Outer Space Treaty, Article IV.

48. Ibid., Article IX.

49. Ibid., Article III.

50. Remarks of Dr. Refaat Rashad of Egypt, Minutes of National Space-Based Positioning, Navigation and Timing Advisory Board, Fourteenth Meeting, 10–11 December 2014, 30, http://www.gps.gov/governance/advisory/meetings/2014-12/minutes.pdf.

51. Chicago Convention, Article 3.

52. Ibid.

53. Samuel Black, *No Harmful Interference with Space Objects: The Key to Confidence Building*, Stimson Center Report, no. 69 (July 2008), 3, https://www.stimson.org/sites/default/files/file-attachments/NHI_Final_1.pdf.

54. Ambassador Roger G. Harrison, "Space and Verification, Volume I: Policy Implications," http://swfound.org/media/37101/space%20and%20verification%20vol%201%20-%20policy%20implications.pdf, 10. Unilateral verification is the first of four layers of verification discussed in the study. The others are cooperative, multilateral, and "open."

55. JP 3-14, II-6.

56. JP 3-14, Appendix E.

57. PNT Advisory Board Minutes. For example, Dr. Robert Lutwak, program manager, Defense Advanced Research Projects Agency, is working to provide GPS equivalent signals in a degraded environment; and Joey Cheng, "When GPS falters, where will the military turn?," Defensesystems.com, 18 February 2014, http://defensesystems.com/articles/2014/02/18/gps-alternatives.aspx.

58. Philip G. Mattos and Fabio Pisoni, "Quad-Constellation Receiver: GPS, GLONASS, Galilea, BeiDou," GPS World, 1 January 2014, http://gpsworld.com/quad-constellation-receiver-gps-glonass-galileo-beidou/; and Mike Gruss, "Pentagon Begins Revising DOD Space Policy," Space News, 14 April 2016, http://spacenews.com/pentagon-begins-revising-national-security-space-policy/.

59. Presidential Policy Directive 4, 5.

60. Ibid.

61. "North Korea Jams GPS, Launches Missile," Voice of America News, 4 April 2016, http://learningenglish.voanews.com/content/north-korea-jams-gps-launches-missile/3265073.html.

62. "GLONASS Failure Confirms Backup Need," Air Traffic Management, 8 April 2014, http://www.airtrafficmanagement.net/2014/04/glonass-failure-confirms-urgent-backup-need/.

63. The Judge Advocate General's School, United States Air Force, *Air Force Operations and the Law* (Maxwell Air Force Base, AL: The Judge Advocate General's School, 2014), 15. Nations participating in negotiation of the Convention on the Prohibition or Restrictions of the Use of Certain Conventional Weapons did not conclude that blinding as such or a blinding laser weapon caused unnecessary suffering but decided for policy reasons to prohibit their use.

64. China conducted an official antisatellite weapon (ASAT) test in 2007 and was assessed to carry out another in May 2013. The United States shot down a failing satellite which was widely seen as an ASAT test. Russia announced the resumption of its ASAT program in 2009. India has announced it plans to develop an ASAT capability.

65. Agreement to Reduce Risk of Outbreak of Nuclear War Between the United States of America and the Union of Soviet Socialists Republics, 30 September 1971, http://avalon.law.yale.edu/20th_century/sov001.asp.

66. US Department of State, Bureau of International Security and Nonproliferation, Narrative, Agreement Between the Government of The United States of America and the Government of The Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas, 25 May 1972, http://www.state.gov/t/isn/4791.htm.

67. UN Office for Outer Space Affairs, "Current and Planned Global and Regional Navigation Satellite Systems and Satellite-based Augmentation Systems," International Committee on Global Navigation Satellite Systems, 2010, http://www.unoosa.org/pdf/publications/icg_ebook.pdf.

68. Presidential Policy Directive 4, 5.

69. Ibid.

70. Jonty Kasku-Jackson, "International Commercial Avenues to Complement Deterrence Actions," *Space and Defense Journal* 7, no. 1 (Winter 2014): 33–34, http://www.usafa.edu/df/dfe/dfer/centers/ecsds/docs/Space_and_Defense_7_1.pdf.

71. Harrison, "Space and Verification, Volume I." This "open" verification is the fourth of four layers of verification discussed in the study. The others are unilateral, cooperative, and multilateral.

72. Richard Ned Lebow, *Deterrence* (New York: Routledge Handbook of Security Studies, 2010), 397. Quoting Patrick M. Morgan's "Deterrence: A Conceptual Analysis," (Beverly Hills, CA: Sage Publications, 1983).

73. Avery Goldstein, *Deterrence and Security in the 21st Century; China, Britain, France, and the Enduring Legacy of the Nuclear Revolution* (Stanford, CA: Stanford University Press, 2000), 22–24.

74. Ibid.

75. Ibid.

Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot

Mark Raymond

Abstract

The cyber-regime complex is governed by a sprawling array of rules, implemented in a decentralized manner by a large number of public and private actors. Since there is no guarantee that the future evolution of the cyber-regime complex will occur in a manner conducive to Internet stability and global interoperability, the "responsibility to troubleshoot" (R2T) is an important hedge against the significant costs associated with cyber disruption.

Even if a global prohibition regime were adopted, there would be good reasons to ensure the existence of a robust set of institutionalized mechanisms for mitigating and remediating various kinds of intended and unintended disruptions to Internet stability and interoperability. While prohibition may be worth pursuing, it is clearly insufficient. At least for the foreseeable future, previously agreed-upon mitigation and management processes will also be required.

* * * * *

The cyber domain is widely acknowledged to be in the midst of a process of global rulemaking that includes an array of public and private actors from across the globe.[1] Many of these rules pertain, more or less directly, to issues of international security. Indeed, the question of cyber norms has been on the agenda of the First Committee of the United Nations General Assembly since 1998. Their work has made significant progress in the two most recent reports of its Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.[2] The work of the GGE is vitally important; however, this state-centric process cannot be treated in isolation from the broader landscape of

---

Mark Raymond is the Wick Cary Assistant Professor of International Security at the University of Oklahoma and a Fellow at the Center for Democracy and Technology. He holds a PhD in political science from the University of Toronto.

Internet governance and Internet policy—even though it concerns matters traditionally understood as the exclusive purview of states. Security and intelligence practitioners increasingly affect, and are affected by, decisions made about Internet governance and Internet policy in a variety of contexts at the global, regional, and even domestic levels. Many of these decision-making processes occur at least partially within the private rather than the public sphere.[3] Collectively, these processes of rulemaking entail the emergence of a broader cyber-regime complex alongside the narrow technical regime for Internet governance in an era characterized by the impending integration of the Internet and cyberspace with virtually every domain of human activity.[4] This process of regime complex formation is ongoing and remains contentious. Contention over Internet issues and the creation of this emerging cyber-regime complex is driven by a variety of factors, including the breadth of issues implicated (trade, security, human rights, etc.) and the diversity of participants in terms of actor type, interests, values, and views of legitimate procedures for rulemaking.[5]

Even the most optimistic projection for the nascent cyber-regime complex must acknowledge that, for the foreseeable future, most governance will remain decentralized. Decisions about policy, rules, and norms will be made by an extremely heterogeneous set of players that will often operate with a high degree of autonomy. Even where there are clear hierarchical authority relations between participants, the sheer complexity and pace of governance in this area will create autonomy in practice. Yet the shared global physical and logical resources crucial to the cyber domain mean that decisions made by these various parties may have implications for, and intended or unintended effects on, those outside their own jurisdictions. As a result, decisions made in one part of the cyber-regime complex can negatively impact the stability and interoperability of the network for others. The combination of the possibility of such effects and a highly decentralized regime complex exacerbates challenges of coordination and conflict resolution among an extremely diverse set of actors.

Since the various participants in the emerging global cyber-regime complex have distinct and at least partially incommensurate values and interests, policy coordination efforts are likely to remain limited. They will also be inhibited by the complexity of the subject matter. In such situations, one possible approach is to establish a shared commitment to

"do no harm" or to refrain from taking steps that could negatively affect the stability or global interoperability of the cyber domain and the ability of the players to make use of it. Such an approach motivates recent calls for a norm of noninterference in what has been called the "public core" of the Internet.[6] Elimination of such cyber behavior is unlikely, in part because actors cannot agree completely (or even substantially) on the bounds of acceptable behavior. Accordingly, simple rules and norms of prohibition are unlikely to be sufficient for ensuring the viability of the cyber-regime complex. Further, a simple prohibition regime would likely be insufficient even in a world of angels. The reality of a massively complex, open global system built on the principle of "permissionless" innovation, combined with the law of unintended consequences, suggests the desirability of having previously agreed-upon means of responding when the activities of one group have negative implications (intended or not) for others.

This article argues that the capacity to effectively manage the set of challenges can be enhanced by cultivating a responsibility to troubleshoot (R2T).[7] First it argues that the decentralized nature of the global cyber-regime complex combines with the shared logical resources and physical infrastructure of the Internet to produce both strategic opportunities and externalities that affect other parties. One solution to these problems would be to establish a prohibition regime. Next it surveys other prohibition regimes employed to address international security threats. In doing so, it gives context to the common wisdom that prohibition is virtually impossible in the cyber domain and shows that elements of a proto-prohibition regime for the cyber domain are identifiable.[8] However, while prohibition may be worth pursuing, it is clearly insufficient. At least for the foreseeable future, mitigation and management processes will also be required. Accordingly, the third section explores options for an R2T as a core component of the global cyber-regime complex.

Decentralized Governance of a Global System

While cyberspace is often understood as a global commons or even a pure public good, it is more accurately described as a set of nested "club" goods, since it is excludable and typically non-rivalrous in consumption[9] and since decisions about cyberspace are taken in a myriad of separate institutional contexts arrayed in complex and variable authority relations.[10] At the most basic level, all Internet users are members of a single

club: the club of global Internet users. Simultaneously, all users are also members of at least two other kinds of clubs—a club of Internet users in a particular state and a club of Internet users relying on a particular Internet service provider (ISP). Each of these clubs has different procedural rules for rulemaking and interpretation. National clubs of Internet users typically work according to the corresponding state's processes for legislation, regulation, and jurisprudence, though some states also have multi-stakeholder bodies governing some aspects of Internet policy. Clubs of users relying on a particular ISP are more commonly governed by contractual arrangements and terms of service, with civil law as a backdrop. Other notable clubs include those with special responsibility for core Internet technical functions, such as the Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Engineering Task Force (IETF).

As the Internet has become enmeshed with more and more aspects of economic, social, and political life, the narrow legacy Internet governance regime concerned with core technical functions such as the development of technical protocols and the management of Internet names and numbers has been drawn into a nascent global cyber-regime complex.[11] The result is that organizations with primary interests and responsibilities removed from the Internet and cyberspace are beginning to make decisions and to enact rules that can have significant unintended consequences for the stability and interoperability of the cyber domain. These actors include military and security agencies, antitrust regulators and consumer watchdogs, human-rights bodies, international-trade bodies, and others.

These various entities and organizations nevertheless share the same physical infrastructure as well as globally harmonized standards and protocols for exchanging packets between the various independent networks that comprise the Internet and for resolving Internet domain names into Internet protocol (IP) address numbers. The combination of the end-to-end principle and the principle of permissionless innovation has been central to the rapid global spread of Internet access and to its economic potential; however, these principles have also enabled the actions and decisions of individual organizations to have far-ranging effects on the stability and interoperability of the broader global network.

Such effects are often unintended consequences of attempts to exercise control over Internet content in the service of various social, economic,

and political policy objectives. Examples include a global YouTube outage caused by Pakistani attempts to block domestic access to video content deemed inappropriate on religious grounds, domain name seizures by American law enforcement agencies intended to enforce intellectual-property laws, and ongoing European efforts to implement a "right to be forgotten" with respect to online search engines. These examples, and others, are indicative of what has been called "the turn to infrastructure in Internet governance."[12]

Cyber attacks, financially motivated cybercrime, and cyber espionage, whether conducted by states or firms, employ Internet infrastructure and mechanisms of technical Internet governance to accomplish unrelated objectives. Like content filtering and blocking measures, these activities can have negative unintended consequences for global Internet stability and interoperability. Some effects may be quite direct in nature. Manipulating the underlying technology and protocols may simply be done badly and cause technical problems. Given the low and rapidly falling barriers to entry in this field, significant cyber capabilities are likely to be acquired by a large number of public and private organizations with relatively low levels of expertise and sophistication; such novices may be particularly prone to execution errors. Other negative unintended effects on Internet stability and interoperability will be indirect in nature. The most likely pathways for ill effects include: (1) attempts to "harden" networks to make them less susceptible to intrusion but sacrifice openness as a result, leading the network topology to more closely resemble a "cybered Westphalia"[13]; and (2) escalating spirals of retaliation that cause episodic service interruptions and other collateral damage to third parties.

All of these diverse activities are enacted for reasons. Whether we evaluate these as good or bad reasons is beside the point of the argument being advanced here. The key point is that a large number of actors will be capable of forming their own views about the desirability of such forms of cyber conduct and also of *acting* on the basis of such views. It is this potential for autonomous action—which itself may have *further* unintended consequences—that makes these problems especially serious.

One approach to managing problems associated with unintended consequences in a decentralized governance environment would be to pursue prohibition of various forms of problematic cyber conduct. Grounds for such a ban might be rooted entirely in considerations of

long-term consequences for Internet stability and interoperability, or they might also draw on complementary justifications having to do with respect for state sovereignty or individual human rights. Several bans on particular kinds of international conduct exist, and some have persisted for extended periods of time. What follows is a survey of several existing global prohibition regimes and the prospects for applying such an approach to cybersecurity governance.

Prohibition Regimes and International Security Governance

The common view of international politics—as a lawless Wild West in which sovereign states confront an anarchic system that compels them to act ruthlessly or perish—is mistaken. Political scientist Tanisha M. Fazal, whose research focuses on the relationship between sovereignty and international law, has convincingly shown that—at least since 1945—the rate of "state death" has fallen sharply in response largely to changing norms of conquest.[14] While international norms, like all social rules, may sometimes be violated, the norm against acquiring territory by conquest appears to exert a significant constraining effect on state behavior to the point where many states in the international system, including several permanent Security Council members, appear to have ruled it out entirely as a policy option. International condemnation of Russia's actions in Crimea demonstrates the continuing strength of the norm even as it requires acknowledgment that enforcement is imperfect.

Predation is hardly the only international conduct subject to prohibition. The extensive international relations literature documenting such regimes catalogs numerous cases of varying success.[15] Here the focus is on cases prohibiting conduct directly relevant to international security, to make three important points: (1) prohibition regimes are useful tools for achieving security policy objectives, (2) there are initial signs of a developing prohibition regime that captures multiple kinds of cyber conduct, and (3) even in a perfect world, such a prohibition regime is insufficient to address the problems associated with decentralized governance of a shared global facility.

One prominent global prohibition regime bans gross violations of fundamental human rights. An example is the ban on genocide codified in the Convention on the Prevention and Punishment of the Crime of Genocide (1948)—a prohibition that is also a *jus cogens* norm of inter-

national law under Article 53 of the Vienna Convention on the Law of Treaties.[16] Similarly, the prohibition against torture is also such a norm of international law in addition to a treaty obligation under the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984). In both cases, bans on particular forms of international conduct are framed in terms of these norms, which are binding on states regardless of their consent and which do not permit derogation. This latter quality of *jus cogens* norms substantially limits the varieties of special pleading open to states under the area of customary international law known as the law of state responsibility.[17]

Another class of internationally prohibited behaviors pertains to battlefield conduct. Wayne Sandholtz, a professor of international relations and law, has shown, for example, that wartime plunder has moved from a normal and expected part of war to prohibited behavior.[18] Similarly, political scientist Ward Thomas has argued that there is a relatively robust international norm against assassination.[19] There is also a ban on particular kinds of weapons. For example, biological and chemical weapons are subject to bans. The Biological Weapons Convention (1972) prohibits not only the use but also the production of this class of weapons,[20] though it lacks provisions for monitoring or inspection. In contrast, the Chemical Weapons Convention provides for extensive inspections in support of the associated taboo.[21] Bans have also been created for certain classes of conventional weapons. Examples include the ban on antipersonnel landmines[22] as well as the ban on cluster munitions.[23] In contrast, attempts to impose control on the international transfer of small arms and light weapons have been less successful.[24]

Prohibition in the Cyber Domain

There are also signs of a developing global prohibition regime in the cyber domain. This proto-regime has at least three notable components. The first deals with promoting international cooperation on cybercrime. The Budapest Convention on Cybercrime commits state parties to harmonizing their domestic legal regimes with respect to computer crime. It also commits parties to good-faith cooperation in investigating and prosecuting such crimes across borders.[25] As such, it effectively seeks to deal with the problem of decentralized governance by negotiating common standards at the global level and leaving implementation to

domestic authorities. While a useful step, it has been ratified by only 47 nations, primarily advanced industrial democracies.

The second component of the emerging cyber prohibition regime consists of work primarily by the United Nations GGE seeking to clarify the applicability of the law of armed conflict in the cyber domain. The group includes the governments of the United States, China, and Russia; it therefore reflects the preferences and understandings of key states. The 2015 report made several key advances. It expressed the belief that "voluntary, non-binding norms of responsible State behavior can reduce risks to international peace, security and stability." It further made several concrete recommendations for such norms. Finally, in a discussion of the application of international law to information and communications technologies (ICT), the GGE explicitly noted "established legal principles . . . including, where applicable, the principles of humanity, necessity, proportionality and distinction."[26] American officials have indicated, though, that some states are thus far unwilling to make "more robust statements on how international law applies" in the cyber domain.[27] These efforts are preliminary, at best, and a great deal will depend on how these norms are implemented in concrete cases.

The final component of this proto-regime is the least developed. It involves the bilateral agreement between China and the United States regarding economic cyber espionage. In a September 2015 statement, the two governments indicated that "neither the U.S. nor the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage." The agreement also provided for the establishment of additional government-to-government contacts for the review of cybercrime allegations.[28] Published reports have indicated that American firms continue to suffer intrusions originating in China that are said to be attributable to government-linked hackers.[29] Accordingly, it is important to be realistic about the likelihood of Chinese compliance; however, it may be that the value of the agreement is in publicly committing China to a norm from which its derogation can be criticized. International relations professor Daniel C. Thomas, whose research focuses on issues of European integration and international governance, has argued that the Helsinki Accords had this effect in committing the Soviet Union to human-rights norms and thereby helping to bring about the end of Communist rule.[30]

Thus, prohibition regimes are an important component of a global-governance toolkit. There are good reasons to believe that some of the regimes discussed above have at least reduced the incidence and severity of particular kinds of undesirable conduct; however, these regimes vary in their comprehensiveness, formality, and effectiveness. In assessing the likely effectiveness of a cyber-prohibition regime, a number of foreseeable problems arise pertaining both to whether other actors can be convinced to adopt a prohibition regime and whether a prohibition regime can be effectively implemented even if other actors are convinced of its utility and appropriateness.

Prohibition regimes are typically employed to deal with conduct that is widely agreed to be immoral or unethical. Thus, the degree of moral revulsion generated is an important determinant of whether actors will agree to them. To the extent that some actors see different forms of cyber conduct as consistent with their identities or their substantive understandings of justice, they are unlikely to agree to prohibit such conduct. State conduct of economic cyber espionage provides an illustrative example. Some states and their populations may retain a more mercantilist understanding of what Australian constructivist scholar Christian Reus-Smit has called "the moral purpose of the state"[31] and thus believe aiding national firms counts (at least in the domestic arena) as praiseworthy state conduct. Such an argument is consistent with international security specialist Jacques Hymans's finding that leaders' perceptions of national identity are an important driver of state decisions regarding nuclear proliferation.[32]

Even if actors agree on what behaviors they want to prohibit, there may be other reasons a global prohibition regime lacks effectiveness. Political scientists Margaret Keck and Kathryn Sikkink have suggested that transnational advocacy networks are most successful in achieving their objectives when they are opposing conduct that entails physical harm to innocents and when that harm is the result of a short causal chain that easily connects the behavior with the resulting harm.[33] Given that many cyber harms accrue in the first instance to corporations rather than individuals (for example, intellectual property or brand damage), it may be difficult to generate sufficient moral revulsion to support a broad regime prohibiting many forms of problematic cyber conduct. Further, many cyber harms typically involve highly complex and opaque causal chains

that individual policy makers and voters are unlikely to understand in any depth.

Convincing others to support a prohibition regime dealing with particular forms of cyber conduct will also be more difficult to the extent that prohibiting such conduct will also undermine actors' attempts to achieve other valued goals. There are a variety of problems associated with dual-use technology. State security agencies, for example, may see particular forms of malicious code as critical to fulfilling their war-fighting and intelligence-gathering missions—even if they might agree that some uses of such technologies should be restricted.

Research also indicates that the presence of powerful champions on either side of an issue can affect the success or failure of advocacy efforts.[34] Such champions matter not only in terms of persuading other actors but also in determining which issues advocates decide to contest; further, champions may be organizations occupying positions of network centrality, in addition to individual norm entrepreneurs.[35] While the United States has attempted to champion a norm against economic cyber espionage, its efforts have been undermined by revelations about the activities of the American intelligence community. Most technology sector and civil-society organizations have focused on contesting privacy and other human-rights issues, whether or not in response to state surveillance online. Reluctance to publicly disclose data breaches to protect reputation and share value may well limit the willingness of other firms to champion prohibitions on many forms of problematic cyber conduct.

Implementing Cyber Prohibition

Aside from challenges in securing political agreement on an expanded, robust cyber prohibition regime, there are two important aspects to address in implementing any such measures: the use of formal versus informal instruments and complications arising from monitoring and enforcement.

Most global-prohibition regimes rely heavily on formal legal instruments that codify the proscribed behavior and obligations of various parties for monitoring, enforcing, and otherwise implementing the ban. However, considerable risks are associated with the use of hard-law instruments in this context; soft-law modalities may be more effective.[36] First, treaties and customary international law bind only states. Given the low barriers to entry and the key role of the private sector in the cyber domain, a hard-law global-prohibition regime would not directly

bind many of the relevant actors. Further, insofar as a hard-law instrument binds states to implement and enforce prohibitions within their own borders and to cooperate with other states in doing so, it could be expected to lead to a substantial number of requests under existing mutual legal-assistance treaties. Where mutual legal assistance is not effective, there may also be attempts to employ the law of state responsibility to pursue remedies. Such measures would place states in the difficult position of being responsible for the management of problem-solving on a global network that is expected to expand to several billion connected devices and on which it is often difficult to attribute particular conduct to specific actors. Even for advanced industrial democracies, it is questionable whether such arrangements are feasible; for emerging markets and developing states, the situation would be even more difficult.

A second reason to be skeptical of hard-law instruments for prohibiting problematic cyber conduct is that there are legitimacy risks associated with the codification of rules that are either unlikely to be obeyed or extremely difficult to enforce. Such rules risk becoming dead letters and serving as constant temptations for violators to argue that actors do not believe the proscribed conduct is actually inappropriate.

Finally, monitoring and enforcement present serious challenges for a global-prohibition regime in the cyber domain, whether it is implemented via hard- or soft-law mechanisms. The issue presents clear enforcement problems among a large number of actors on an issue where attribution is generally difficult. Therefore, violations are both likely and difficult to prevent or punish. Access to the technology required to conduct such activities is already widespread and available from a large number of suppliers based in different countries. These technologies also typically have multiple purposes, further complicating efforts to curtail proliferation.

Despite these considerable challenges, soft-law prohibition norms are generally inexpensive to promote and can have substantial constraining effects on behavior when internalized. Accordingly, current prohibition efforts should be pursued with the realization that they will not provide sufficient tools to deal with problems arising from decentralized governance of a shared global facility. In particular, prohibition should be coupled with robust, institutionalized means of responding to intended and unintended disruptions to Internet stability and interoperability.

The Responsibility to Troubleshoot

The insufficiency of global-prohibition norms to deal with problematic cyber conduct means that there will be an ongoing need for mechanisms to mitigate and manage such conduct when it does occur. While these mechanisms will naturally involve technology (improving hardware, software, and related technical standards), policy must also include attempts to address the social dimensions of such conduct or run the risk that bad actors will adapt and innovate, finding new ways to realize their goals. Measures should be aimed at reducing the frequency and severity of disruptive cyber conduct, fostering cooperation in repairing damage caused by misconduct, and preventing the escalation of such incidents into even more serious disputes or conflicts. Cultivating a responsibility to troubleshoot can enhance global capacity to manage challenges associated with decentralized cyber governance.

Coping with Unintended Consequences

The core challenge is to cope with negative effects on the stability or global interoperability of cyberspace. Since these kinds of effects are not typically intended outcomes, the remainder of this article emphasizes means for coping with unintended consequences rather than with intended effects. However, since determining intention is often difficult in practice, there is a strong argument for presuming any such negative effects to be unintended. If nothing else, publicly treating such events under a presumption that they are unintended serves two valuable purposes. First, it reduces the likelihood of hostility and escalation. Second, refusal to cooperate in resolving problems may provide prima facie evidence to third parties that the effect was intended (or at least welcomed) and demonstrate bad faith on the part of the responsible actor, thereby increasing reputational costs from engaging in such conduct.

Resolving these problems requires effective and reliable methods of quickly identifying and remedying the effects of malicious code and other means of disrupting cyberspace. These tasks are complicated not only by technical problems of diagnosis, attribution, and implementation but also increasingly by problems of jurisdiction in what Naval War College professors of strategy Chris C. Demchak and Peter Dombrowski have termed a cybered Westphalian age.[37] The decentralized nature of the international system and the cyber-regime complex create or exacerbate a host of problems in securing broad, reliable cooperation in responding to

disruptions in the cyber domain. Aside from complications arising from domestic politics and international rivalries, these difficulties include differences in culture, institutions, specific domestic legal regimes, and basic capacity (infrastructure, skilled personnel, and financing).

Furthermore, it is not immediately obvious who should be responsible for *providing* such cooperation. Most Internet infrastructure is privately owned, and most jurisdictions have multiple large-network operators. Are such firms responsible, and if so, are they individually or collectively responsible? Further, a variety of actor types transmits information over these networks. In some cases, this information itself may be responsible for the disruption. What responsibility do Over-The-Top content providers, non-technology firms acting as Internet consumers, state actors, civil-society groups, and private individuals bear? Computer emergency response teams (CERTs) typically assume responsibility for this level of cooperation and assistance as part of their mission statements,[38] but CERTs are highly varied in their capacity and in their scope of work.[39]

These difficulties will not be quickly or easily overcome. One useful step in doing so, however, would be to supplement prohibition efforts with the cultivation of a norm that all relevant actors must participate in good faith in efforts to resolve threats to the stability and interoperability of cyberspace. This requirement can be understood as an R2T. The underlying rationale for this suggestion is that norms shape behavior in a number of ways, for example by reducing the propensity of actors to engage in conduct that violates applicable norms and by shaping responses to violations by prompting criticism or sanctions.[40] Note, especially, that because they enable criticism and sanctioning behavior, norms can have significant and helpful effects even in cases where compliance falls substantially short.

The notion that even sovereign states have international responsibilities should not be controversial. The most basic of these—noninterference in the domestic affairs of other states—is foundational to the modern international system. Several other responsibilities are inherent to modern international law. These include the principle that treaties must be observed (*pacta sunt servanda*) and other *jus cogens* principles. The bodies of customary and conventional international law are also similarly binding on sovereign states. Among the latter, the UN Charter deserves special mention in creating responsibilities pertaining to the use of force and to compliance with measures authorized by the UN

Security Council. The 2015 GGE report affirmed the applicability of the charter, in its entirety, in the cyber domain.[41]

As with any other field of social life, actors will sometimes fail to live up to their responsibilities. International law explicitly contemplates such situations. It does so in the first instance by making states responsible for their internationally wrongful acts, requiring them to provide apologies, damages, and other forms of restitution. Absent their willingness to do so, international law also authorizes wronged states to take certain self-help measures. Most importantly, even in exercising self-help, states have responsibilities to do so according to the terms of identifiable rules. As with rules of the road in many other areas of international politics, the law of state responsibility has taken important steps toward codification (and thus greater precision) in the latter half of the twentieth century. [42] This effort has, thus far, culminated in the publication of the International Law Commission's *Draft Articles on Responsibility of States for Internationally Wrongful Acts.*[43] While not yet formally adopted by states in the form of a treaty, the articles have been endorsed on multiple occasions by the UN General Assembly.

If anything, contemporary understandings of sovereignty are increasingly qualified by concomitant responsibilities. The "responsibility to protect" (R2P) is an important recent example.[44] Further, notions of international responsibility are increasingly extended to non-state actors. The International Criminal Court recognizes individuals as bearing responsibility for certain kinds of grievous offenses even when undertaken in an official state capacity. Efforts to inculcate an ethos of corporate social responsibility, such as the UN Global Compact, also seek to create and uphold responsibilities for firms. It should not be controversial to extend notions of international responsibility, including an R2T, to various kinds of non-state actors.

Relationship to Responsibility to Protect

The R2P is arguably the most significant addition to the body of international responsibilities since 1945. Rather than a single responsibility, it entails three related responsibilities arranged to ensure the greatest possible redundancy while reducing costs in terms of both sovereignty and enforcement. The primary obligation is that of the state to its own citizens, specifically, to protect them from genocide, war crimes, and crimes against humanity. This obligation includes not committing or

inciting those acts against the state's own population, as well as protecting the population against the perpetration of such acts by third parties. The international community also has, in the first instance, the obligation to "encourage and assist" states in carrying out this obligation to their own citizens. In cases where states are unwilling or unable to fulfill the primary responsibility, R2P holds that the international community has a collective responsibility to provide such protection. It specifies that this is preferably done by peaceful means but that stronger measures are authorized if such means are impractical or unsuccessful.[45]

While the legal status of R2P is admittedly uncertain and the analogy between the R2P and any potential R2T is imperfect at best, surveying these shortcomings is instructive for effectively advocating and implementing an R2T. First, given the privatization of key Internet infrastructure, the limited capacity and expertise of many states with cyber operations, the low barriers to entry for the creation of significant cyber disruptions, and the difficulty of decisively attributing specific conduct to particular actors, allocation of an R2T exclusively to states would be unlikely to prove effective. In keeping with the avowedly multi-stakeholder nature of Internet governance, any R2T would need to be borne not only by states but also by firms and voluntarily by organizations with the means to contribute to ensuring its efficacy.

Second, the nature of the foundational responsibility in the two situations differs. The R2P is foremost an obligation of the state to its own citizens. In contrast, an R2T would be offered equally by states to citizens and noncitizens since it pertains in substance to the functioning of a global communications facility. Further, if the R2T is borne in part by non-state actors, it cannot be owed on the basis of the relationship between state and citizen. The conception of the Internet as a governance system comprised of a set of nested clubs, as mentioned earlier, provides two distinct and non-mutually exclusive bases for grounding an R2T. On one hand, the obligation can be grounded in reciprocity: the responsibility of all clubs of Internet users to refrain from disruptive cyber conduct in return for the assurance that all other clubs will provide them the same consideration. This ground creates an obligation owed by groups to other groups. On the other hand, the obligation can also be grounded in the terms of membership for the most basic and universal club: the club of all global Internet users. This ground creates an obligation owed by members of a group to each other. Both routes are possible, and both

can be pursued without contradiction since the substantive obligation is the same in both cases. Given the lack of a strong cosmopolitan ethos and the strength of more particularistic attachments in social life, the first basis may well prove more compelling overall, but the cosmopolitan basis resonates more clearly with the human-rights regime.

Third, the nature of the subsidiary collective responsibility also differs. The difficulty of attributing cyber conduct poses severe challenges for any efforts to implement collective action to intervene in the case of major cyber disruptions or extremely significant levels of other problematic cyber conduct such as large-scale economic cyber espionage. Taking steps that might include property damage or loss of life, at least with the collective authorization envisaged by the R2P, will likely demand the ability to demonstrate culpability in a public and convincing manner. At a more pragmatic level, inaccurately directed responses are unlikely to eliminate the undesired conduct and are further likely to prompt retaliation and loss of legitimacy. It is also doubtful whether there are any forms of cyber conduct sufficiently grave to satisfy the proportionality standards implicit in the R2P, which applies only in situations of genocide, war crimes, and crimes against humanity. Prior to reaching this level, such cases would almost certainly trigger other rules permitting a collective response, like the UN Charter provisions for self-defense and for the maintenance of international peace and security. The R2T is a means for addressing conduct of serious international concern that falls short of the extreme acts that trigger the R2P. Therefore, there is no need for the R2T to require (or authorize) more than the use of peaceful, cooperative means. The concept of a responsibility to troubleshoot cannot be a panacea to answer all problems arising from the cyber domain. To the extent that this responsibility is adopted, however, some problems can be made less severe and perhaps reduced in frequency. It is therefore a potentially important component of the broader cyber-regime complex currently in the process of formation. The R2T proposed here is consistent with the recommendations of the 2015 Group of Governmental Experts. The GGE endorsed assistance for less-developed countries but also indicated that "capacity-building involves more than a transfer of knowledge and skills from developed to developing States, as all States can learn from each other about the threats that they face and effective responses to those threats." This speaks to a broad awareness that international cyber assistance is not simply a matter of development. Further,

the group proposed several candidate norms that indicate general support for the notion that providing assistance is appropriate international behavior.[46] These candidate norms are discussed in more detail below. In general, the GGE recommendations are primarily focused on state actors and do not develop the notion that an R2T might also apply to non-state actors. Further, given the preliminary state of international legal development in this area, the GGE merely expresses support for candidate norms. This is a sensible starting point but falls well short of a notion of responsibility.

Implementing the Responsibility to Troubleshoot

Several current and future options exist for implementing the R2T. As in many other areas of Internet and cyber governance, states have useful roles. One such role pertains to information sharing. In general terms, this may involve sharing information on an ongoing basis to facilitate diffusion of best practices in cybersecurity. The GGE suggested, for example, that states should "encourage responsible reporting of ICT [information and communications technologies] vulnerabilities and share associated information on available remedies."[47] Information sharing may also involve more specific efforts in response to particular instances of problematic cyber conduct. This cooperation will often involve law enforcement agencies. In this vein, the GGE called for states to "consider how best to cooperate to exchange information, assist each other, prosecute terrorist or criminal use of ICTs, and implement other cooperative measures to address such threats."[48]

State involvement in implementing an R2T will need to go beyond information sharing to encompass a direct role in incident response. States are already significant network operators; their activities in this regard may have unintended effects on other parties. Further, as states play larger regulatory roles in the cyber domain, the number of channels through which state action can produce negative effects on Internet stability and interoperability is likely to grow. Finally, many states have created bodies to assist firms and individuals in dealing with cyber disruptions. These bodies may themselves produce unintended consequences for users outside the state's jurisdiction. In each of these cases, the state is itself the source of a kind of problematic cyber conduct. It is not unreasonable to suggest, therefore, that it bears a degree of responsibility to those affected by its actions. Even where the state is not the direct cause

of cyber conduct that damages others, it may bear some responsibility under international law to states whose citizens are adversely affected.

The GGE took preliminary steps toward recognizing such responsibilities in proposing that states should "respond to appropriate requests for assistance by other States whose critical infrastructure is subject to malicious acts" and that they should "respond to appropriate requests to mitigate malicious activity aimed at the critical infrastructure of another State emanating from their territory."[49] While promising, these candidate norms are limited only to acts that target the critical infrastructure of other states, leaving most firms and citizens of other states relatively unprotected. In limiting the candidate norms to covering "malicious acts" the GGE also left unintended consequences (the primary problem discussed in this article) unaddressed. Further, there are numerous ambiguities in the phrasing. It is not clear, for example, what constitutes an "appropriate request" or even what is included under "critical infrastructure." Even if these candidate norms are ultimately accepted by most states, additional work remains to be done.

The work of mitigating and resolving problematic cyber conduct once it has begun is in large part dependent on technical competencies in engineering and computer science. But such work cannot occur effectively and reliably at the global level without proper governance and administrative structures to enable it. Over the last several years, Internet governance issues have become increasingly contested. Individual governments, including those of the United States, China, Russia, Brazil, and others, have initiated or increased efforts to exert influence over these issues. Incumbent entities including the Internet Corporation for Assigned Names and Numbers, the Internet Engineering Task Force, and the Internet Society (ISOC) have also undertaken efforts to defend or expand their roles, and other players like the International Telecommunication Union (ITU), Organization for Economic Cooperation and Development (OECD), and World Economic Forum (WEF) have also sought enhanced roles. Of particular importance in implementing the R2T, however, are organizations dedicated to emergency response. CERTs, sometimes called computer security incident response teams (CSIRT), can—and often do—play important roles in efforts to respond to cyber disruptions.

Since 1990, the Forum of Incident Response and Security Teams (FIRST) has provided a degree of coordination among these groups.

Its membership is relatively global but includes little representation in Africa and the Middle East.[50] Further, members are disproportionately clustered in the developed world, and developing world members generally lack resources and expertise. FIRST has also undertaken efforts to coordinate with the International Organization for Standardization (ISO) and ITU to ensure lessons learned from computer security incidents are incorporated into efforts to revise and create technical standards. It is also currently in the process of developing a curriculum to ensure CSIRT training is consistent and of high quality. Individual members also organize and join special interest groups on a voluntary basis according to their interests.

The GGE explicitly recognized the importance of CSIRTs in its 2015 report. It called on states to "not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams . . . of another State" and further indicated that states should "not use authorized emergency response teams to engage in malicious international activity."[51] These candidate norms suggest that there may be support for providing CSIRTs with a degree of protected status under international law.

Existing CSIRT programs and initiatives provide a solid foundation for implementing many parts of an R2T, especially if their trustworthiness and freedom to operate can be protected under international law, but in several important areas further development would be beneficial. First, expanding educational offerings will provide an important service to the global community. Second, additional work is needed in creating organizations in areas of the world where CSIRTs are less common. While FIRST cannot accomplish this alone, it can play an important advocacy and mobilization role alongside assistance from other Internet community organizations and other stakeholders, including governments acting in their capacity as providers of and catalysts for development aid and capacity building. Third, the CSIRT community needs to engage in broader outreach to educate a wider array of organizations about its role and importance. Network operators, technology firms, universities, and some large financial institutions either have their own CSIRTs or are accustomed to working with them, but as the "Internet of Things" dramatically broadens the number of Internet-connected devices and objects, these concerns will become broadly relevant to firms both as producers and consumers. Ensuring that stakeholders are

apprised of appropriate points of contact and available resources will facilitate timely, cooperative mitigation and remediation. These functions all parallel the requirement in R2P that actors assist each other in carrying out their primary responsibility. They are also consistent with other norms in the international system emphasizing the importance of providing capacity-building and technology transfer assistance to developing states.[52] Capacity in this sense includes not only technology itself but also knowledge about governance issues pertaining to information and communications technologies.

The suggestions above deal with education, outreach, and capacity building. In addition, it would be helpful to increase and institutionalize CSIRT cooperation and coordination at a more operational level. One modest first step in this regard would be the establishment of a global clearinghouse system for notification of cyber disruptions and other problematic cyber conduct. Beyond notification, such a system could also perform a "handshaking" function, connecting parties experiencing issues with verified, trustworthy groups with the expertise and willingness to assist. Such a system could also help reduce duplication of effort. Finally, FIRST might play a role in developing and disseminating best practices. States and other stakeholders could play critical supporting roles in these endeavors, including by encouraging or requiring actors to make use of these mechanisms in responding to cyber disruptions rather than (or at least in addition to) employing private means of response.

Many forms of problematic cyber conduct revolve around access to sensitive information. Further, efforts to mitigate such conduct may bring CSIRT members and law enforcement officials into contact with the sensitive information of third parties, including those in other legal jurisdictions—for example, of individuals whose devices are part of illicit botnets. Accordingly, it is vital that efforts to implement an R2T are especially sensitive to compliance with human-rights protections and civil liberties, to prevent the inadvertent agglomeration of excessive powers by law enforcement and security agencies. The GGE recognized the importance of human rights, calling on states specifically to "respect Human Rights Council resolutions 20/8 and 26/13 . . . as well as General Assembly Resolutions 68/167 and 69/106."[53] Each of these resolutions pertains to digital rights. This requirement of an R2T is parallel to the Brazilian notion of a "responsibility while protecting" governing conduct of the international community in upholding the

R2P.[54] Whereas in implementing R2P the primary danger is to individuals' physical security, in R2T the primary danger is to their privacy and digital rights. Accordingly, a responsibility while troubleshooting (RWT) will reflect this difference.

Efforts to implement an R2T must also consider financing mechanisms. Insufficient funding for work on Secure Sockets Layer (SSL) was revealed to have played a role in the failure to identify and rectify the "Heartbleed" flaw.[55] Only after the flaw was publicly revealed did major technology firms agree to provide funding for the development of what had become a backbone of Internet commerce.[56] Financing mechanisms to implement the R2T will need to take advantage of a variety of modalities, including private-sector funding as well as public-private arrangements. However, there are reasons to be wary of unorthodox funding streams and to preserve the notion of public-sector financing (including at the global level) for some key functions.

While voluntary Internet-community efforts to fund and develop technology standards have been largely successful, these efforts may be prone to market failures of the kind that afflicted SSL. Further, it is not immediately obvious that SSL should need to rely on the private sector for funding, given that governments are among its most important users. Government reliance on SSL appears to be increasing. On 8 June 2015, a White House memo announced the requirement that "all publicly accessible Federal websites and web services only provide service through a secure connection" and noted explicitly that "the strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS)," which may use SSL.[57] Setting aside questions about the wisdom of designating a specific single encryption standard for government web services, this public reliance on a particular technology raises the question whether the public should play a role in funding the development and maintenance of that technology.

Regardless of questions about the proper roles for the public and private sectors in financing efforts to deal with problematic cyber conduct, there is a need to ensure that funders do not acquire undue influence over the implementation of R2T. Steps should be taken to implement arms-length arrangements that guard against the corruption or capture of such efforts in the service either of profit or of national interest.

Fully developing and implementing an R2T, including a set of best practices for RWT, would require considerable consultation and care among a diverse set of global stakeholders. The most recent GGE report provides grounds to conclude that major governments may be receptive to some steps in this direction. As international law expert Duncan Hollis has argued, other parts of this agenda may also emerge from regional, bilateral, or even unilateral steps.[58] It would likely also be possible for the technology industry and technical Internet governance bodies to make meaningful progress without including states; however, such scenarios must take into account the possibility that some states could block efforts in their own territory on national security or other grounds and that purely private efforts would likely underprovide services in the developing world.

Conclusion

That states have international responsibilities is beyond doubt, though the nature of those responsibilities continues to evolve. While the notion that non-state actors have international responsibilities is more novel, it is nonetheless increasingly well established in international criminal law, international humanitarian law, corporate social responsibility, and in other issue areas. Nevertheless, there are multiple reasons to doubt the likelihood that efforts to ban problematic cyber conduct will succeed in the foreseeable future. At most, it may be plausible to generate support for a commitment to "do no harm" to the stability and interoperability of the Internet for others, even if some states are determined to exercise increasing surveillance powers and control over access to content within their own borders. Even if a global prohibition regime were adopted, there would be good reasons to ensure the existence of a robust set of institutionalized mechanisms for mitigating and remediating various kinds of intended and unintended disruptions to Internet stability and interoperability.

This article has explored possible modalities for, and challenges in implementing, a responsibility to troubleshoot. An R2T would need to apply to states, international organizations, and technology firms as well as to large commercial Internet users and relevant civil-society groups. The Forum of Incident Response and Security Teams is well positioned for an expanded role; however, realizing this potential will require a great deal of assistance from other actors. Especially in its initial phases,

the R2T should be embodied in hortatory soft-law instruments that permit greater flexibility and experimentation, that carry lower negotiating costs than formal hard-law instruments of international law, and that more easily enable the participation of non-state actors.[59] The R2T should additionally be accompanied by a responsibility *while* troubleshooting that commits engaged parties to implementing best practices for the protection of sensitive data encountered in the process of mitigating and remediating threats to Internet stability and interoperability.

The creation of an R2T and an accompanying RWT will ultimately require a sustained advocacy campaign by a transnational network including government officials, international organization staff, corporate officers, and especially civil-society technologists and activists. Securing agreement on the desirability of social rules and successfully implementing them will no doubt be difficult. However, the alternative is not a scenario in which the cyber domain is entirely ungoverned by rules and in which actors have no responsibilities whatsoever. Cyberspace is already governed by a sprawling array of rules, implemented in a decentralized (and sometimes only partially overlapping) manner by a large number of public and private actors. Further, it is extremely likely that this emerging cyber-regime complex will continue to develop. New rules will be made to govern the cyber domain, some existing rules will fall into disuse, and others will be reinterpreted, changed, and applied in novel ways. The only question is the eventual trajectory of this rule system. Accordingly, it is not immediately clear that the development of an R2T is significantly less likely than other less desirable outcomes. Moreover, the likelihood of particular outcomes can be shaped by the exercise of agency. Since there is no guarantee that the future evolution of the cyber-regime complex will occur in a manner conducive to Internet stability and global interoperability, the R2T is an important hedge against the significant costs associated with cyber disruption in a context of highly decentralized governance. SSQ

Notes

1. Laura DeNardis, *The Global War for Internet Governance* (New Haven, CT: Yale University Press, 2014); Mark Raymond and Laura DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution," *International Theory* 7, no. 3 (2015): 572–616, doi:10.1017/S1752971915000081; and Madeline Carr, "Power Plays in Global Internet Governance," *Millennium: Journal of International Studies* 43, no. 2 (2015): 640–59, doi:10.1177/0305829814562655.

See also Tim Maurer, "Cyber Norm Emergence at the United Nations—An Analysis of the Activities at the UN Regarding Cyber-security," Discussion Paper 2011-11 (Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011), http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

2. United Nations (UN), Office for Disarmament Affairs, "Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," UN General Assembly (UNGA) A/68/98 (2013), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement; and UNGA A/70/174 (2015), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement. For scholarly assessments of the earlier iterations of the GGE, see Maurer, "Cyber Norm Emergence," and Eneken Tikk-Ringas, "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee, 1998–2012" (Geneva: ICT4Peace Publishing, 2012).

3. Mark Raymond, "Engaging Security and Intelligence Practitioners in the Emerging Cyber Regime Complex," *Cyber Defense Review* 1, no. 2 (forthcoming).

4. Joseph S. Nye Jr., "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series*, no. 1 (Waterloo, ON: Centre for International Governance Innovation, 2014), https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf.

5. Mark Raymond and Gordon Smith, eds., *Organized Chaos: Reimagining the Internet* (Waterloo, ON: Centre for International Governance Innovation, 2014); and Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine, and Mark Raymond, "The Emergence of Contention in Global Internet Governance," *Global Commission on Internet Governance Paper Series*, no. 17 (Waterloo, ON: Centre for International Governance Innovation, 2015), https://www.cigionline.org/publications/emergence-of-contention-global-internet-governance.

6. Dennis Broeders, *The Public Core of the Internet: An International Agenda for Internet Governance* (Amsterdam: Amsterdam University Press, 2015), http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_internet_Web.pdf.

7. Duncan Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52, no. 2 (2011): 374–432, http://www.harvardilj.org/2011/07/issue_52-2_hollis/. The concept of R2T is similar to what Hollis has called an "e-SOS" facility.

8. For such a view, see Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013): 30–36, doi:10.1162/ISEC_a_00138.

9. Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs*, International Engagement on Cyber III (2013), 53–64, http://journal.georgetown.edu/wp-content/uploads/2015/07/gjia13005_Raymond-CYBER-III.pdf.

10. Raymond and DeNardis, "Multistakeholderism."

11. Nye, "Regime Complex."

12. Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds., *The Turn to Infrastructure in Internet Governance* (New York: Palgrave, 2015).

13. Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no.1 (Spring 2011): 32–61, http://www.au.af.mil/au/ssq/2011/spring/demchak-dombrowski.pdf.

14. Tanisha M. Fazal, *State Death: The Politics and Geography of Conquest, Occupation, and Annexation* (Princeton, NJ: Princeton University Press, 2007).

15. Ethan A. Nadelmann, "Global Prohibition Regimes: The Evolution of Norms in International Society," *International Organization* 44, no. 4 (1990): 479–526, doi:10.1017/S0020818300035384. Global prohibition regimes date to the earliest stages of the constructivist turn in IR theory.

16. Jan Wouters and Sten Verhoeven, "The Prohibition of Genocide as a Norm of Jus Cogens and its Implications for the Enforcement of the Law of Genocide," *International Criminal Law Review* 5 (2005): 401–4, doi:10.1163/1571812054940049. *Jus cogens* are fundamental principles of international law that are accepted by the international community of states as norms, from which no derogation is permitted.

17. UN, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries," 2008, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

18. Wayne Sandholtz, *Prohibiting Plunder: How Norms Change* (New York: Oxford University Press, 2007).

19. Ward Thomas, "Norms and Security: The Case of International Assassination," *International Security* 25, no. 1 (2000): 105–33, doi:10.1162/016228800560408.

20. UN Office for Disarmament Affairs, The Biological Weapons Convention, 10 April 1972, http://disarmament.un.org/treaties/t/bwc/text.

21. Richard Price, "A Genealogy of the Chemical Weapons Taboo," *International Organization* 49, no. 1 (1995): 73–103, http://dx.doi.org/10.1017/S0020818300001582.

22. Richard Price, "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines," *International Organization* 52, no. 3 (1998): 613–44, http://dx.doi.org/10.1162/002081898550671; and Adam Bower, "Norms without the Great Powers: International Law, Nested Social Structures, and the Ban on Antipersonnel Mines," *International Studies Review* 17, no. 3 (2015): 347–73, http://dx.doi.org/10.1111/misr.12225.

23. Matthew Bolton and Thomas Nash, "The Role of Middle Power-NGO Coalitions in Global Policy: The Case of the Cluster Munitions Ban," *Global Policy* 1, no. 2 (2010): 172–84, doi:10.1111/j.1758-5899.2009.00015.x; and Bonnie Docherty, "Breaking New Ground: The Convention on Cluster Munitions and the Evolution of International Humanitarian Law," *Human Rights Quarterly* 31, no.4 (2009): 934–63, http://muse.jhu.edu/article/363660.

24. R. Charli Carpenter, "Vetting the Advocacy Agenda: Network Centrality and the Paradox of Weapons Norms," *International Organization* 65, no. 1 (2011): 69–102, http://dx.doi.org/10.1017/S0020818310000329.

25. Council of Europe, Budapest Convention on Cybercrime (2004), accessed 17 January 2016, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

26. UNGA A/70/174 (2015), accessed 17 January 2016, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement. See especially 7–8 and 13.

27. Michele Markoff, "Advancing Norms of Responsible State Behavior in Cyberspace," DipNote: US Department of State Official Blog, 9 July 2015, https://blogs.state.gov/stories/2015/07/09/advancing-norms-responsible-state-behavior-cyberspace.

28. Ellen Nakashima and Steven Mufson, "U.S., China Vow Not to Engage in Economic Cyberespionage," *Washington Post*, 25 September 2015, https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

29. Ellen Nakashima, "China Still Trying to Hack U.S. Firms Despite Xi's Vow to Refrain, Analysts Say," *Washington Post*, 19 October 2015, https://www.washingtonpost.com/world

/national-security/china-still-trying-to-hack-us-firms-despite-xis-vow-to-refrain-analysts-say/2015/10/18/d9a923fe-75a8-11e5-b9c1-f03c48c96ac2_story.html.

30. Daniel C. Thomas, *The Helsinki Effect: International Norms, Human Rights, and the Demise of Communism* (Princeton, NJ: Princeton University Press, 2001).

31. Christian Reus-Smit, *The Moral Purpose of the State: Culture, Social Identity, and Institutional Rationality in International Relations* (Princeton, NJ: Princeton University Press, 1999).

32. Jacques E.C. Hymans, *The Psychology of Nuclear Proliferation: Identity, Emotions and Foreign Policy* (Cambridge, UK: Cambridge University Press, 2006).

33. Margaret E. Keck and Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Ithaca, NY: Cornell University Press, 1998), 27.

34. Joshua W. Busby, *Moral Movements and Foreign Policy* (Cambridge, UK: Cambridge University Press, 2010).

35. Carpenter, "Vetting the Advocacy Agenda."

36. On the distinction between hard and soft law, see Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organization* 54, no. 3 (2000): 421–56, http://dx.doi.org/10.1162/002081800551280.

37. Demchak and Dombrowski, "Rise of a Cybered Westphalian Age."

38. For example, see "FIRST Vision and Mission Statement," Forum of Incident Response and Security Teams (FIRST), accessed 8 September 2016, https://www.first.org/about/mission.

39. Mark Raymond, Aaron Shull, and Samantha Bradshaw, "Rule-Making for State Conduct in the Attribution of Cyber-Attacks," in Kang Choi, James Manicom, and Simon Palamar, eds., *Mutual Security in the Asia-Pacific: Roles for Australia, Canada and South Korea* (Waterloo, ON: Centre for International Governance Innovation, 2015).

40. These expectations are consistent with the constructivist literature in international relations. See, among many others: Emanuel Adler, "Seizing the Middle Ground: Constructivism in World Politics," *European Journal of International Relations* 3, no. 3 (1997): 319–63, doi: 10.1177/1354066197003003003; Martha Finnemore and Kathryn Sikkink, "Taking Stock: The Constructivist Research Program in International Relations and Comparative Politics," *Annual Review of Political Science* 4 (2001): 391–416, doi:10.1146/annurev.polisci.4.1.391; and Alexander Wendt, *Social Theory of International Politics* (Cambridge, UK: Cambridge University Press, 1999).

41. UNGA A/70/174 (2015), 12.

42. Kenneth W. Abbott, Robert O. Keohane, Andrew Moravcsik, Anne-Marie Slaughter, and Duncan Snidal, "The Concept of Legalization," *International Organization* 54, no. 3 (2000): 401–19; http://www.jstor.org/stable/2601339.

43. International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, 2001, http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

44. International Commission on Intervention and State Sovereignty, *The Responsibility to Protect* (Ottawa, ON: International Development Research Centre, 2001), http://responsibilitytoprotect.org/ICISS%20Report.pdf.

45. Ibid.

46. UNGA A/70/174 (2015), 11.

47. Ibid., 8.

48. Ibid.

49. Ibid., 11.

50. A complete list of FIRST members (accessed 15 June 2015) can be found at https://www.first.org/members/teams.

51. UNGA A/70/174 (2015), 11.

52. On "special and differential treatment," see Alexander Keck and Patrick Low, "Special and Differential Treatment in the WTO: Why, When and How?" *WTO Staff Working Paper* No. ERSD-2004-03 (2004), accessed 15 June 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=901629.

53. UNGA A/70/174 (2015), 11.

54. Conor Foley, "Welcome to Brazil's Version of 'Responsibility to Protect'," *The Guardian*, 10 April 2012, http://www.theguardian.com/commentisfree/cifamerica/2012/apr/10/diplomacy-brazilian-style.

55. James A. Lewis, "Heartbleed and the State of Cybersecurity," *American Foreign Policy Interests* 36, no. 5 (2014): 294–99, http://dx.doi.org/10.1080/10803920.2014.969176.

56. Jon Brodkin, "Tech Giants, Chastened by Heartbleed, Finally Agree to Fund OpenSSL," *Ars Technica*, 24 April 2014, http://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-fund-openssl/.

57. Tony Scott, Executive Office of the President, Office of Management and Budget, memorandum, subject: Policy to Require Secure Connections across Federal Websites and Web Services, 8 June 2015, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf.

58. Hollis, "An e-SOS for Cyberspace," 426.

59. Mark Raymond, "Renovating the Procedural Architecture of International Law," *Canadian Foreign Policy Journal* 19, no. 3 (2013): 268–87, http://dx.doi.org/10.1080/11926422.2013.845580; Abbott and Snidal, "Hard and Soft Law."

Book Review

Mankind Beyond Earth: The History, Science, and Future of Human Space Exploration by Claude A. Piantadosi. Columbia University Press, 2012, 279 pp.

In *Mankind Beyond Earth*, Claude A. Piantadosi, MD, director of the F. G. Hall Environmental Laboratory at Duke University and 30-year consultant to NASA, examines the plausibility of humankind living beyond Earth. To that end, Piantadosi states that the purpose of the book is to establish evidence supporting a return to the moon. While there is no paucity of literature related to space exploration's past and futuristic examinations of life in space, Piantadosi's work is one of the first to ground the argument firmly in an extensive body of scientific evidence. Despite heavy doses of biology, physics, and chemistry, Piantadosi's work is readily accessible to many readers due to his straightforward explanations.

Given Piantadosi's overarching thesis that argues for an American return to the moon, one might surmise that he would take a purely scientific argumentation. Piantadosi surprises the reader. In building up to his major proposition, Piantadosi reviews the state of US space activity and shows that the technological lead the nation once held is quickly eroding. Moreover, he suggests that America's "scientific illiteracy" tends to devalue science and results in confusion on how to evaluate new science (p. 3). This confusion has led, in his opinion, to the expensive detours of the 2010 National Space Policy's asteroid missions (p. 40). Furthermore, Piantadosi suggests that such shortsightedness may well lead to the United States relinquishing its lead in the space sector to the up-and-coming Chinese space program. In fact, he states that if the nation continues "busily chasing asteroids" and allows the historical trend of space programs to continue, then China will likely beat the United States to the moon, where it will develop the necessary follow-on technologies to voyage to Mars (p. 205).

Still, while there is urgency in Piantadosi's words, he does not conflate aimless activity with deliberate, careful planning designed to further American space power. To wit, he not only cautions against frivolous space excursions but also warns that attempting to be the hare in the next space race could prove unbearably expensive. Instead, the nation must be the tortoise.

Throughout the book, Piantadosi balances between highlighting the urgency of going to the moon, and eventually Mars, with the reality that nothing comes easily in space. In fact, much of the book takes great care in making the case for a return to the moon. Piantadosi takes the first steps in walking this tightrope in his second chapter, where he explains the realities of space and travel within the domain. While he acknowledges the usefulness of futuristic thought, he admits that there is too much to be accomplished now to spend time dreaming of what could one day be (p. 44).

Chapters 3 and 4 provide an historical overview of humankind's space endeavors and, given the author's medical background, the history of the study of physiology in space. Piantadosi uses these two chapters to build the case as to why the United States must return to the moon, which he argues in detail in chapter 5. Importantly, he does

more than merely make the case for a return to the moon; he offers ways to do so with current technology and lists what would be needed to establish a settlement on the lunar surface, which he believes is a requirement for follow-on deep-space exploration.

After offering convincing arguments for returning to the moon, Piantadosi spends the next five chapters discussing the challenges of deep-space exploration. Whether discussing cosmic radiation in chapter 9 or the dilemmas of producing sustenance using indigenous resources in chapters 6 and 7, Piantadosi methodically works towards the culminating point of the book's second part, which is chapter 10's discussion of how humankind will travel to and set foot on Mars.

Such a discussion on the challenges of interplanetary travel leads to part 3, where the author argues why the United States should travel to Mars. Much of the argument hinges on the fact that few other planets provide hospitable environments in which explorers could even venture. Indeed, Piantadosi concludes his final chapter by hearkening back to John von Neumann. He admits that maybe von Neumann was correct in his assessment that the best humanity could do to explore outer space was to send robotic probes. To wit, as humankind learns more about the cosmos, it has discovered the uniqueness of Earth; while there are many potential planets out there, so far, few exhibit the qualities of Earth. Many are inhospitable, and those that may be friendly to humans are sufficiently far away that even relativistic speeds (fractions of the speed of light) make such travel essentially improbable due to concerns over resources, genetic bottlenecking aboard spacecraft, and myriad other reasons. For that reason, Piantadosi states, "Our own uniqueness and space's insuperability are the best incentives we have to take the best possible care of Spaceship Earth" (p. 250).

Overall, this book provides reasonable arguments for an American return to the moon and a follow-on mission to Mars. The biggest critique of the book is the unstated assumption that the United States will go to Mars. In other words, it appears that Piantadosi takes it as a foregone conclusion that the United States will attempt to go to Mars. That is not to say that he builds a straw man argument for returning to the moon. Indeed, his argument for going to the moon is compelling based on its merits without the consideration he gives for subsequent Martian endeavors. Nevertheless, he never fully questions the aim of a US space program. Such a critique has troubled NASA since the United States beat the Soviet Union to the moon in 1969. Back then, national prestige powered our efforts. Today, it seems (and Piantadosi's arguments support this supposition), the nation continues its space program to benefit from the ways that space science can be used to detect problems on Earth, and the nation goes for pure research (pp. 5–6). In other words, the United States continues its largely scientifically focused space program for science's sake. Yet as recently as February 2016, Congress questions the "science for science's sake" approach.

To be fair, Piantadosi does touch on other reasons for returning to the moon. Specifically, he discusses the economic potential of mining and suggests that economic incentives may be the necessary carrot to drive the establishment of a moon settlement (p. 102). He is a medical researcher and not an economist; his argument for bolstering the American space program may gain more traction when combining scientific and

commercial reasons for a lunar return. If "flag follows trade," as many scholars have suggested, then it may be the merchants who lead the nation to Mars and beyond.

The student of strategy can take away three points from this book. The first two points deal with preparation. First, as Piantadosi asserts, space technology requires long lead times. The same might be said of war-fighting capabilities. The strategist, therefore, must account for those lead times in crafting strategy. As J.F.C. Fuller attested, strategy should precede force structure, planning, and expenditure. Yet, if technology is the long pole in the tent, the strategist must accord proper consideration to its development during the formulation of strategy. Second, preparation is also paramount for the strategist in another fashion. The strategist cannot simply select the strategic conditions that are just right but must prepare for those conditions that are wrong (p. 48). Concerning Piantadosi's book and this reviewer's earlier allusion to economic development being the primary driver of future space power development, the strategist cannot solely focus on military matters but must also have a finger on the pulse of the greater environment in which the military operates. Thus, if space development "takes off," then it is reasonable to suggest that the nation will need to protect its space merchants. When combining this assertion with the first takeaway highlighting technology's long lead time, one can conclude that waiting until the time is right equates to tardiness. National defense can ill afford sleeping on the watch.

Third, Piantadosi's final observation may prove the most relevant for the student of strategy. By reminding the reader that careful stewardship of our current planet should out-prioritize seeking other planets, Piantadosi highlights the fact that resources are neither inexhaustible nor invulnerable. In fact, the National Security Strategy and the Air Force Strategic Master Plan espouse these ideas. Accordingly, the strategist should consider new ways of using the resources one has. One can only build strategy's bridge with the materials available. Game-changing technologies like space-based solar power provide one way that the nation can exploit a new development. In the same breath, many discuss third offsets and game-changing weapons. What if a third offset were, instead, a capability that obviated adversary attempts to influence (such as petroleum is now) or interfere with (such as they were during Operation Enduring Freedom) our resources and their concomitant supply chains? Piantadosi does not discuss such ideas, but his ideas lead to such extrapolation and discussion. The scientific material found in Piantadosi's work will not appeal to every reader, but because he forces the reader to think critically about the nation's space program and because his ideas have basis in strategy writ large, this book is highly recommended.

Maj Ryan Sanford, USAF

Relevant Online Reviews: http://www.au.af.mil/au/afri/reviews.asp.

Pussycats, by Martin van Creveld. Reviewed by Rebecca Jensen.

The China Boom, by Ho-fung Hung. Reviewed by David Anderson.

Ancient Chinese Thought Modern Chinese Power, by Yan Xuetong. Reviewed by Maj John Barrett, USAF.

Terrorism in Cyberspace, by Gabriel Weimann. Reviewed by Lt Col Deborah K. Dusek-Wells, USAF, Retired

Mission Statement

Strategic Studies Quarterly (*SSQ*) is the strategic journal of the United States Air Force, fostering intellectual enrichment for national and international security professionals. *SSQ* provides a forum for critically examining, informing, and debating national and international security matters. Contributions to *SSQ* will explore strategic issues of current and continuing interest to the US Air Force, the larger defense community, and our international partners.

Disclaimer

The views and opinions expressed or implied in *SSQ* are those of the authors and should not be construed as carrying the official sanction of the US Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

Comments

We encourage you to e-mail your comments, suggestions, or address change to: **StrategicStudiesQuarterly@us.af.mil**.

Article Submission

The *SSQ* considers scholarly articles between 5,000 and 15,000 words from US and international authors. Please send your submission in Microsoft Word format via e-mail to:

StrategicStudiesQuarterly@us.af.mil

Strategic Studies Quarterly (SSQ)
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112–6026
Tel (334) 953–7311

View *Strategic Studies Quarterly* online at **http://www.au.af.mil/au/ssq/**

Free Electronic Subscription

A forum for critically examining, informing, and debating national and international security.



"Aim High . . . Fly-Fight-Win"