

# SSQ STRATEGIC STUDIES QUARTERLY

---

SUMMER 2018

VOLUME 12, NO. 2

---

## **The 2018 National Defense Strategy: Continuity and Competition**

Kelly A. Grieco

---

## **The Trump Nuclear Posture Review: Three Issues, Nine Implications**

Stephen J. Cimbala

---

### **FEATURE ARTICLE**

## **Attribution and Operational Art: Implications for Competing in Time**

Lt Col Garry S. Floyd Jr., USAF

---

## **Beyond the Tweets: President Trump's Continuity in Military Operations**

Peter Dombrowski

Simon Reich

---

## **A New Security Framework for Geoengineering**

Elizabeth L. Chalecki

Lisa L. Ferrari

---

## **Space Arms Control: A Hybrid Approach**

Brian G. Chow

---

---

# SSQ STRATEGIC STUDIES QUARTERLY

---

## **Chief of Staff, US Air Force**

Gen David L. Goldfein, USAF

## **Commander, Air Education and Training Command**

Lt Gen Steven L. Kwast, USAF

## **Commander and President, Air University**

Lt Gen Anthony J. Cotton, USAF

## **Commander, LeMay Center for Doctrine Development and Education**

Maj Gen Michael D. Rothstein, USAF

## **Director, Air University Press**

Dr. Ernest Allan Rockwell

---

## **Editorial Staff**

Col W. Michael Guillot, USAF, Retired, Editor

Donna Budjenska, Content Editor

Nedra O. Looney, Prepress Production Coordinator

Daniel M. Armstrong, Illustrator

Kevin V. Frey, Webmaster

---

## **Advisors**

Gen Michael P. C. Carns, USAF, Retired

James W. Forsyth Jr., PhD

Christina Goulter, PhD

Robert P. Haffa, PhD

Jay P. Kesan, PhD

Charlotte Ku, PhD

Benjamin S. Lambeth, PhD

Martin C. Libicki, PhD

Allan R. Millett, PhD

---

## **Contributing Editors**

Stephen D. Chiabotti, PhD, *School of Advanced Air and Space Studies*

Mark J. Conversino, PhD, *School of Advanced Air and Space Studies*

Kelly A. Grieco, PhD, *Air Command and Staff College*

Michael R. Kraig, PhD, *Air Command and Staff College*

Dawn C. Murphy, PhD, *Air War College*

David D. Palkki, PhD, *Air War College*

Nicholas M. Sambaluk, PhD, *Air Command and Staff College*

# STRATEGIC STUDIES QUARTERLY

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

SUMMER 2018

VOLUME 12, NO. 2

## Policy Forum

- The 2018 National Defense Strategy:  
Continuity and Competition* ..... 3  
Kelly A. Grieco
- The Trump Nuclear Posture Review: Three Issues,  
Nine Implications* ..... 9  
Stephen J. Cimbala

## Feature Article

- Attribution and Operational Art: Implications for  
Competing in Time* ..... 17  
Lt Col Garry S. Floyd Jr., USAF

## Perspectives

- Beyond the Tweets: President Trump's Continuity in  
Military Operations* ..... 56  
Peter Dombrowski  
Simon Reich
- A New Security Framework for Geoengineering* ..... 82  
Elizabeth L. Chalecki  
Lisa L. Ferrari
- Space Arms Control: A Hybrid Approach* ..... 107  
Brian G. Chow

## Book Reviews

<i>The Logic of American Nuclear Strategy: Why Strategic Superiority Matters</i> .....	133
By: Matthew Kroenig	
Reviewed by: Todd C. Robinson	
<i>Strategic Cyber Deterrence: The Active Cyber Defense Option</i> .....	134
By: Scott Jasper	
Reviewed by: Stephen Bucci	
<i>US Foreign Policy and Defense Strategy: The Evolution of an Incidental Superpower</i> .....	136
By: Derek S. Reveron, Nikolas K. Gvosdev, and Mackubin Thomas Owen	
Reviewed by: LTC Kurt P. VanderSteen, USA, Retired	
<i>Getting Nuclear Weapons Right: Managing Danger and Avoiding Disaster</i> .....	137
By: Stephen J. Cimbala	
Reviewed by: Mel Deaile	
<i>The President's Book of Secrets: The Untold Story of Intelligence Briefings to America's Presidents from Kennedy to Obama</i> .....	139
By: David Priess	
Reviewed by: Damon Coletta	
<i>Future War: Preparing for the New Global Battlefield</i> .....	141
By: Robert H. Latiff	
Reviewed by: Capt Sean E. Thompson, USAF	
<i>Courting Science: Securing the Foundation of a Second American Century</i> .....	143
By: Damon V. Coletta	
Reviewed by: Lt Col Joe Bassi, PhD, USAF, Retired	

# The 2018 National Defense Strategy: Continuity and Competition

After nearly two decades of fighting Islamic terrorists and insurgents, including the wars in Afghanistan and Iraq, the United States Department of Defense is refocusing on great power competition. The unclassified summary of the new *National Defense Strategy (NDS)*<sup>1</sup> is unequivocal: “Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security.” By focusing on near-peer threats and declaring a new era of great power competition, the *NDS* sounds a sober warning: “Today, every domain is contested—air, land, sea, space, and cyberspace.” It lists China and Russia as the central challenges to US prosperity and security and mentions rogue regimes such as North Korea and Iran as destabilizing states, though it is for China alone that the *NDS* reserves its strongest language. Given growing Chinese capabilities and political ambitions, Beijing seeks “Indo-Pacific regional hegemony in the near-term and displacement of the United States to achieve global preeminence in the future.”

To meet such a challenging strategic environment, the *NDS* calls for a “more lethal, resilient, and rapidly innovating Joint Force, combined with a robust constellation of allies and partners” to “sustain American influence and ensure favorable balances of power.” The three pillars of the strategy are to restore readiness and build a more lethal force, strengthen traditional alliances and build new partnerships, and reform the business practices and efficiency of the Pentagon. This *NDS* proposes to drastically reorient US defense priorities to prepare for great power competition and conflict. But to the extent the *NDS* offers a strategy at all, it fits squarely within the post–Cold War strategic tradition of military preeminence and forward-based presence.

Each of the lines of effort—improvements to military readiness and modernization, strengthening alliances and partnerships, and reforms to the department—represents more continuity than change in the Trump administration’s defense policies. First, this *NDS* doubles down on US military investments, striking familiar themes about technological innovation, force modernization, and defense capacity. With calls to “restore readiness and modernize our military,” the strategy seeks to develop and leverage new technologies, such as “advanced computing, ‘big data’

analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology” to gain a decisive competitive advantage over potential adversaries. The idea of leveraging technological innovations is nothing new; it dates back to at least the post–Vietnam War period—and beyond. Indeed, the readiness improvements and technologies singled out as necessary to “ensure we will be able to fight and win the wars of the future” are the kinds of capabilities previously proposed as part the Third Offset Strategy, put forward by former Deputy Secretary of Defense Robert Work.

Second, when it comes to alliances and partnerships, this *NDS* remains firmly committed to a forward military posture and to the alliances and partnerships the current administration inherited. As a candidate, Donald Trump regularly criticized US allies for not contributing a fair share to the burden of collective defense and questioned the relevance of NATO, describing it as obsolete. These complaints were not unfair, as our European allies have cut their defense budgets to the bone since the end of the Cold War. In this new defense strategy, however, the Trump administration toes the line on alliances in Europe and Asia that have been cornerstones of US defense strategy for the past 75 years. This *NDS* echoes former administrations, declaring, “Mutually beneficial alliances and partnerships are critical to our strategy, providing a durable, asymmetric strategic advantage that no competitor or rival can match.” It further affirms the critical role of alliances and partners in “maintaining favorable balances of power that deter aggression and support the stability that generates economic growth.” Even the strategy’s prioritization of the Indo-Pacific, NATO, and the Middle East is nothing new, at least for anyone who has read the 2012 *Defense Strategic Guidance* or the 2014 *Quadrennial Defense Review*.

Along with the European Reassurance Initiative and the renewal of US security guarantees to Japan (both initiatives of the Trump administration over the past year), this *NDS* signals the US will not turn inward as so many commentators feared. If anything, this administration is even more ambitious than the last one as it seeks to attract new partners, thus incurring additional security obligations. Even as this *NDS* proposes “transitioning from large, centralized, unhardened infrastructure to smaller, dispersed, resilient, adaptive basing,” it still envisions a forward force posture, albeit one better able to maneuver and survive under attack. The emphasis of the 2018 *NDS* on US allies and partners thus

indicates that the US global role will not shift dramatically under the “America First” presidency, and the US military presence and operations overseas will continue unabated. In other words, it’s business as usual.

Finally, the promise to reform the business practices and effectiveness of the Pentagon is also nothing new. Almost every secretary of defense promises to reform the defense department. The George W. Bush–era defense reforms of secretary of defense Robert Gates are still ongoing. Gates made a serious effort to overhaul the military’s procurement, acquisition, and contracting process, but more than eight years and two secretaries of defense later, fundamental acquisitions change remains elusive. In recent years, Congress has used the National Defense Authorization Act to mandate organizational reforms within the Pentagon. Current defense secretary James N. Mattis will now have his chance to take on the department’s infamous bureaucracy. Of course the Pentagon is poised to receive a major cash infusion, with defense spending projected to rise to \$629 and \$647 billion for fiscal years 2018 and 2019, a \$165 billion hike over budget caps for the next two years. This budget windfall, even if short-lived, removes financial incentives for the department to become more efficient. Giving the Pentagon all it wants is not the way to inspire innovation and improve efficiency; shrewdly crafted budget constraints may focus it on better spending choices and urgently needed innovation.

But how will building a more agile and lethal, forward-deployed force—even if more innovative and less wasteful—make the US more secure? The United States is inherently secure, with the largest economy in the world and an enviable geographical position, endowed with ample natural resources, wide oceans, and relatively weak neighbors to the north and south. All of this suggests that the American security position is far from precarious. And yet the United States spends more on national defense than all of its competitors’ militaries combined. How will seeking more military power by spending more on national defense better protect the American people and their interests?

Unfortunately, the unclassified summary of the *NDS* leaves this critical question not only unanswered but also unasked. The closest it comes is with the pronouncement, “The surest way to prevent war is to be prepared to win one.” It is difficult to argue against such logic. But none of the strategic difficulties of the past two decades have arisen because the military was not strong enough to prevail in battle, a point apparently lost on this administration. As Gates observed astutely, “One of

the most important lessons of the wars in Iraq and Afghanistan is that military success is not sufficient to win.”<sup>2</sup> In short, more military means alone are not sufficient to achieve US national security objectives.

As a statement on strategy, this *NDS* is wanting, as it offers no discernible theory of victory. A good defense strategy aligns policy, that is, the political *ends*, with strategic *ways* and military *means* as well as offers a theory of how and why the specific force structure, force posture, and mix of capabilities should be expected to achieve the desired outcomes. In this defense strategy (at least, the unclassified summary), the pursuit of military power is the end in itself. It is unclear what building an even stronger military accomplishes in terms of US interests in the South China Sea or confronting Russian aggression.

Instead of reflecting on the strategic blunders of the past 16 years, the administration embraces the mistaken notion that a more muscular approach to American foreign policy improves our relative power position. The *NDS* depicts the emerging security environment as “more complex and volatile than any we have experienced in recent memory” and warns the “long-standing rules-based international order” is under severe threat. Both China and Russia are building militaries to compete with the United States, North Korea has acquired nuclear weapons, Iran has grown more aggressive across the Middle East, and operations continue unabated against jihadist terrorists. Given the United States has been the single most powerful state in that global order, could it be that the militarized and forward-leading foreign policy of the last two decades contributed to these worrisome trends?


Regardless, this *NDS* advances the same self-defeating, unnecessary, and costly strategic prescriptions as the Clinton, Bush, and Obama administrations. It characterizes the past 16-plus years as “a period of strategic atrophy” when it has been anything but. The US has not suffered from an absence of strategy but has instead pursued a consistent strategy of primacy since the end of the Cold War. From the wars in Iraq and Afghanistan to military interventions in Bosnia, Kosovo, Libya, and Syria as well as counterterrorism worldwide and freedom-of-navigation operations in the Persian Gulf and the Pacific, the US has consistently sought to remain the strongest military power in the world and shown a willingness to use military force to shape the global order.

Unfortunately, this muscular strategic approach has been largely unsuccessful. Strategic activism has generated predictable pushback from



other states and nonstate actors. Together with the *National Security Strategy*, this *NDS* adheres to the same grand strategy of primacy as practiced for nearly 30 years, supported by a massive increase in defense spending. But more of the same is likely only to reproduce the same pattern of strategic frustration that the US has experienced since the end of the Cold War: irremediable disorder and self-generated threats.

What is the United States to do? For most academic realists, the answer is clear: focus a more restrained grand strategy on preventing Chinese dominance of the Indo-Pacific region. Since the US is relatively secure and therefore faces few threats to its safety, it need not engage in unnecessary, risky, and costly military activities in a fruitless attempt to preserve American global primacy. History attests repeatedly to the self-defeating nature of great power ambitions and warns against the risks of actively pursuing power-maximizing strategies. For the past 30 years, the American hegemonic project has proved both unsustainably expensive and strategically illusory.

Instead, the US should pursue a more cautious, balance-of-power strategy in Asia while engaging with regional actors to limit the capacity of jihadist terrorists to strike the homeland. Consistent with the emphasis of this *NDS*, a strategy of restraint prioritizes great power competition over terrorism. Given concerns about the rise of China, it would focus on the deterrence and containment of Chinese military power. At the same time, it would shift most of the burden of building military power to deter Russia in Europe to the Europeans, so that the United States can better concentrate its resources in the Indo-Pacific theatre. It would also mean avoiding unnecessary wars, including a preventative attack on nuclear North Korea. The US military would be less active. Used sparingly, American economic and military power should not be squandered in futile attempts at remaking the internal affairs of other countries by the point of the spear—a conclusion shared by this *NDS*. Such a strategy calls for the United States to exercise more discipline in its policy goals and military means, avoid unnecessary military engagements, and genuinely reconstitute the nation's strength for this era of renewed great power competition. 

**Kelly A. Grieco**

*Air Command and Staff College  
Air University*

**Notes**

1. The excerpts in this policy forum piece can be found in Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Office of the Secretary of Defense, 2018), <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
2. Robert M. Gates, Landon Lecture (speech, Kansas State University, Manhattan, KS, 26 November 2007), <http://archive.defense.gov/speeches/speech.aspx?speechid=1199>.

# The Trump Nuclear Posture Review: Three Issues, Nine Implications

President Donald J. Trump's *Nuclear Posture Review (NPR)* is especially important because of its timing and contents.<sup>1</sup> Together with the administration's *National Security Strategy* and other documents related to defense and security policy, the *NPR* offers both continuity and change with respect to the Obama administration's policy statements and guidelines. Russia and China are identified in national security documents as US peer competitors and as systemic disrupters that constitute the main threats to international stability and future American security. This recognition in the *NPR* and other documents of a return to great power rivalry as the fulcrum of military-strategic activity, including deterrence, explicitly embraces political realism as the preferred model for interpreting international politics.

Some of the Trump administration's proposed changes in nuclear policy and force structure planning affect US national security in three aspects: nuclear force modernization, nuclear arms control, and non-proliferation. Although theorists and military strategists may treat these three issues as distinctly compartmentalized, in practice they overlap and together contain important implications for nuclear deterrence. Summarized below are nine such implications.

First, the Trump administration plans to deploy new lower-yield warheads, including weapons for use on Trident II D-5 submarine-launched ballistic missiles. The implication is that this would provide additional targeting options for the most survivable arm of the strategic nuclear triad. New warheads for Trident missiles might be as low as 1 to 2 kilotons, as opposed to 100 kt or more, allowing for more discrimination in target selection and less collateral damage in case of actual use.

Second, a new nuclear-capable sea-launched cruise missile (SLCM) would be developed and deployed. The proposed deployment of nuclear-capable SLCMs is a good illustration of an issue that overlaps force modernization and arms control stability. Nuclear-armed SLCMs were previously deployed by the US until 2011 when the program was cancelled. The assumption is that the nuclear SLCM would provide additional non-strategic nuclear response capability that is rapidly deployable in theater conflicts in Europe or Asia. These capabilities would contribute to US nuclear reassurance of allies who might otherwise be more vulnerable

to nuclear blackmail. Sea-launched nuclear missiles could also support arms control: they would be neither first-strike vulnerable nor most suitable for preemptive attacks. The possible deployment of nuclear SLCMs could also be used as bargaining chips as against Russian departure from the Intermediate Nuclear Forces (INF) Treaty (like the original ground-launched cruise missiles in the 1980s, prior to the INF Treaty) and resulting deployment of additional nonstrategic nuclear weapons in European Russia.<sup>2</sup> However, expert analysts have warned that new sea-based nuclear weapons can have drawbacks with respect to deterrence and arms race stability. According to Lawrence J. Korb, “Because the United States already has a sub-launched conventional cruise missile, adding a nuclear cruise missile to the inventory means the Russians would have to assume any (submarine-launched) cruise missile is in fact a nuclear weapon. And finally, producing new small-yield nuclear weapons could provoke an arms race in that realm—even though the United States already possesses 1,000 low-yield nuclear weapons, including the B-61 bomb and an air-launched cruise missile that can deliver yields between 0.3 to 170 kilotons.”<sup>3</sup>

Third, the Trump administration foresees an increased probability for a nuclear response to a strategic nonnuclear attack, for example, cyberattacks that might cause large numbers of US or allied casualties; widespread destruction of critical infrastructure, including electric power grids, communications, and digital supervisory control and data acquisition systems; and, especially, cyberattacks against components of nuclear command, control, and communications (C3) and early warning systems. Of course, this assumes that the problem of attribution of the source for any such cyberattack could be solved with sufficient clarity—no small challenge.<sup>4</sup>

Fourth, nuclear planning guidance assumes that a wider spectrum of nuclear capabilities is necessary to improve deterrence of Russia and China. Administration planners are especially concerned about Russian and Chinese temptations to “escalate for de-escalation”: to engage in limited nuclear first use to prevent defeat in a conventional war, with the expectation that the other side would back down. This line of thinking follows the arguments of some expert analysts that effective deterrence now requires greater attention to threats posed by diverse adversaries and contexts, including the possible exploitation of limited nuclear threats and/or nuclear coercion by great powers and rogue states.<sup>5</sup> On the one

hand, the *NPR* addresses the concern that a larger spectrum of nuclear weapons could make decision makers more prone to engage in nuclear first use. It states, “To be clear, this is not intended to, nor does it enable, ‘nuclear war-fighting.’ Expanding flexible US nuclear options now, to include low-yield options, is important for the preservation of credible deterrence against regional aggression. It will raise the nuclear threshold and help ensure that potential adversaries perceive no possible advantage in limited nuclear escalation, making nuclear employment less likely.”<sup>6</sup>

On the other hand, whether the availability of a wider range of nuclear yields will increase the likelihood of escalation is dependent not so much on military-technical factors as on political ones. It is unpredictable before the fact whether the “deterree” on the receiving end of an intentionally limited nuclear attack will interpret these strikes as deliberately controlled bargaining measures or as preludes to a more ambitious symphony of destruction.

Fifth, there is little apparent emphasis on the importance of nuclear arms control, including extension of the New START strategic nuclear arms reduction treaty (signed in 2010 and expiring in 2021 unless extended to 2026 by mutual agreement). Trump’s position on New START extension is unclear. Also with respect to nuclear arms control, the US and Russia are possibly on a path of permanent departure from one of the most important arms limitation agreements of the previous century: the INF Treaty that has prevented for decades the development and deployment of US and Soviet or Russian ground-launched ballistic and cruise missiles within the ranges of 500–5,500 kilometers.

Some Russians now regard this treaty as obsolete and argue that INF has increased Russia’s vulnerability to neighboring states with growing inventories of ballistic missiles. As well, Russia views NATO enlargement and US missile defense deployments in Europe as provocative to its security, requiring a larger menu of usable nuclear weapons and launchers deployed in Europe. But the US and NATO regard Russia’s annexation of Crimea and destabilization of eastern Ukraine, together with Russia’s frequent reminders of its nuclear capabilities with respect to perceived threats from the US and NATO, as provocative and destabilizing of European security, therefore requiring enhanced NATO preparedness across the spectrum of deterrence.

Sixth, there is not much apparent interest in the topic of nonproliferation, with the exception of North Korea and Iran. Trump wants to scuttle

the Iran deal or revise it, which puts the United States at potential odds with the other members of the five permanent members of the UN Security Council (China, France, Russia, the United Kingdom, and the US) plus Germany who are cosignatories to the *Joint Comprehensive Program of Action*.<sup>7</sup> Supporters of the Iran nuclear deal feel that abrogation of the agreement would actually increase the risk of Iran eventually becoming a nuclear weapons state. Critics of the Iran nuclear deal argue that it merely slows down Iran's march to the bomb and allows Iran to move closer to the status of a virtual nuclear weapons state, meanwhile expanding its inventory of long range missiles with reach across the Middle East and into Europe.

Seventh, the nuclear modernization plan to support the Trump policy review accepts the Obama modernization plan committing an estimated \$1.2 trillion over 30 years, plus new weapons proposed by Trump.<sup>8</sup> The Trump *NPR* modernization will maintain all three legs of the current strategic nuclear triad of intercontinental land-based missiles (ICBM), submarine-launched ballistic missiles (SLBM), and bombers. The *NPR* notes that eliminating any leg of the triad would “greatly ease adversary attack planning” and “allow an adversary to concentrate resources and attention on defeating the remaining two legs.”<sup>9</sup> Ohio-class ballistic missile submarines (SSBN) will eventually be replaced by Columbia-class SSBNs, maintaining at least 12 SSBNs available throughout the transition. The US ICBM force of Minuteman III missiles will be replaced beginning in 2029 by the ground-based strategic deterrent, including the modernization of some 450 launch facilities supporting a deployed ICBM force of 400 missiles.<sup>10</sup> The administration also plans to deploy a next-generation strategic bomber (the B-21 Raider) that will eventually replace elements of the conventional and nuclear-capable bomber force, beginning in the mid-2020s. Currently the bomber leg of the triad consists of 46 nuclear-capable B-52H and 20 nuclear-capable B-2A strategic bombers.<sup>11</sup> Critics have questioned whether a new strategic bomber and a replacement for the air-launched cruise missile called the long-range stand-off cruise missile are both necessary and whether a new land-based missile is needed to replace Minuteman III or if Minuteman should be refurbished at lower cost.<sup>12</sup>

Eighth—ignored or virtually so—is the accelerating risk of war due to accident or miscalculation, especially in Asia but also in Europe as between Russia and NATO.<sup>13</sup> Too many US and Russian nuclear missiles remain

on alert, according to some expert analysts; others dismiss this as a serious problem. Cold War history shows that in times of peace or crisis leaders may misperceive warning information or misinterpret the behavior of their counterparts. Future warning and command and control systems may invite attack on themselves unless they are protected against prompt cyberattacks or lurking malware inserted prior to the eruption of a crisis.

Ninth and more abstract, a case can be made for the arrival of cognitive deterrence as an umbrella term to refer to present and future challenges to nuclear stability and security. To some extent deterrence has always been about psychology and mind games, as the works of noted theorists such as Robert Jervis and Thomas Schelling have explained.<sup>14</sup> However, at the level of applied science and military-strategic planning, many past issues of deterrence were argued about in terms of hardware: numbers and kinds of launchers, warheads, re-entry vehicles, and the physics or engineering of their performance parameters. Future deterrence discussions must also take into account the priority of software and network security. The scope of such discussions will include the potential for flawed or degraded networks and nuclear C3 systems to fail the required crisis management, intrawar deterrence, or conflict termination “stress tests.”<sup>15</sup> “Deterrence” old style is a difficult term to apply in cyberspace, and cyberspace itself is not holding still.<sup>16</sup> Formerly cyberspace was conceived as just another domain for which military leaders had to plan deterrence and defense. But cyberspace has the potential to evolve into the master narrative of military-strategic behavior by default: the history of military-technical revolutions in the United States is rich with illustrations of techno-fixation triumphing over strategy. The nexus among policy, strategy, and military operations (ends, ways, and means) is vulnerable to disruption at both ends of the “strategy bridge” as Colin Gray has described it.<sup>17</sup>

## **Conclusion**

The Trump administration *NPR* offers proposals and perspectives that require careful consideration by the US national security community. It is more evolutionary than revolutionary in recognizing the need to recapitalize the nuclear force and to rethink the need for flexible nuclear responses in a changing security environment. However, the implications for nuclear arms control are mixed. While the overall size of the

US nuclear force may not change very much, the quality of the force and its supporting command and control systems must pass newer stress tests between now and 2046 when modernization plans are fulfilled. The role of nuclear employment policies in deterring escalation in limited war remains problematic and begs the question: Are we headed for a lower threshold between conventional war fighting and nuclear first use in Europe or Asia? If so, plans for nuclear deterrence and arms control must fit within a policy-strategy-operations continuum that recognizes the uniqueness of nuclear dangers and the need for strategic discipline in deterrence and arms control. **SSQ**

**Stephen J. Cimbala\***

*Pennsylvania State University—Brandywine*

#### Notes

\*Grateful acknowledgment is made to Paul Bracken and Paul Davis for comments on an earlier draft. They are not responsible for any arguments or opinions in this study.

1. Office of the Secretary of Defense (OSD), *Nuclear Posture Review (NPR)* (Washington, DC: Department of Defense, February 2018), <https://www.defense.gov/News/SpecialReports/2018NuclearPostureReview.aspx>. For analysis and commentary, see Lawrence J. Korb, “Why Congress Should Refuse to Fund the NPR’s New Nuclear Weapons,” *Bulletin of the Atomic Scientists*, 7 February 2018, <https://thebulletin.org/commentary/why-congress-should-refuse-fund-npr%E2%80%99s-new-nuclear-weapons11493>; David E. Sanger and William J. Broad, “To Counter Russia, U.S. Signals Nuclear Arms Are Back in a Big Way,” *New York Times*, 5 February 2018, <https://www.nytimes.com/2018/02/04/us/politics/trump-nuclear-russia.html>; Hans M. Kristensen, “The Nuclear Posture Review and the U.S. Nuclear Arsenal,” *Bulletin of the Atomic Scientists*, 2 February 2018, <https://thebulletin.org/commentary/nuclear-posture-review-and-us-nuclear-arsenal11484>; Hans Rühle, “The New US Nuclear Posture Review: Return to Realism,” *National Institute for Public Policy*, no. 427, 7 February 2018, <http://www.nipp.org/2018/02/07/ruhle-hans-the-new-us-nuclear-posture-review-return-to-realism/>; Sanger and Broad, “Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms,” *New York Times*, 16 January 2018, <https://www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html>; Michael R. Gordon, “U.S. Plans New Nuclear Weapons: Pentagon Weighs ‘Low-Yield’ Warhead and Sea-Based Cruise Missile, Igniting Debate over Strategy,” *Wall Street Journal*, 16 January 2018, <https://www.wsj.com/articles/u-s-plans-new-nuclear-weapons-1516063059>; and Richard Burt and John Wolfsthal, “America and Russia May Find Themselves in a Nuclear Arms Race Once Again: Despite the Trump Administration’s Decision to Treat It as an Afterthought, Arms Control



*The Trump Nuclear Posture Review: Three Issues, Nine Implications*

Is Not Dead,” *National Interest*, 17 January 2018, <http://nationalinterest.org/feature/america-russia-may-find-themselves-nuclear-arms-race-once-24100>.

2. Low-yield SLBM warheads and a modern nuclear-armed SLCM are discussed in the *Executive Summary* of OSD’s *Nuclear Posture Review*, 8, <https://media.defense.gov/2018/Feb/02/2001872877/1-1/1/EXECUTIVE-SUMMARY.PDF>. On the possibility of using nuclear SLCMs as a bargaining chip, see RadioFreeEurope/RadioLiberty, “M Mattis: Proposed U.S. Cruise Missile a Bargaining Chip with Russia,” 6 February 2018, <https://www.rferl.org/a/russia-mattis-cruise-missile-bargaining-chip/29023940.html>.

3. Korb, “Why Congress Should Refuse.”

4. Expert commentary on this aspect of the *NPR* includes Ruhle, “The New U.S. Nuclear Posture Review: Return to Realism,” 2. Challenges to US defense and other vital networks and IT capabilities are examined in the final report of the Defense Science Board Task Force on Resilient Military Systems, *Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, January 2013), <http://www.dtic.mil/dtic/tr/fulltext/u2/a569975.pdf>.

5. See Keith B. Payne, “Nuclear Deterrence in a New Age,” National Institute for Public Policy, Information Series no. 426, 13 December 2017, <http://www.nipp.org/2017/12/13/payne-keith-b-nuclear-deterrence-in-a-new-age/>. Other experts warn that nuclear weapons have been used with greater success in support of deterrence, compared to lesser effectiveness in support of coercion or coercive diplomacy. See Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (Cambridge, UK: Cambridge University Press, 2017).

6. OSD, *NPR Executive Summary*, 8.

7. For the text, see European Union External Action Service (EEAS), *Joint Comprehensive Plan of Action* (Vienna, Austria: EEAS Strategic Communications Division, 14 July 2015), [https://eeas.europa.eu/headquarters/headquarters-homepage/8710/joint-comprehensive-plan-action\\_en](https://eeas.europa.eu/headquarters/headquarters-homepage/8710/joint-comprehensive-plan-action_en). See also Lawrence Korb and Katherine Blakeley, “This Deal Puts the Nuclear Genie Back in the Bottle,” *Bulletin of the Atomic Scientists*, Expert Commentary, 15 July 2015, <http://thebulletin.org/experts-assess-iran-agreement-20158507>.

8. Jon B. Wolfsthal, Jeffrey Lewis, and Marc Quint, *The Trillion Dollar Nuclear Triad: US Strategic Nuclear Modernization over the Next Thirty Years* (Monterey, CA: James Martin Center for Nonproliferation Studies, January 2014), [http://cns.miis.edu/opapers/pdfs/140107\\_trillion\\_dollar\\_nuclear\\_triad.pdf](http://cns.miis.edu/opapers/pdfs/140107_trillion_dollar_nuclear_triad.pdf).

9. OSD, *NPR Executive Summary*, 6.

10. OSD, 6.

11. OSD, 6.

12. For example, see Darius E. Watson, “Rethinking the US Nuclear Triad,” *Strategic Studies Quarterly* 11, no. 4 (Winter 2017): 134–50, [http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11\\_Issue-4/Watson.pdf](http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-4/Watson.pdf). Cost projections for alternative US nuclear force structures are discussed in US Congressional Budget Office, *Approaches for Managing the Costs of U.S. Nuclear Forces, 2017–2046* (Washington, DC: Congressional Budget Office, October 2017), 15–20.

13. On this issue, see Jeffrey Edmonds, “How America Could Accidentally Push Russia into a Nuclear War,” *National Interest*, 6 February 2018, <http://nationalinterest.org/feature/how-america-could-accidentally-push-russia-nuclear-war-24378>; and Ernest J. Moniz, “Global Nuclear Risks,” 11 January 2018, transcript, Center for Strategic and International Studies, Washington, DC, <https://www.belfercenter.org/publication/ernest-j-moniz-addresses-global-nuclear-risks>.

14. See, for example, Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989); Jervis, *The Illogic of American Nuclear Strategy* (Ithaca, NY: Cornell University Press, 1984); and Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2008).

15. See Andrew Futter, “The Double-Edged Sword: US Nuclear Command and Control Modernization,” *Bulletin of the Atomic Scientists* (29 June 2016), <http://thebulletin.org/double-edged-sword-us-nuclear-command-and-control-modernization.html>; and Futter, *Cyber Threats and Nuclear Weapons: New Questions for Command and Control, Security and Strategy* (London: Royal United Service Institute for Defence and Security Studies, RUSI Occasional Paper, July 2016).

16. Pertinent discussion appears in P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), and in Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012).

17. Colin S. Gray, *The Strategy Bridge: Theory for Practice* (New York: Oxford University Press, 2010), 24–43.

# Attribution and Operational Art: Implications for Competing in Time

*Lt Col Garry S. Floyd Jr., USAF*

## Abstract

The world is wired with networks and unblinking sensors that track everything from spending habits to the movements of armies. Yet, despite the proliferation of data, attribution remains an enduring problem. A plane crashes into a building. A nuclear physicist dies under mysterious circumstances. So-called fake news spreads disinformation across social media on the eve of an election. These things happen and too often the world is left with questions about who to hold accountable. Decision makers need a way to assess attribution problems caused by adversaries, while also identifying and understanding opportunities when they hold and might utilize an attribution advantage. This article offers a model that visualizes attribution decisions and their associated risks at the operational and strategic echelons of command. The model is tested across three mini-case studies. What emerges in the analysis is a novel approach planners can use in considering covert operations, an approach that better accounts for the attribution problems inherent to operations in the cyber domain. The results of the analysis further suggest that properly leveraging attribution advantage creates opportunities for controlling the timing and tempo of military operations. Finally, this article presents several recommendations about how attribution advantage can be pursued at lower echelons in multi-domain operations that may offer some defense against attribution problems imposed by adversaries.



---

Lt Col Garry S. Floyd Jr. currently serves on the Algorithmic Warfare Cross Functional Team within the Office of the Undersecretary of Defense for Intelligence. He is a career intelligence officer and former intelligence squadron commander. Floyd holds several masters degrees, including international relations (Troy University), military art and science (US Army School of Advanced Military Studies), and most recently, strategy and technology integration (Air University).

During a keynote speech to the Air Force Association in September 2016, Air Force Chief of Staff Gen David Goldfein described his vision of the future of warfare as the intersection of an effects grid, a sensing grid, and multi-domain command and control. He further stated that “if you take a look at the effects grid, you have to create effects that are attributable, or not attributable. Sometimes I want them to know it’s me, sometimes I don’t.”<sup>1</sup> General Goldfein offers a compelling perspective on the nature of modern and future war. Yet when one considers airpower and the US Air Force the images that most likely come to mind are those of a fighter pilot straining against gravity through difficult maneuvers or a bomber crew tirelessly flying long-range strike missions across the globe. Why, then, did the senior ranking general in the world’s most powerful air force make reference to “non-attributable combat capabilities and effects?

The answer lies in understanding the role that attribution might play in operational art, and specifically, how attribution can help one side gain an advantage in the dimension of time. Attribution is defined here as the act of “ascribing agency to an agent.”<sup>2</sup> Whenever anything terribly bad or wonderful and good happens human nature demands an answer about whom to hold responsible, whom to reward, or whom to punish.

In operational art, attribution can be a tool well suited to the task of dominating the dimension of time. Time refers to that human-made construct that influences nearly every aspect of society by measuring the relationship between events. Seeking advantage in the dimension of time can be defined as diplomatic and military efforts designed to influence or disrupt decision cycles of opponents to gain more time or control the timing of events. Military theorist John Boyd envisioned weapons and operational concepts that could “simultaneously compress” time for one side while stretching it out for the other to “generate a favorable mismatch in time (and) the ability to shape (an environment) and adapt to change.”<sup>3</sup> So where is the crossroad of attribution, Boyd’s pursuit of advantage in time, and an emerging focus on military operations across multiple domains?

The promise and prominence of war fighting in the cyber domain is one part of the answer, but there is a broader context, also reflected in General Goldfein’s message, that speaks to the enduring nature of war. Despite every attempt to thwart them with technology, the basic elemental forces of war—uncertainty, friction, and chance—still loom over the battlefield, menacing even the best laid plans. With proper

planning and execution, non-attributable effects are possible in every war-fighting domain. There is diversity in non-attributable effects. It can be cognitive, logical, or physical in nature. In this sense, non-attributable effects might include covert aerial drone strikes, difficult-to-trace offensive cyberattacks, special operations forces operating deep in another country, or information attacks designed to undermine rival governments.

Attribution advantage occurs when one party in a conflict creates a military effect and then intentionally and successfully exercises influence over the detection and attribution of that effect while thwarting similar efforts from adversaries. This article first explores the cognitive terrain where uncertainty thrives despite increasingly persistent intelligence sensors. Next, it briefly reviews existing military doctrine on deception and considers the relationship between deception and attribution. Then the article offers a model that provides a method for evaluating when nonattributed effects should be pursued, when self-attribution might prove beneficial, and the implications for both. Self-attribution in this context occurs when a party takes credit, or perhaps blame, for an action that they may or may not have taken. The potential utility of the model offered in this paper is evaluated in three mini-case studies as notional examples: Putin's invasion of Crimea, US support for the Afghan mujahideen during the Soviet occupation of Afghanistan, and the dramatic events surrounding the Sony Pictures hack. What emerges is that attribution advantage—for those who can gain it—offers opportunities in the contest for time, but not without serious implications that must be considered and accounted for in planning. Boyd sought to “collapse (an) adversary's system into confusion and disorder by causing him to over- and underreact to activity that appears simultaneously menacing as well as ambiguous, chaotic, and misleading.”<sup>4</sup> The concept of attribution advantage supports those aims.

### **Attribution and the Cognitive Domain**

Attribution problems are rooted in the cognitive domain, that space in the minds of commanders where facts and fears contest for decision. While many scholars, observers, and practitioners have attempted to frame the immense cognitive challenges of war, none have done so with more impact than Carl von Clausewitz. Uncertainty and friction dominate in Clausewitz's depiction of war, looming insidiously to varying

degrees behind nearly every decision in the prosecution of campaigns and battles. While Clausewitz never uses the phrase “cognitive domain,” his words describe its nature. He wrote that “war has a way of masking the stage with scenery crudely daubed with fearsome apparitions” and that the “difficulty of *accurate recognition* constitutes one of the most serious sources of friction in war, by making things appear entirely different from what one had expected.”<sup>5</sup> Clausewitz further elaborated about how new information tends to “trickle” in to the commander, making him “more, not less uncertain.”<sup>6</sup> The stark reality of war in terms of the effects created by friction, uncertainty, fear, chance, and danger is precisely what makes attribution advantage so compelling.

Attribution advantage suggests that both strategic-level decision makers and operational-level commanders should give thought to attributing combat effects in multi-domain operations. There may be situations in which operational benefit might be had in purposeful self-attribution. Scenarios in which self-attribution causes adversaries to question entire information streams or data sources are one example. This might involve informing an adversary that their weather radars are no longer providing accurate storm tracking or that the facilities where they store fuel are no longer accurately measuring the amounts on hand. Informing an adversary that their command systems data is being tampered with may cause that adversary to lose trust in an information conduit or a source. A most likely and immediate result of doing so is that the adversary’s decision processes will suddenly take longer as the adversary attempts to find decision data they can trust. Longer decision cycles expose the adversary to additional intelligence collection efforts and potentially enhance kinetic targeting. While self-attribution might mean sacrificing a capability, advantages in time can be found by surprising the enemy.

Clausewitz and Boyd frame war as a daunting mental endeavor given its violence and the consequences of failure. Perhaps the minds of decision makers may soon prove even more vulnerable to manipulation as an emerging conditions of warfare. The internet, by its very nature, aside from providing an effective conduit for non-attributable effects, may be magnifying decision makers’ susceptibility to cognitive manipulation. Nicholas Carr takes on the task of understanding the internet’s influence on mankind’s collective ability to think critically in *The Shallows: What the Internet Is Doing to Our Brains*. Carr describes the internet as “an interruption system,” and his findings suggest that the

internet is making it both practically and physiologically more difficult for humans to think deeply about problems.<sup>7</sup> This does not bode well for the human species writ large, much less the military commander. Daniel Kahneman, in *Thinking, Fast and Slow* and in numerous other publications, has explained the myriad number of ways in which the human mind is already primed to reach incorrect conclusions from hastily assimilated data.

Kahneman challenges the notion that actors in a political or economic arena behave rationally and therefore predictably by unveiling a litany of shortcomings and biases. He does this by describing human thinking as happening in two separate and distinct systems. The first he dubs “System 1” thinking that “operates automatically and quickly,” which is opposite from “System 2” thinking that is more deliberate and useful in complex situations.<sup>8</sup> Kahneman demonstrates that human failings are often the result of heuristic processes employed in System 1 thinking to reach expedient solutions. Indeed, he offers an entire lexicon of heuristic practices that can lead to cognitive inspired failings. One particularly powerful idea is his WYSIATI concept, an acronym for What You See is All There Is.<sup>9</sup> Kahneman asserts that in System 1 thinking, “the measure of success is the coherence of the story it manages to create. The amount and quality of the data on which the story is based is largely irrelevant.”<sup>10</sup> When the battlefield is the mind of an enemy commander, System 1 and System 2 thinking become new avenues of approach in key terrain.

Indeed, taken together, Kahneman and Carr’s portrait of the cognitive domain suggests that the human mind is increasingly vulnerable to attack despite the digital assistants making their way into every modern home. The minds of decision makers are no less vulnerable, despite their assumed access to exquisite sources of intelligence. Non-attributable effects, or effects generated with the intent of eventual and purposeful self-attribution, magnify uncertainty. An operational objective might be to maximize uncertainty to push adversary decision makers from System 1 to System 2 thinking for the purpose of expanding decision time. Another line of operation might include covertly inserting data that blends in with the background data fueling the adversary’s shallow System 1 thinking. Still another method might involve finding ways to alter command signals moving from the headquarters to the field. Subordinates reserving their System 2 thinking for other tasks may prove vulnerable in cultures where questioning orders from higher echelons is not encouraged.

## **Attribution and Deception**

Vulnerabilities inherent within the cognitive domain suggest that the attribution problem has its basis in deception. Deception is prerequisite for attribution advantage whenever or wherever detection cannot be avoided. For example, perhaps one generates an effect that its adversary is not only unaware of but remains unaware of until some critical moment when it discovers that a critical capability is suddenly impotent or providing inaccurate data. At that moment, when the adversary discovers an effect, subterfuge about who is responsible fuels attribution advantage and preserves flexibility for the aggressor. Another possibility is that the target is made aware of the effect by its adversary but not its author, and the proffered symptoms of the problem lead the target toward attributing the source of the problem to other causes. Machines, in fact, do sometimes break down and humans in the loop are always prone to error. The advantages an operational artist derives from these opportunities hinge upon deception. In many of these scenarios, where detection is rightly presumed to be only a matter of time, someone or something is always being lied to or misled. In those moments, the information streams upon which decisions are made are polluted and unsafe. When stealth enables a non-attributable effect, the adversary does not even know not to trust their systems, data, or processes for as long as detection is delayed.

Deception is fundamental to generating non-attributable effects. There is always some element of deception at work, even in those instances where the introduction of deceptive or false information is not the primary goal of the operation. While current joint doctrine on military deception does not directly address the pursuit of attribution advantage, it does provide guidance that seems applicable. There is an action element coded in joint military deception doctrine. The object of deception operations is not simply to mislead, but to force a desired outcome concerning the enemy. For example, US Department of Defense Joint Publication 3-13.4 defines military deception as actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.<sup>11</sup>

Achieving attribution advantage is a balance between positive and negative actions of both the party with initiative and the target of the



desired nonattributed attack. Positive actions mean “doing something” while negative actions refer to one side or the other “not doing something.” For the party with the initiative, positive actions involve building a strong case for plausible deniability or leaving behind clues in the wake of an operation that lead an adversary to misattribute the cause of the effect. Again, for the party with the initiative, negative actions eschew active misdirection in favor of efforts aimed to achieve stealth. Whichever approach the operational artist pursues, the goal is to cause the adversary to make a bad decision, a positive action, or to perhaps miss a critical opportunity through negative action or inaction.

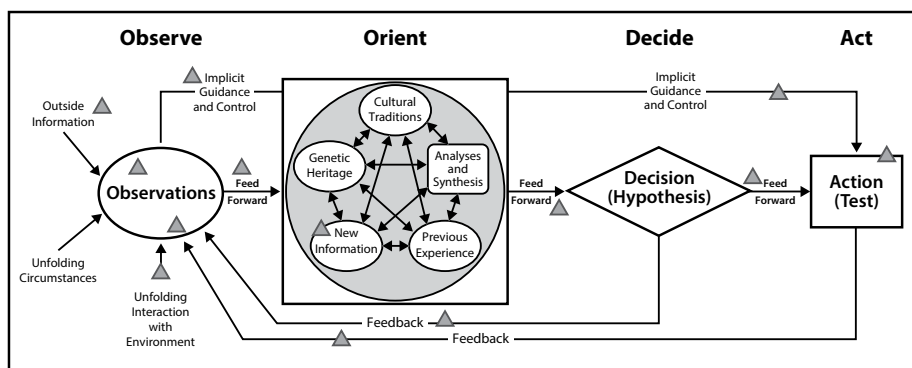
Joint doctrine explores the approaches to deception by introducing the concept of conduits to explain these various approaches. Conduits are defined as “information or intelligence gateways to the deception target. Conduits may be used to control flows of information to a deception target. It is rare that a deceptive message is sent directly to the deception target itself. Most often, deception messages are sent to intelligence collectors (conduits) with the expectation that the deceptive message will systematically make its way to the deception target.”<sup>12</sup>

While the concept of conduits seems sound and logical, joint doctrine seems to unnecessarily constrain the operational artist’s thinking. Indeed, in the near future, it may be common for actors with the initiative to send “deceptive messages” directly to decision makers. The question becomes one of just how directly and effectively that can be accomplished balanced against the perceived necessity for stealth and nonattribution.

However, it is worth noting that deception is a tool that is also available to defense. Eric Gartzke and John R. Lindsay point out that “if it is easy for a covert attacker to gain access to an organization’s data, it is also easy for a network protector to feed the attacker data that are useless, misleading, even harmful.”<sup>13</sup> If one considers attribution advantage as something to be won in the cognitive domain, and the contest between offensive and defensive efforts in deception, Boyd’s famous “OODA Loop” begins to look less like a theory about decision-making processes depicted in a wire diagram and more like a terrain map of targets in a contested battlespace.

Through the OODA Loop, Boyd explained basic decision making as observing, orienting, deciding, and acting upon information. SAF targeteers traditionally place red triangles on the targets upon

which they desire to create effects. If one places a few triangles on the OODA Loop it begins to look like a map of physical space or perhaps a campaign map for the cognitive battleground (see figure 1). The small triangles indicate targets for the aggressor or traps the defender leaves open to its attacker. The result is that attribution becomes a question to be answered in the synchronization of effects in multiple war-fighting domains, for all of the parties involved in the conflict.



**Figure 1. Boyd's final OODA-loop sketch.** (Adapted from Grant Tedrick Hammond, *The Mind of War: John Boyd and American Security* [Washington, DC: Smithsonian Institution Press, 2001], 190.)

## Operational Art and Attribution Advantage

Clausewitz described the atmosphere and the challenges inherent with the cognitive domain. However, Sun Tzu's guidance from over 2,000 years ago may be more relevant to the operational art of attribution advantage. Sun Tzu wrote, "War is the art of deceit. Therefore, when able, seem unable; when ready, seem unready; when nearby, seem far away; and when far away, seem near . . . if [your opponent] is humble, encourage his arrogance . . . if he is internally harmonious, sow divisiveness in his ranks. Attack where he is not prepared; go by way of places where it would never occur to him you would go."<sup>14</sup>

Sun Tzu's contribution to military thinking and strategy is the art and practice of indirect warfare. Winning without fighting still means winning. The terms by which the desired result is achieved are simply different. The mindset that accompanies indirect warfare is useful in considering warfare in the cognitive domain and the exploitation of attribution advantage.

Boyd drew some important distinctions between the approaches taken by Clausewitz and Sun Tzu to warfare in the cognitive domain. He suggested that Clausewitz “failed to address the idea of magnifying an adversary’s friction and uncertainty.”<sup>15</sup> Further, Boyd’s understanding of Sun Tzu is that commanders should seek opportunities to “shape the enemy’s perception of the world to manipulate his plans and actions.”<sup>16</sup> That understanding is reflected in Joint Publication 3-13.4 in that the purpose of deception operations should be to cause the enemy to either do or not do something tangible, rather than simply to make the enemy think something. Considering the pursuit of attribution advantage as a cognitive avenue of approach suggests an indirect method for setting conditions for the conflict, such as the timing and location.

To pursue a nonattributed effect, or to self-attribute an effect previously undetected or unattributed by an adversary, is to seize the initiative in the cognitive domain. The questions that now emerge turn upon operational utility, risk, planning, and execution. The answers may be found in the measures of effectiveness by which the risk and operational utility of attribution advantage might be assessed. Defining those measures of effectiveness can be thought of as establishing the questions decision makers and planners should ask prior to execution. Some of these questions include:

**How much damage will this attack cause to the targeted system?**

The question of damage is not trivial. The amount of damage done may correlate directly to the adversary’s response. Further, given the rise of social media, the impact of operations on public opinion is felt sooner, providing just-war traditions like proportionality with new strength.

**How long until the adversary detects something is wrong in the targeted system that is, how long before effects become visible or measureable?**

Regardless of the domain in which effects are created, detection of effects by an adversary starts the clock on the adversary’s response. In a seminal work on covert actions, Gregory Treverton wryly asserts that covert operations are always eventually discovered.<sup>17</sup> If taken as truth, delaying detection is the first order for the side with initiative. Preventing or delaying attribution becomes the challenge upon discovery.

### **What is the likelihood this operation might cause unintended damage?**

Some authoritarian regimes seem to have developed an immunity to the concept of collateral damage. However, for most, the question of unintended damage is crucial, particularly when nonattributed effects are the goal. The political consequences of severe collateral damage can only be magnified when they occur during the execution of a covert operation.

### **Is plausible deniability feasible?**

Recently the leader of a nuclear-armed nation was able to foster ambiguity and maintain a semblance of plausible deniability in an era of constant coverage by both the media and intelligence sensors. Further, disinformation branded as “fake news” seems to have given new life to an old concept. Plausible deniability places the burden of proof on the accuser. An intelligence service may have evidence of an offense committed by an actor, but whether policy makers can use that to publicly make their case without compromising sensitive sources and methods is always in question. Of course, plausible deniability is not necessarily an easy path for the would-be attacker. Joseph Nye points out that an “attacking government or non-state actor knows what its role was, but it cannot be sure how good the opposing forensics and intelligence are.”<sup>18</sup> Nye’s focus was on deterrence in cyberspace, but the statement stands for other covert actions as well.

### **What is the assessed ability to shape attribution toward another actor?**

The truism that perception is reality holds sway, and circumstantial evidence can be thought of as camouflage for the mischievous. When two parties are in conflict, it provides near perfect cover for a third party to skillfully exploit the situation, whatever the motivations. False-flag attacks, where assailants disguise themselves as another, should be expected.

### **How vulnerable are one’s own interests should a tool, asset, or operation be discovered?**

This is particularly relevant in the cyber domain. Before an elegant cyberattack is unleashed on some unsuspecting adversary, one should

first explore the possible implications if the weapon is discovered and then repackaged and redirected against its creators.

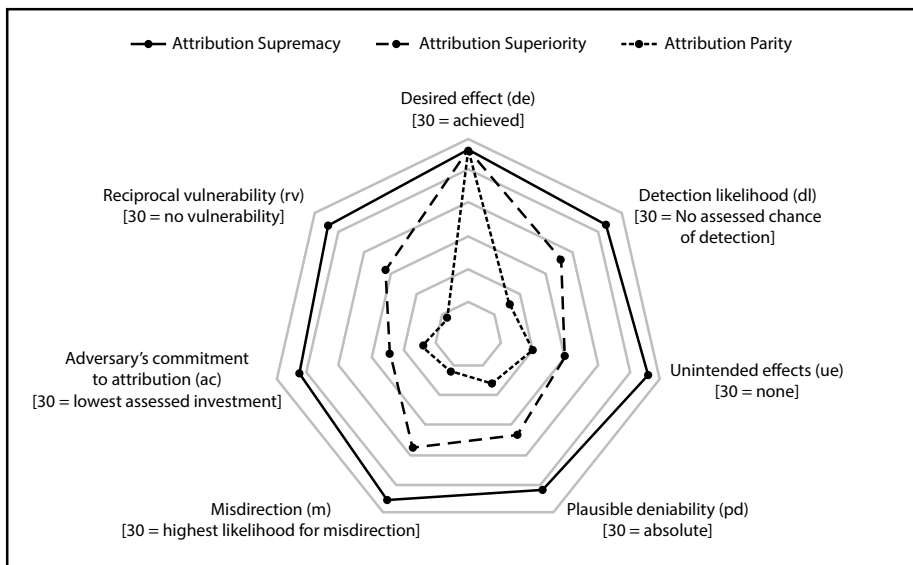
**What attribution resources might an adversary bring to bear once an effect is discovered?**

Some actors simply have more capabilities to apply against an attribution problem than others. However, an aggressor should always bear in mind that when something “new” is observed, whether in the physical or the digital realm, the discovery draws attention from those seeking either to understand it, counter it, or replicate what has been found.

### **Modeling Attribution**

The model represented by the spider chart in figure 2 is offered to address these questions by providing a graphical depiction of the operational utility and risks of weaponizing attribution under various conditions. The attribution advantage model provides seven vectors upon which to measure the merits of attribution. It provides a method for framing the opportunities and risks associated with pursuing nonattributed effects and whether one should self-attribute an effect or capability that might otherwise have remained stealthy. The model is meant to help an operational commander or decision leader better understand when they have an attribution advantage and guide their thinking about how and when they should use that advantage.

For the purpose of introducing the model, three conditions are set in figure 2, and in each the assumption is that the desired effect can be achieved with the highest possible confidence. In practice, scoring within the model will always be somewhat subjective, as scoring is necessarily based on the best available all-source intelligence on the adversary’s capabilities and situation, as well as one’s understanding of one’s own capabilities (see appendix for further discussion of scoring). Further, it is once again important to note that this model is not meant solely for the cyber domain. The model is intended as a means to analyze the attribution question across the range of covert capabilities, from cyberattacks to stealthy air strikes and special operations employment.



**Figure 2. The attribution advantage model**

Borrowing from airpower doctrinal terms, the highest tiered condition is “attribution supremacy.” Under conditions of attribution supremacy, the aggressor possesses a weapons platform, tool, or capability that achieves the desired effect with little chance of detection and little chance of causing unintended effects. In a scenario where attribution supremacy exists, the aggressor is highly certain of its ability to maintain plausible deniability, is confident that it can misdirect attribution toward another party or cause, and has taken steps to ensure that it is invulnerable to the attack it is about to unleash on its opponent. Further, the party with the initiative assesses that its target will dedicate minimal resources to discover attribution, either by choice or because of resource scarcity. In conditions of attribution supremacy, incentives for aggressors to conduct operations designed to produce non-attributable effects are very high. The party with initiative is also in position to control the timing of attribution. If decision makers and planners sense an advantage in self-attribution, they can do so given their limited vulnerability to a reciprocal attack and the lack of unintended consequences for which they might be held accountable. Finally, under conditions of attribution supremacy, the assailant is highly confident it can attribute attacks intended to be non-attributable delivered by its enemy or interested third parties. That confidence might stem from exquisite access to adversary

decision making or simply the ability to mass resources against attribution problems.

Sustained attribution supremacy may be difficult to maintain or even achieve. A more realistic objective for an aggressor might be “attribution superiority.” Plausible deniability and successful misdirection are achievable—but more temporary. The advantage of preventing one’s actions from being detected is more fleeting. Therefore accounting for the discovery of one’s actions is more prudent during operational planning. Further, under conditions of attribution superiority, the ability to remain undetected may prove localized, meaning the target might remain unaware of an attack, but other interested parties may prove able to gather and process data suggesting that something is afoot. When a third party detects an act or an attack that they assume the perpetrator wishes to remain secret, they face an important series of questions. Do they attribute the act publicly, spoiling the apparent, perhaps temporary attribution superiority the aggressor had enjoyed? Do they covertly confront the aggressor conducting the act in pursuit of some profit or political advantage? Do they covertly inform the aggrieved party, again for some profit or advantage? Or do they simply remain quiet, preserving the ability to detect and attribute until some greater benefit might be had?

However, many scenarios are likely to more closely resemble “attribution parity,” depicted in figure 2 by points plotted more toward the center of the graph. Risks abound under conditions of attribution parity. Perhaps the actor possesses a platform that is highly effective but is equally as vulnerable to the weapon, given the costs of preemployment inoculation or postattack remedy. Furthermore, under conditions of attribution parity, the development of a special capability might make it exquisitely complex and costly to produce. This might frustrate plausible deniability or technical efforts to misdirect attribution. Lindsay suggests “the increasing costs of attack against valuable targets [offer] some hope that strategies of denial can protect vital systems. The vulnerability of anonymous attackers to compromise in the most complex targets also offers some hope for deterrence strategies.”<sup>19</sup> Lindsay primarily focuses on the attribution problem in the cyber domain, but his statement holds true across domains. The employment of an exquisite capability limits the possible number of responsible actors, as high-value targets are often the most well defended.

Still another problem for the side seeking to go on the offensive under conditions of attribution parity are the unintended effects that a covert operation might have and the blowback that may result from discovery. Many reporters and scholars have focused on the Stuxnet computer worm, which comprised a highly sophisticated cyberattack that targeted Iran's nuclear facilities. If David Sanger's reporting is accurate, key US policy makers at the highest level did not demand assurances that the worm would not cause unintended damage until after it had begun spreading to unintended systems in cyberspace.<sup>20</sup> Unintended or collateral damage is no longer simply a concern for targeteers employing traditional bombs or cruise missiles.

The conditions found in attribution parity suggest the party attempting to seize the initiative has very little control over whether or not attribution occurs and may be vulnerable to an attack delivered via a similar platform. There is a high risk of detection, as the adversary is likely to invest significant resources to attribute the attack once the effect is discovered. Treverton puzzles over how decision makers seem to always believe that their covert operations will remain secret, despite ample evidence that suggests otherwise.<sup>21</sup> That said, if mitigation is available for the vulnerability problem, there may be scenarios at attribution parity where self-attribution should be considered as a means to control the narrative or to enhance one's future credibility for launching future attacks. Finally, attribution parity implies that one's adversary may be very capable of creating their own difficult-to-attribute effects. This creates conditions favorable to long, limited conflicts where the risk of sudden, uncontrolled conflict escalation is continually high.

### **Attribution Advantage in Practice: Putin, Ukraine, and Crimea**

Vladimir Putin's Russia seems to have an implicit understanding of the political risks and benefits of attribution. Since 2013, Russia has reportedly been involved in military interventions and linked to offensive cyber actions in Syria, the Baltic States, Georgia, and Ukraine. In 2014, British Broadcasting Corporation (BBC) News captured a dilemma shared by the news media, scholars, and other observers of military matters:

The internet has no shortage of photographs and videos showing armed men in Crimea who look like members of the Russian military. Their guns are the same as those used by the Russian army, their lorries have Russian number plates and they



speak in Russian accents. Yet according to President Vladimir Putin, they are in fact members of “self-defense groups” organized by the locals who bought all their uniforms and hardware in a shop. This poses a challenge to the media covering the crisis: what do you call people who are officially not there?<sup>22</sup>

Just short of a year later, BBC News reported that Putin, in a documentary made for Russia’s state-run news service, had admitted a military role in the annexation of Crimea well before Crimeans held a referendum on self-determination.<sup>23</sup> Certainly, Putin’s moves in Crimea and the timing of his pronouncements suggest grand strategic design and operational planning.

Mathew Kroenig suggests that Russia, in knowing that it would likely fail in a direct conventional conflict with the United States and its North Atlantic Treaty Organization (NATO) allies, must “use hybrid warfare to make its revisionist actions as subtle as possible, avoiding moves that would trigger an automatic, robust response.”<sup>24</sup> He describes the tools available to Russia via hybrid war thusly: (Russia) can use the pretext of protecting Russian nationals, ties to sympathetic elements within the victim country, propaganda campaigns, cyberattacks, irregular warfare including professorial soldiers in unmarked uniforms (the so-called little green men), and coercion through the massing of conventional forces on the border.<sup>25</sup> Kroenig and many others suggest that these were the tactics Russia employed in Georgia, eastern Ukraine, and Crimea. Further, creating and maintaining ambiguity is essential. Marcel Van Herpen, who has examined Russia’s brand of hybrid warfare, writes:

An integral part of this new kind of warfare is the “plausible deniability” of the implication of the aggressor nation’s soldiers, Spetsnaz, or secret services. This “plausible deniability” is supported by an “information war” that accompanies the hostilities and that has the objective to convince public opinion at home and abroad of the aggressor’s version of the facts.<sup>26</sup>

Contesting the cognitive domain through information warfare is a critical component of hybrid warfare. When an actor seemingly invests effort and resources into shaping public opinion for both domestic and foreign audiences it suggests it is attempting, at least to some extent, to avoid some undesirable outcome or cost. In other words, Russia’s actions in Crimea imply that Russia’s leadership was in some way uncertain or insecure about the possible backlash from foreign or domestic quarters. While that is likely true to some extent, by intentionally fostering the appearance of ambiguity Russia provided an escalation “off-ramp” for its

adversaries. Ambiguity is useful to those playing for more time when the costs of direct intervention or further escalation seem too high.

While current analysis benefits from hindsight, the notional example attribution advantage model in figure 3 frames some of the attribution considerations for Russia's actions in Crimea. The specific values offered in this model and the others offered in this paper, though informed by available open-source information, are notionally assigned and intended to explore the terms and framework of the overall model (see appendix for more details on the author's scoring). That said, desired effect (*de*) and reciprocal vulnerability (*rv*), are notionally and subjectively rated here at 21 and 23 of 30 possible points. One cannot know whether Russian planners could have forecasted similar scores before the operation, but it seems feasible. Assuming the desired effect was a change in Crimea's political status, putting troops on the ground proved effective. Further, aside from possible reciprocal actions in cyberspace, Russia appears to have been relatively invulnerable to a Ukrainian response.

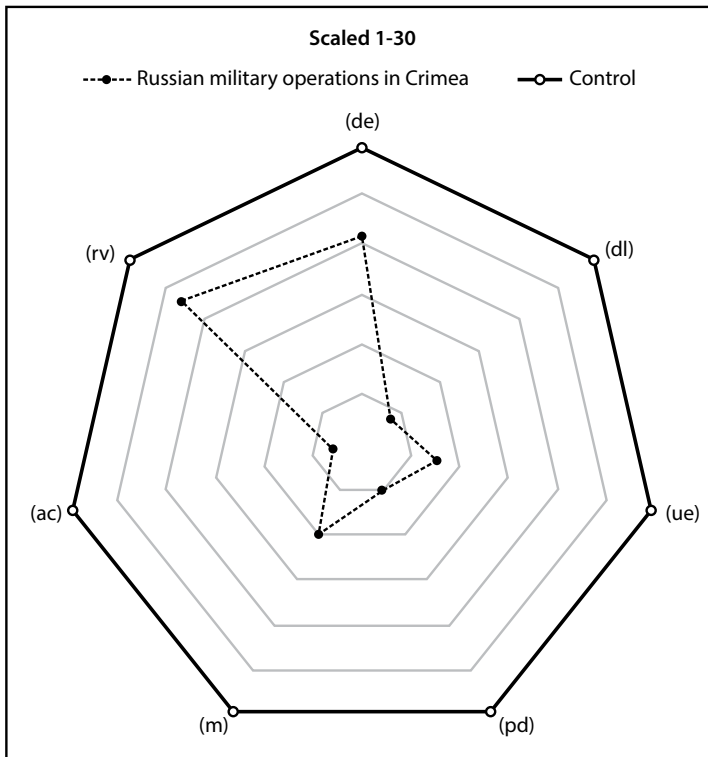


Figure 3. Attribution advantage in Crimea

However, as noted in the constriction in the curve, strategic and operational risk increases greatly across the remaining axes. Given the reasonable assessment that Ukraine would invest heavily to attribute an alleged violation of its sovereignty, the adversary's commitment (*ac*) moves close to center, a notional score of 3. The expected intense focus from both Western intelligence services and media coverage further suggest that misdirection (*m*) and plausible deniability (*pd*) values would also demonstrate high levels of operational risk, hence their notional scores of 5 and 10. Russia did reportedly experience unintended effects (*ue*) as a result of its overall operations in Crimea and Ukraine, and the score of 8 here that a planner might have forecasted may be generous. Perhaps the most notable example included the shoot-down of a Malaysian jet airliner, which resulted in 298 civilian deaths.<sup>27</sup> Despite Russian denials, numerous sources, including Ukraine, held Moscow responsible for the incident. Finally, given the situation on the ground, the success of misdirection (*m*) efforts seems to have been limited, despite Moscow's efforts to divert responsibility for the airline crash and other violations to other causes. Overall, this example model suggests that Russia's actions in Crimea were risky on a number of fronts and that ambiguity could never have been sustained for very long. However, given Russian forces' proximity to the operations area, Putin did not need much time. Whether Putin's opponents leveraged attribution problems and the appearance of ambiguity as a political cover for doing relatively nothing over that short span of time is another question.

### **Attribution Advantage in Practice: The Soviet Invasion of Afghanistan**

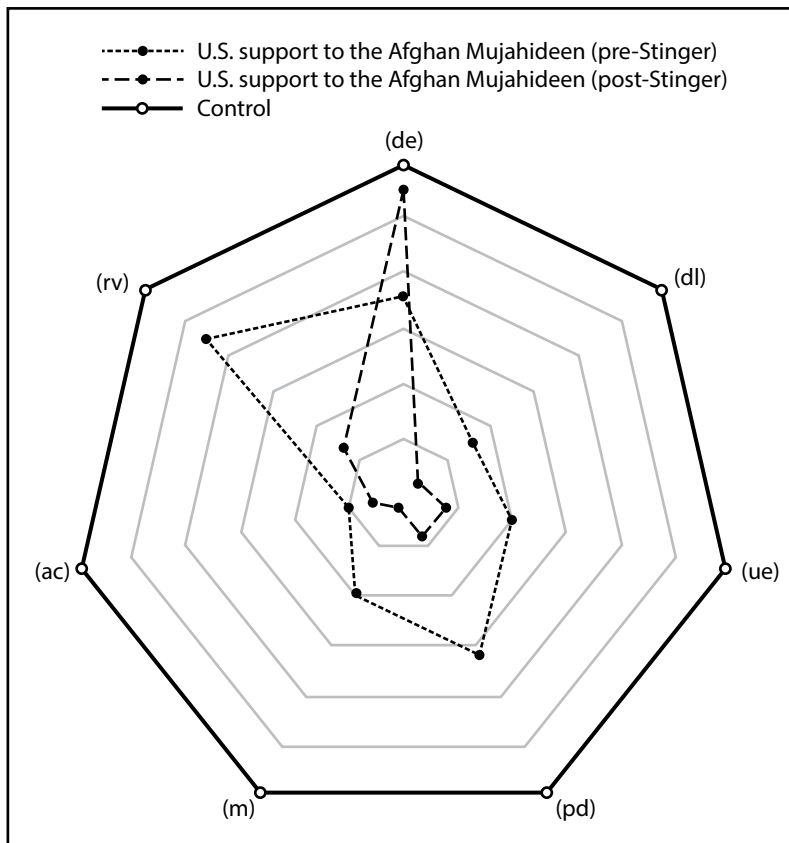
The United States has frequently leveraged attribution to conduct covert operations. America's support to the Afghan mujahideen following the Soviet Union's invasion of Afghanistan remains one of the largest known covert operations in history, and it provides a useful example of weaponized attribution. In George Crile's account of the Central Intelligence Agency's (CIA) support to the mujahideen, plausible deniability seems to underlie every major decision. Crile describes how Charlie Wilson, a congressman from Texas, played a major role in helping, and sometimes forcing, the CIA to leverage the United States Congress's power of the purse to provide the mujahideen with the weapons they needed to fight the Soviet occupation. Plausible deniability was a constant necessity.<sup>28</sup> Crile states there was an "implicit understanding in Afghanistan" that the

“United States would not taunt the Soviets with an overt demonstration of involvement.”<sup>29</sup> Policy makers and intelligence analysts determined that maintaining plausible deniability was necessary because they feared that in its absence, the conflict might escalate beyond the borders of Afghanistan.

Both Crile and Treverton make it clear that Pakistan’s fear of a Soviet invasion drove the need for subterfuge.<sup>30</sup> Pakistan’s leaders walked a tight-rope amidst a backdrop that has become all too familiar. Refugees were pouring out of Afghanistan; creating the conditions necessary for their return meant aiding them in their fight against the Soviets. However, if those aid efforts went too far, the Soviets might retaliate. Pakistan’s president frequently told foreign diplomats and military personnel “we must make the pot boil for the Russians but not so much that it boils over into Pakistan.”<sup>31</sup> Facing a perennial threat from India, Pakistan could ill afford a second front with the Soviets.

The attribution advantage model helps explain attribution’s role in the shifting nature of the risks the Americans and Pakistanis faced over time. Crile’s account makes it clear that the Soviets enjoyed an asymmetric advantage over the mujahideen in the form of the Mi-24 “Hind” attack helicopter. The Hind was an armed killer, and the mujahideen stood little to no chance of success when a Hind appeared over battlefield. The question of what to do to help the mujahideen against the helicopters consumed Wilson and others. According to Crile, the CIA worked to ensure that any weapons provided to the mujahideen would appear as Soviet in origin.<sup>32</sup> The answer to the Hind problem lay in providing the mujahideen with a portable surface-to-air missile that could shoot down the helicopters. Crile writes that as late as the fall of 1985 those familiar with the problem knew the Stinger “was the best mule-portable plane killer in the world...but...the CIA was adamant about not introducing the American weapon. Putting in the Stinger would have been like advertising the CIA’s involvement in the war in Red Square.”<sup>33</sup> However, after a policy review, and facing the realization that plausible deniability was all but untenable given that “over three quarters of a billion dollars annually” was then flowing to the mujahideen, the CIA relented and the Stinger entered the fight.<sup>34</sup> The Stinger decision provides a benchmark for studying how the role of plausible deniability and attribution evolved over time.

The example model in figure 4 depicts the risks involved for the United States and Pakistan both prior to and after the introduction of the Stinger. By all accounts the Stinger made a significant impact in favor of the mujahideen. As the CIA understood, Russian detection rose and plausible deniability evaporated with the Stinger's arrival, hence the significant difference in their scoring. Unintended effects were a matter of great concern, and notionally score low in both scenarios at 10 pre-Stinger and 4 after. Crile writes that prior to 1986 "the idea of a Khomeini loyalist shooting down a TWA flight with a General Dynamics Stinger was too much" given the difficulty of controlling whose hands the missiles ended up in.<sup>35</sup> That concern suggests a higher than preferred level of reciprocal vulnerability (notional scores of 23 and 7). That the Soviets would dedicate significant resources to understanding the origin of the new threat killing its helicopters was a given.



**Figure 4. US attribution advantage during the Soviet invasion of Afghanistan**

With hindsight emerges an additional unintended consequence, perhaps unfathomable to decision makers at the time. To maintain plausible deniability, American military aid to the mujahideen flowed through Pakistan. Crile contends that the Afghans “had no idea” their mules were loaded down with weapons paid for by American taxpayers, suggesting that to them, the weapons were “gifts from Allah” or perhaps Pakistan.<sup>36</sup> In his epilogue, Crile reflects deeply on the chain of events that connect the Soviet withdrawal from Afghanistan to the 11 September 2001 terrorist attacks. Crile does not frame the point explicitly, but one is left to wonder what impact a different approach to attribution taken early in the conflict might have had across the years that followed.

This example clearly reflects that time was an important factor in the context of the CIA’s covert support. Early on the CIA planners wanted to raise the costs for Russia for as long as they could. They were unsure how long their mujahideen proxies could stand up to Russia’s superior firepower. Once the Afghans proved their resilience the CIA’s support grew to the point where attribution became more likely. That increased risk is evident in the model given how the points collapse in toward the center. However, by the time the Stingers were introduced to the battle space, the risk of Russian retaliation against Pakistan had become less of a concern.

### **Attribution Advantage in Practice: North Korea Goes Offline**

December 2014 should be remembered as an important moment in the history of cyberwarfare. Controversy arose over a movie, whose unlikely plot revolved around a CIA attempt to assassinate North Korean dictator Kim Jong-un. The North Koreans were not amused. According to the BBC, as early as June 2014 a spokesman on North Korea’s state-run news agency declared, “Making and releasing a movie on a plot to hurt our top-level leadership is the most blatant act of terrorism and war and will absolutely not be tolerated. . . . If the US administration allows and defends the showing of the film, a merciless counter-measure will be taken.”<sup>37</sup>

Press reports from North Korea often seem rather hyperbolic and bellicose when focused on the United States. However, by the following November, Sony Pictures, the company responsible for *The Interview*, found itself to be the target of a crippling cyberattack. Sony’s networks experienced severe outages, the salaries and social security numbers for thousands of

employees were made public, and several unreleased movies leaked to the public.

North Korea publicly supported the hack but denied a direct role, suggesting that North Korean “supporters” and “sympathizers” around the world were likely responsible.<sup>38</sup> The saga did not stop there, even as Sony delayed release of the movie over terror threats to movie theaters. In mid-December, following Sony’s delayed release, Kim Zetter, an internet security reporter for *Wired.com*, wrote:

In the service of unraveling the attribution mess, we examined the known evidence for and against North Korea . . . . We have to say that attribution in breaches is difficult. Assertions about who is behind any attack should be treated with a hefty dose of skepticism. Skilled hackers use proxy machines and false IP addresses to cover their tracks or plant false clues inside their malware to throw investigators off their trail. When hackers are identified and apprehended, it’s generally because they’ve made mistakes or because a cohort got arrested and turned informant.<sup>39</sup>

Given the stated difficulties of cyber attribution, Zetter and her team at *Wired.com* concluded that the available evidence against North Korea was thin and circumstantial.<sup>40</sup> Of note, two years later Fred Kaplan stated in his book *Dark Territory: The Secret History of Cyber War* that the National Security Agency “had long ago penetrated North Korea’s networks: anything that its hackers did, the NSA could follow.”<sup>41</sup> Still, the entire episode frames the difficult issue of cyber attribution—but the story does not end there.

Just days after Zetter’s analysis in *Wired.com*, someone or something severed North Korea’s extremely limited connection to the internet.<sup>42</sup> According to Kaplan and his sources:

The United States government played no part in the shutdown. A debate broke out in the White House over whether to deny the charge publicly. Some argued that it might be good to clarify what a proportional response was not. Others argued that making any statement would set an awkward precedent: if U.S. officials issued a denial now, then they’d also have to issue a denial the next time a digital calamity occurred during a confrontation; otherwise everyone would infer that America did launch that attack, whether or not it actually had, at which point the victim might fire back.<sup>43</sup>

It is worth noting that at least one group reported evidence and published analysis suggesting that North Korea’s loss of its internet connectivity was due to a distributed denial of service attack and that a hacktivist group was likely involved.<sup>44</sup> Still, the dilemma for US policy

makers in similar situations remains. Time is a valuable commodity in a place like Washington, DC, where the next election, congressional recess, or holiday is always looming. Time spent debating a response to accusations is time not spent advancing other agendas. Thus, in the cyber domain, when someone else seizes attribution advantage, the effect on decision cycles in terms of debating response options is very real.

As in the earlier scenarios, the attribution advantage model (see figure 5) is intended to help planners and decision makers ask good questions about these respective operations. The assessments represented by the graph are intended as examples, though they are somewhat informed through the benefit of hindsight and open-source information. At the very least, those capable of carrying out operations such as these should be able to make an assessment in response to the questions posed in the model. Of note, the following analysis assumes that someone intentionally took down North Korea's internet, meaning human or mechanical error was not to blame, although that still remains possible.

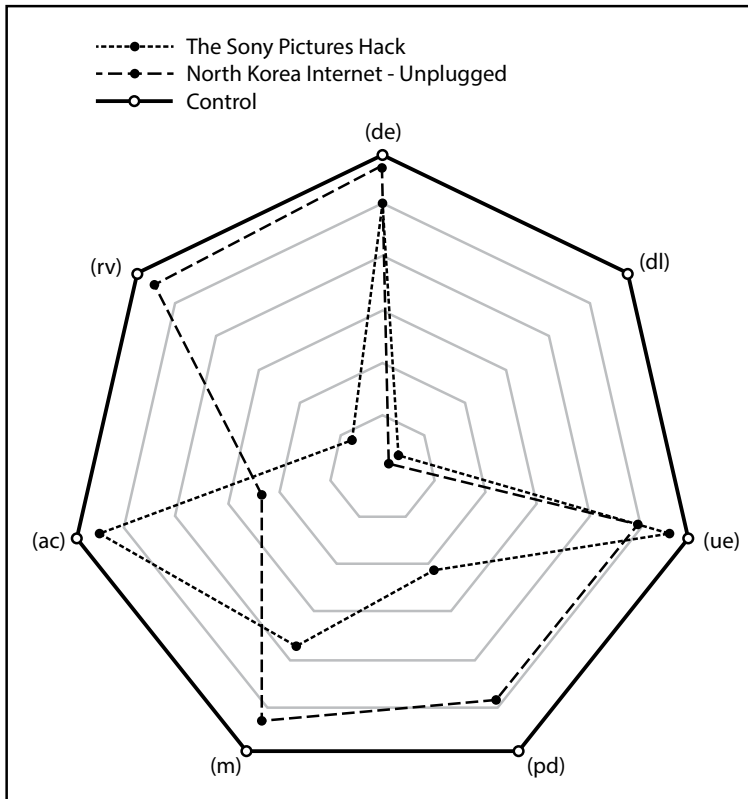


Figure 5. North Korea cyberwarfare, 2014



Clearly both attacks should score highly in terms of desired effect. This model assesses their notional score at 28 and 30 on the 30-point scale. North Korea's internet infrastructure, by all accounts, is made vulnerable by its small scale. While the Sony Pictures hack proved highly effective, in both cases the perpetrators likely had a reasonable expectation that they could achieve their desired effects. Of course, the perpetrators should not have had any expectation of their attack going undetected given the nature of the attacks. The model assesses a detection likelihood score of close to zero. These attacks were fundamentally different than other famous attacks. Stuxnet, the cyberattack against Iran's uranium centrifuges, likely provides a better example of an attack in which stealth was pursued. In fact, stealth was central to the worm's trust-exploiting design. Of Stuxnet, cyber experts Singer and Friedman write, "the most insidious part [is] . . . it was an integrity attack par excellence. Stuxnet didn't just corrupt the process, it hid its effects from the operators and exploited their trust that the computer systems would accurately and honestly describe what was taking place."<sup>45</sup>

Stealth, in terms of the target not knowing anything was happening, was not a requirement in the Sony hack or the attack that severed North Korea's internet. When Sony's users logged onto their machines in the early stages of the attack they were greeted by skulls on their monitor accompanied by a message that they had been hacked.<sup>46</sup> One can assume Kim Jong-un quickly discovered that his internet connection had been severed. Stuxnet provides a good example of an effect created to put more time on the clock for other political actions.

Unintended effects are more difficult to judge in this case based on the available open-source information, but logic suggests the chances of unintended effects were low, notionally scoring 26 for the Sony hack and 23 for North Korea going unplugged. If the assailants that severed North Korea's internet connection had only intended to bring down one website, for example Korea's state-run news agency, then they overreached in their attack. This seems unlikely given the aforementioned evidence that a denial of service attack brought down North Korea's internet. The "smash and grab" nature of the Sony hack leaves little room for consideration of unintended effects.

Plausible deniability and misdirection seemingly discover high scores on the graph. The model in figure 5 rates their possible values at 25 and 19 respectively. Kaplan attributed the Sony hack to North Korea, but

only with the apparent hindsight benefit of a source that may have had access to classified US government information. Attribution seemed far less certain for Zetter at *Wired.com* and others. While circumstances led many to assume the United States turned off North Korea's internet, Kaplan is equally decisive in his claim that the United States was not responsible. It is difficult to know if the respective assailants concerned themselves much with attribution or misdirection. That said, their results speak for themselves.

For the hackers who conducted the attacks, judging their adversary's commitment to attribution and their own reciprocal vulnerability seems relatively straightforward. Surely Sony's assailants understood that Sony, a leading institution in a multibillion dollar industry, could marshal significant resources for attribution on its own, not counting any support that might have been offered by the US government. Indeed, without help from China or some other interested party, North Korea would seem to have fewer capabilities available for attribution than Sony. The model assesses a high score for reciprocal or "in-kind" vulnerability for whoever cut North Korea's internet, as North Korea seems to have been unable to appropriately place the blame. As such, for North Korea, whether the attacker was a hacktivist group or cyber warriors based in the United States, returning the favor would likely have proven difficult.

Again, for the purposes of this analysis the question of reciprocal vulnerability focuses on whether an attacker should fear their cyber weapon being turned on them. In other words, if an attacker "unveils" a new weapon in any domain then reciprocal vulnerability should be a concern. Whoever attacked Sony likely had only minor concerns in this area. Surely they would have assumed that Sony would not respond directly. A better question might have been whether or how the United States would respond. One might surmise from Kaplan, or from Singer and Friedman's depiction of the various policy debates, that America would not have responded to an attack against a business with an all-out cyber assault of its own.

This leaves hacktivist groups, which represent something of a wild card. Hacktivists militantly support a variety of issues, so the potential for a reciprocal attack conducted as retribution for the Sony hack seems high. For example, the loose-knit hacker group known as Anonymous has a reputation for retaliating against the suppression of speech. Hacktivists emerge as likely suspects in the attack that led to North Korea

briefly losing its internet connection. Indeed, when thinking about reciprocal vulnerability, the question of who will respond to an attack, if the attack is properly attributed, seems just as important as whether someone will reciprocate. Some actors are simply far less constrained than others.

## **Recommendations for the Future**

### **Accept Risks at Lower Command Echelons**

US Army doctrine defines operational art as “the pursuit of strategic objectives, in whole or in part, through the arrangement of tactical actions in time, space, and purpose.”<sup>47</sup> That definition appropriately conveys the requirement for military planners to synchronize operations across war-fighting domains. There simply is no potential for synchronicity and synergy if the right effects do not happen across the desired domains at the right time. Therefore, if a nonattributed effect is desired, that effect must be generated at the right moment in concert with other more visible efforts.

Further, in line with deception doctrine, there must be an operational reason to pursue nonattribution. One area where nonattributed effects might prove particularly effective is in shaping the battlespace in support of future operations. Kaplan relates the story of Operation Orchard, in which he claims that an elite Israeli cyber unit successfully hacked Syria’s air-defense radars in such a way as to keep Syria’s radar screens blank while the Israeli Air Force launched a devastating attack on a Syrian nuclear facility.<sup>48</sup> To maximize the chance that their fighters could penetrate Syrian airspace unnoticed, the Israeli team had to achieve the cyber effect at just the right time. This was a covert cyber operation, a perfect example of a covert, nonattributed effect achieved at just the right time, for just the right amount of time, in support of the overall operational plan.

The Operation Orchard example highlights the necessity for synchronization across domains or, put another way, it is an example of multi-domain operations in action. That level of integration and planning suggests several things about planning and execution. Clearly, an airstrike against another country’s secret nuclear program would require strategic level direction. However, planning, coordination, and execution in

real time could likely have occurred at a lower echelon. Indeed, given the synchronization necessary for the cyber operators to control the Syrian air picture just as the fighters were preparing to penetrate Syrian airspace suggests the necessity for tight command and control integration. It also implies that the Israelis were prepared to “lose” whatever tool they employed in the hack. That willingness is critical for synchronizing operations at lower echelons.

This suggests the need for further development of operational constructs and doctrine that push planning, decision making, and execution for non-attributable effects down to lower command echelons. The establishment of small teams at multi-domain operations centers (MDOC) with access to US Cyber Command tools and authorities that resemble Air Force National Tactical Integration cells that already support the air component in the joint fight seems warranted. These specially trained, cyber-oriented integration teams would play a key role in helping future MDOC strategy and targeting cells leverage attribution as a source of advantage.

The attribution advantage model examples seem to support the idea of pushing execution authority for nonattributed effects to lower echelons. In near perfect conditions of attribution supremacy, the overall risk is such that decisions impacting real-time coordination and execution can likely be assigned to lower echelons of command. Of course, the highest echelon authority would most likely always need to approve something like Operation Orchard. The Israelis appear to have intended that operation as a surgical use of military force, in what was likely hoped to be a singular event. However, had the Israeli action been part of a prolonged air campaign, the operation might better have been served by pushing authorities down and accepting risk at lower echelons. Pushing that risk down to lower echelons with necessary authorities and capabilities should be considered because doing so seemingly creates opportunities to begin winning the conflict to the left of “Phase 0” on traditional planning timelines.

### **Self-Attribute to Win Time and Boost Deterrence**

Attribution challenges traditional thinking about deterrence, and formulating deterrence strategies against adversaries that have achieved attribution advantage seems inherently difficult. This is because deterrence begins with one actor understanding the capabilities and actions

of another. There is an inherent promise within deterrence that some form of costly retaliation will occur if one actor crosses the “red line” of another. Such retaliation begins with realization and attribution. If one is unaware of being attacked or is unable to attribute the attack, effective retaliation is difficult. In this way, nonattribution creates a difficult problem for effective deterrence strategies. However, self-attribution, which involves credibly claiming responsibility for an act one may or may not have committed, emerges as a tool that can help commanders influence the timing and tempo of conflict.

John Norton Moore brilliantly explored the role deterrence plays in conflicts outside the digital realm between democracies and non-democracies. He defined “effective deterrence” as the “aggregate of external incentives known to and understood by a potential aggressor as adequate to prevent the aggression.”<sup>49</sup> A critical aspect of the relationship between deterrence and attribution is that an actor with digital realm attribution advantage can add two critically important words to the end of Moore’s definition: “if caught.” Further, in his 2003 essay entitled “Solving the War Puzzle,” Moore reached an important conclusion. While exploring the dynamic between democracies and non-democratic states engaged in war he found that “the principle path to major interstate war for democracies seems to be failing to ensure adequate levels of deterrence when confronted by potential aggressors.”<sup>50</sup> Moore then summarized the reasons why deterrence fails:

Deterrence failure can occur because of an absence of adequate military forces, as was true of the U.S. entry into World War II and, in part, the Japanese attack on Pearl Harbor; lack of communication of intent (or even any advance formation of an intent to defend), as was true in the Korean and Gulf Wars; or lack of believability of the guarantee, as was true of British entry into World War II and, in part, Milosevic’s decisions to defy NATO in Bosnia and Kosovo.<sup>51</sup>

Moore focused on interactions between nations, but his conclusions about deterrence would better hold up against a range of state and non-state actors were it not for the complications created by the difficulty of attribution in the cyber domain. Attribution creates an obstacle for deterrence and incentivizes attacks by the weak against the strong.

Henry Kissinger senses the danger in the difficulties of cyberattack attribution. In *World Order*, Kissinger writes that “internet technology has outstripped strategy or doctrine—at least for the time being.”<sup>52</sup> What he means is that the combination of the public’s reliance on the

internet and the internet's current and perhaps inherent vulnerabilities creates incongruence within the international system. Attribution is at the core of his concerns as Kissinger asserts that "when individuals of ambiguous affiliation are capable of undertaking actions of increasing ambition and intrusiveness, the very definition of state authority may turn ambiguous."<sup>53</sup> He continues, stating "actions undertaken in the virtual, networked world are capable of generating pressures for countermeasures in physical reality, especially when they have the potential to inflict damage previously associated with armed attack."<sup>54</sup> But how certain must a "responsible" actor be of the culprit after a particularly damaging or disruptive attack? Such is the nature of attribution advantage.

A nation under cyberattack may feel pressured from within to retaliate, but uncertainty about who conducted the attack and why can lead to decision paralysis or, perhaps worse, conflict escalation with a rival that may not even be responsible for the attack. In a broader sense, time can be thought of as an output in deterrence-based equations. The United States and the Soviet Union seemed destined for armed conflict for decades during the Cold War. However, during moments of crisis the existence of nuclear weapons provided a deterrent to conflict escalation. This bought both sides the time necessary to attempt to achieve their political goals through less destructive means, at least until one side exhausted the resources necessary to sustain the status quo.

The difficulty of the attribution problem and whether attribution remains beyond the reach of traditional deterrence strategies is up for debate. Kissinger suggests that this "new world of deterrence theory and strategic doctrine now in its infancy requires urgent elaboration."<sup>55</sup> USAF Gen Kevin Chilton, in line with Moore's analysis of deterrence failure, suggests that part of the problem is "the lack of a known historical track record of US detection, attribution, and response" which fundamentally challenges the credibility of deterrent threats.<sup>56</sup> He further advocated that responses to cyberattacks need not be limited to the cyber domain.<sup>57</sup> Therein lies the key. If one accepts the notion that time is an output of deterrence calculus, then self-attribution seemingly becomes necessary. If deterrence is a function of capability, credibility, and communication, then at some point capabilities must be made known.

Lindsay points out attackers may derive some benefit in terms of acknowledged capability once an effect for which they are responsible is attributed.<sup>58</sup> Doing so certainly requires the type of thorough evaluation

explored above. In the cyber realm, transparency probably means that some techniques, tools, and even networks should be set aside from more elegant capabilities and made visible only if doing so supports the commander's intent. If a status quo develops in which no one admits capabilities, no one admits detecting the capabilities of others, and no one risks responding to cyberattacks for fear of revealing detection methods, then the ability of deterrence to serve as a well from which to draw time will remain diminished.

### **Wargame Attribution Advantage**

Unlocking the full potential inherent in the above recommendations for weaponizing attribution requires investment in two enabling concepts. First, multi-domain attribution choices must be present in operational war gaming and exercises. Helmuth von Moltke the Elder, who in his military career mastered sweeping technological advances in firepower, transportation, and logistics technology, wrote, "We in the military pay due attention to the progress of science and to inventions in other than military matters. But an invention is not what it is in itself. The value of any invention rests not only in theory, even if correct, but mainly on its practical application by complete technical development . . . it will therefore no longer suffice merely to observe what is done in other areas. We must ourselves perfect the invention."<sup>59</sup>

Perfecting inventions and mastering operational concepts requires realistic training, exercises, and war gaming. A report published by the Defense Science Board echoes Moltke's comments: "Effective experiments are an innovation-enabler . . . these procedures can improve the effectiveness of new defense systems and can create surprise, challenge our adversaries, and help anticipate how new technologies and systems concepts might be used against U.S. forces."<sup>60</sup>

Personalized training tailored to every echelon of command across scenarios modified to present different challenges has the potential to make training more realistic than ever.

Gaming technology and virtual reality will have the potential to increase the frequency and lower the cost of training. While there is nothing that quite compares to the danger of being under fire, technology is creating the opportunity for training opportunities that are profound in their realism. Soldiers, Sailors, Marines, and Airmen must be allowed to employ techniques and tools that leverage the underlying premise

of attribution advantage. For example, cyber domain war games must accurately demonstrate how accesses gained and maintained months or even years before what one might consider the traditional beginning of Phase 0 shaping operations can be brought to bear and synchronized with other effects.

Of course, training should not just revolve around using cyber and other tools to leverage attribution advantage. Commanders at all levels should consider how to respond and even how best to render their best military advice, when the adversary has seized attribution advantage for itself. How does one structure one's thinking in formulating a response when the assailant's identity and motivations are ambiguous? In his book *Misguided Weapons*, Israeli defense expert Azriel Lorber describes a type of technological surprise in war whereby the "existence of a new weapon is known," but its capabilities are not fully considered across "potential battlefield scenarios."<sup>61</sup> Lorber also describes situations where an adversary had actually faced a weapon before, but for whatever reason—perhaps because lessons were not properly learned and applied—is surprised more than once by the same technology. He call this unfortunate state "self-inflicted surprise."<sup>62</sup> Unless war fighters are allowed to succeed and fail in their efforts to leverage attribution advantage it is difficult to imagine how the potential of those techniques might be fully realized in war. Further, war fighters who have not been trained to adequately anticipate and respond to the attribution problems posed by adversaries would seem to be at a disadvantage here, in what may prove to be the age of hybrid warfare.

### **Defend with Open-Source Intelligence**

A second enabling concept required for achieving attribution advantage involves placing increased focus on and investment in open-source intelligence collection, processing, and analysis. Attribution advantage cannot be thought of in offensive terms only. Attribution superiority involves achieving attribution advantage in support of one's own operations while denying it to the enemy. Therefore, defensive measures must be anticipated to thwart the efforts of adversaries who might weaponize attribution toward their own ends.

Open-source intelligence and data mining seem to hold some promise in this regard. Looming advances in artificial intelligence (AI) systems meant to improve our personal lives will quickly find military applications.



AI-empowered analytical processes may prove to be incredibly powerful for open-source intelligence. In his book *The Inevitable*, Kevin Kelly writes about how Google Photo's AI can remember objects in every one of the 130,000 pictures he has uploaded. He also points out that Facebook has AI capable of correctly identifying a single person's face in a crowd of billions.<sup>63</sup> What if that same computer vision technology had been employed against Putin's little green men? In scenarios like Crimea, political leaders may not be able to counter the claims of their rivals without exposing sensitive sources and methods. Open-source intelligence enhanced by artificial intelligence and machine learning seems both promising and necessary.

If one considers open-source intelligence as encompassing everything from foreign news services to tourists posting pictures on social media, what begins to emerge is a data-rich, yet chaotic, information environment. Col Jason Brown recently described this potential as "seeing the data trails" left behind by the various actors in a conflict and described how a "simple tweet" sent at the wrong time could have "blown the cover of the SEAL team sent to kill Osama bin Laden."<sup>64</sup> The varying degree of chaos in the data trails will make following those trails difficult for humans acting alone. This is because the raw data is created and moves throughout the environment in myriad ways.

For example, a tornado forms near a city. The local news channels will report on the event, weather radars will provide data, and individuals near the affected area will take pictures before, during, and after the event. Eventually a complete picture of the event, informed by numerous sensors, emerges and enhances understanding of what happened. AI systems have the potential to bring order out of that chaotic information environment, creating decision-quality information in less time than humans could ever manage on their own. This holds tremendous potential in making weaponized attribution both an offensive and a defensive reality. When an actor in the conflict claims not to be responsible for some atrocity that has happened, AI-driven systems may eventually be able to provide analysts with the open-source information necessary to refute that claim. Disinformation from "fake news" will find itself surrounded by "antibodies" of truth at machine speed. This means the side that better exploits emerging AI technologies will hold a clear advantage in the contest for time. They will be capable of sense-making faster than their adversaries and will be able to burn through the false narratives

future adversaries push in the information environment in less time. From that come flexibility and increased decision space.


## **Conclusion**

Time is everything in attribution advantage. Decision cycles turn upon the ability of command and control systems to accurately connect actions with actors. Attribution emerges as a fundamental component throughout decision making. The problems that attribution can create present both an opportunity for fresh thinking about targeting and a challenge in terms of deterrence, defense, and retaliation.

A number of topics addressed in this article would benefit from additional research. The models captured in the spider graphs were provided as examples intended to help facilitate analysis of the model itself and how the attribution advantage model presented here might help decision makers and planners visualize the risk and opportunities inherent to the pursuit of nonattributed effects. The notional values assigned to the model's various components were derived from unclassified open-source material. While classified data would better inform real-world model employment, for the purpose of this paper the exact numeric values depicted are meant to explore the terms of the model and the general phenomenon of attribution. The real question is whether the attribution advantage model would aid strategic decision makers, commanders, and operational planners with questions about whether to employ nonattributed effects prior to conflict. Exploring that requires specifically tailored war gaming. Finally, the costs and implications of the recommendations made in this paper need further refinement and exploration at a higher classification.

The question of attribution seems to turn upon the degree to which one is seeking to either foster uncertainty or produce friction in adversary systems. There are many scenarios where maintaining the stealth of the effects being generated for as long as possible is necessary to generate the maximum amount of friction in the adversary's systems. Yet, one should expect and plan for every covert operation to be discovered eventually. Still, therein opportunities to gain further advantage await. Leveraging the moment when an adversary discovers a previously undetected effect to foster uncertainty about the effect's origin will often cause the adversary to expand their decision cycles as they attempt to decipher what is happening and who to blame. However, self-attribu-

tion, conducted aggressively and defiantly at the proper moment, may cause the adversary to question the reliability of other data streams. Self-attribution, if accomplished without compromising exquisite, irreplaceable tools and capabilities, seems necessary for reinforcing deterrence, especially in cyberspace.

Seizing attribution advantage means controlling or influencing what adversaries know about what is happening to them, and most importantly, who they blame. This provides the operational artist with a unique method of influencing or even dictating the timing and pace of events, even as they produce additional effects across multiple domains. Therefore, attribution should be made more explicit in planning multi-domain operations, especially for the early phases of conflict. While no one can alter the physics of time, military planners and targeteers should seek to influence the pace at which events unfold. Planners can guide their adversaries toward hasty decisions made on faulty premises or even generate and later take credit for effects that cause adversaries to have so little trust in their data streams that it paralyzes their decision making. There is great opportunity for those who seek and seize the initiative in such moments. 

## APPENDIX

### **Author's Note on Scoring with the Attribution Advantage Model**

As described in the text, scoring within the attribution advantage model is necessarily subjective in that it will always be based on imperfect all-source knowledge of the adversary and, potentially, imperfect knowledge of one's own capabilities. Still, decision makers and planners need ways to structure their thinking about how to identify those moments prior to or even during a conflict when they might hold attribution advantage. Further, the attribution advantage model provides a visualization of risk. The more points an analyst plots toward the center, the higher the assessed level of risk.

Whether employed academically or as an operational planning tool, the scores within the model can only be assessments made from the best available information. For example, operational planners might assess that there is zero percent chance that an effect will have unintended consequences during or after execution. Utilizing this model, they would

give *ue* a score of 30. The planners would then be wise to have an explanation for their certainty ready prior to briefing their commander, because any commander well trained or tested by the inherent uncertainties of war will challenge that assessment. This model is presented as a tool intended to structure both the commander's and the planners' thinking while providing a visual aid that highlights the risks involved in generating effects that one would prefer to remain unattributed, either forever or until the moment of their choosing.

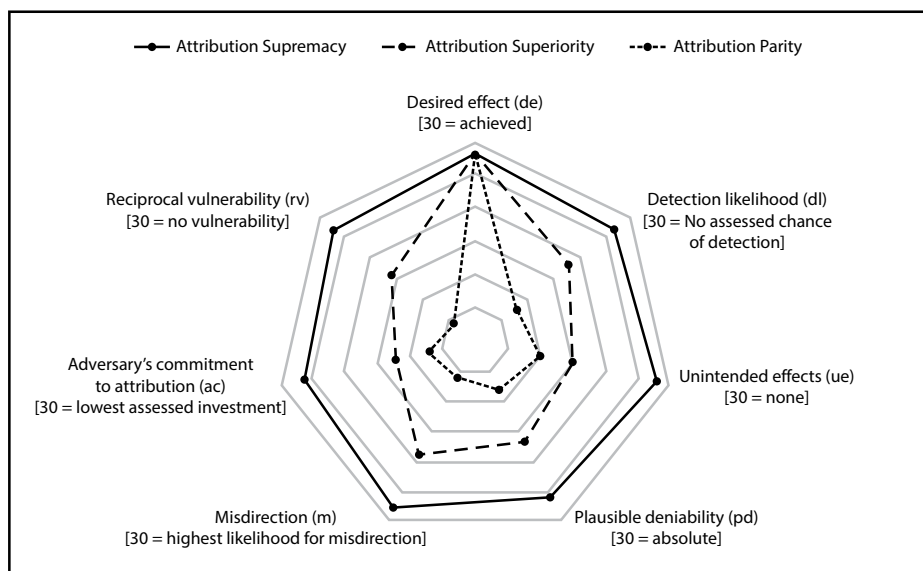
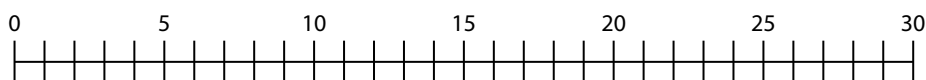


Figure 6. The attribution advantage model

The following scales are offered to further explain the author's intent for scoring in the model, to illustrate scoring in the mini-case studies, and to guide others who might use the model.

### Desired Effect

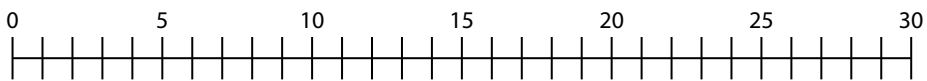


**0:** No assessed chance of achieving desired effect with the capability in question. This might be due to hardening or redundancy in the target or the nature of the adversary's political system.

**15:** The odds of achieving the effect are assessed at 50 percent given the nature of the target, the adversary's preparations for the intended effect, and the nature of aggressor capabilities.

**30:** Achieving the desired effect is an absolute certainty given a clear overmatch between the aggressor's available capabilities and the adversary's vulnerabilities.

### Detection Likelihood

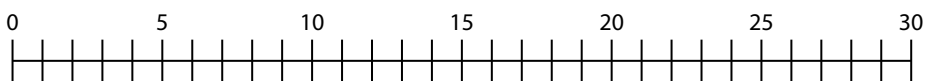


**0:** The adversary will detect or notice this effect the moment it is generated.

**15:** The odds of detection are assessed at 50 percent given the nature of the adversary, the adversary's defenses, and the nature of tools available to achieve the effect

**30:** There is no chance the adversary, or any other party, will ever detect the planned effect.

### Unintended Effects

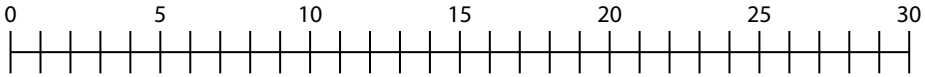


**0:** The effect, once employed, will spread in ways the aggressor cannot control and will have numerous unintended effects throughout the targeted system.

**15:** The likelihood of unintended effects generated is 50 percent, due to limited testing, lack of knowledge about the offensive capability, and unknowns in the targeted system.

**30:** There is no chance of unintended effects based on superior understanding of the target system and a high degree of successful operational testing of the capability being considered.

### Plausible Deniability

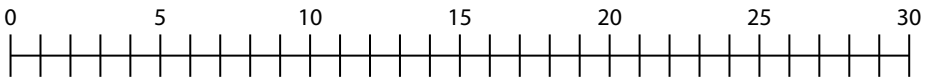


**0:** There is zero chance that the aggressor can make the targeted party and the rest of the world think that some other party is responsible for this effect.

**15:** The odds that the aggressor can plausibly deny responsibility for the generated effect are 50 percent, given the adversary's defenses, third-party interest, and the nature of available capabilities required to achieve the effect.

**30:** There will never be enough proof for an adversary or third party to positively attribute the effect to the aggressor with the certainty necessary to justify retaliation.

### Misdirection

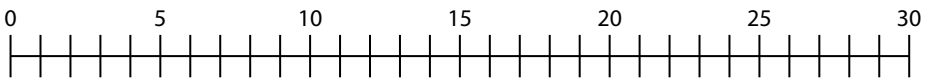


**0:** Not only will the aggressor's action be detected, but also any steps the aggressor took to make it look like some other party was responsible will also be noticed.

**15:** The odds of misdirection working are assessed at 50 percent given the nature of the adversary, the adversary's defenses, and third-party interest and investigation.

**30:** The aggressor's efforts to cause its adversary to believe that some other party is to blame for the aggressor's actions succeed with absolute certainty given the technology in play or the adversary's predispositions and impatience with forensic efforts.

### Adversary's Commitment to Attribution

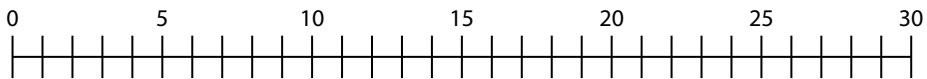


**0:** The adversary and interested third parties possess limitless resources and commitment to forensic efforts designed to uncover the party responsible for the generated effect.

**15:** The adversary and aligned third parties can bring significant forensics capability to bear, and odds that they will eventually attribute an effect accurately are assessed at 50 percent.

**30:** The adversary completely lacks forensics capability with the aggressor's vector for covert attack, and third parties are either unaware or uninterested in offering outside assistance.

## Reciprocal Vulnerability



**0:** The aggressor shares the same vulnerabilities as the adversary, and if the capability is employed, the aggressor will inevitably and unavoidably fall victim to the same capability.

**15:** The odds of the aggressor finding itself vulnerable to the effects it intends to generate against an adversary are 50 percent, given incomplete efforts to insulate itself from the capability.

**30:** The aggressor's capabilities are so tailored and precise, and its own defenses are so secure, that the aggressor is completely immune from the capabilities it intends to unleash against its adversary's in pursuit of some desired effect.

### Notes

1. Gen David Goldfein, "Remarks to 2016 Air Force Association Air, Space, and Cyber Conference" (speech, National Harbor Maryland, 20 September 2016), [http://www.af.mil/Portals/1/documents/csaf/Goldfein\\_Air\\_Force\\_Update\\_Sept\\_2016.pdf](http://www.af.mil/Portals/1/documents/csaf/Goldfein_Air_Force_Update_Sept_2016.pdf).

2. Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1-2 (2015): 4–37, <http://doi.org/ckvx>.

3. John R. Boyd, *Patterns of Conflict* (presentation notes, December 1986), slide 7, <http://www.danford.net/boyd/patterns.pdf>, accessed 3 March 2017. For more on Boyd's concepts, see his new book *A Discourse on Winning and Losing* (Maxwell AFB, AL: Air University Press, 2018), <http://www.airuniversity.af.mil/AUPress/Books/>.

4. Boyd, *Patterns*, slide 7.

5. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 117–18.

6. Boyd, 102.

7. Nicholas G. Carr, *The Shallows: What the Internet Is Doing to Our Brains* (New York: W. W. Norton, 2010), 131.

8. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2013), 20–22.

9. Kahneman, *Thinking*, 85.
10. Kahneman, 85.
11. Department of Defense (DOD), Joint Publication (JP) 3-13.4, *Military Deception* (2017), I-1.
12. DOD, *JP 3-13.4*, I-4.
13. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (June 2015): 316-348, <http://dx.doi.org/10.1080/09636412.2015.1038188>.
14. Roger T. Ames, *Sun Tzu, The Art of Warfare: The First English Translation Incorporating the Recently Discovered Yin-ch'üeh-shan Texts*, 1st ed. (New York: Ballantine Books, 1993), 104.
15. Boyd, *Patterns*, slide 41.
16. Boyd, slide 13.
17. Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987), 4.
18. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 44-71, [https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC\\_a\\_00266](https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266).
19. Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of CyberSecurity* 12, no. 1 (September 2015): 4, <https://doi.org/10.1093/cybsec/tyv003>.
20. David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, 1st ed. (New York: Crown Publishers, 2012), 205.
21. Treverton, *Covert Action*, 4.
22. Vitaly Shevchenko, "'Little Green Men' or 'Russian Invaders?'" BBC News, 11 March 2014, <http://www.bbc.com/news/world-europe-26532154>.
23. "Putin Reveals Secrets of Russia's Crimea Takeover Plot," BBC News, 9 March 2015, <http://www.bbc.com/news/world-europe-31796226>.
24. Mathew Kroenig, "Facing Reality: Getting NATO Ready for a New Cold War," *Survival* 57, no. 1 (February-March 2015): 45, <http://doi.org/bt9t>.
25. Kroenig, "Facing Reality."
26. Marcel Van Herpen, *Putin's Wars: The Rise of Russia's New Imperialism*, 2nd ed. (London: Rowman and Littlefield, 2015), 270.
27. Nicola Clark and Andrew E. Kramer, "Malaysia Airlines Flight 17 Most Likely Hit by Russian-Made Missile, Inquiry Says," *New York Times*, 13 October 2015, [https://www.nytimes.com/2015/10/14/world/europe/mh17-malaysia-airlines-dutch-report.html?\\_r=0](https://www.nytimes.com/2015/10/14/world/europe/mh17-malaysia-airlines-dutch-report.html?_r=0).
28. George Crile, *Charlie Wilson's War: The Extraordinary Story of the Largest Covert Operation in History* (New York: Atlantic Monthly Press, 2003), 217-18.
29. Crile, *Charlie Wilson's War*, 217.
30. Treverton, *Covert Action*, 213.
31. Crile, *Charlie Wilson's War*, 128.
32. Crile, 105.
33. Crile, 405.
34. Crile, 419-21.
35. Crile, 405.
36. Crile, 105.
37. "North Korea Threatens War on US over Kim Jong-Un Movie," BBC News, <http://www.bbc.com/news/world-asia-28014069>, accessed 10 March 2017.



38. “North Korea Denies Responsibility for ‘Righteous’ Hack Attack on Sony,” BBC News, <http://www.bbc.com/news/world-asia-30366449>, accessed 10 March 2017.
39. Kim Zetter, “The Evidence that North Korea Hacked Sony Is Flimsy,” *Wired.com*, 17 December 2014, <https://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin/>.
40. Zetter, “Evidence.”
41. Fred M. Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), 269.
42. Nicole Perlroth and David E. Sanger, “North Korea Loses Its Link to the Internet,” *New York Times*, 22 December 2014, [https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html?\\_r=0](https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html?_r=0).
43. Kaplan, *Dark Territory*, 271–72.
44. Dan Holden, “North Korea Goes Offline,” *Arbor Networks*, 22 December 2014, <https://www.arbornetworks.com/blog/asert/north-korea-goes-offline>.
45. P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, ed. Allan Friedman (New York: Oxford University Press, USA, 2014), 117.
46. “The Interview: A Guide to the Cyber Attack on Hollywood,” BBC News, 29 December 2014, <http://www.bbc.com/news/entertainment-arts-30512032>.
47. US Army Doctrine Publication 3.0, *Unified Land Operations* (Washington, DC: Headquarters, Department of the Army, October 2011), 9, [https://www.army.mil/e2/rv5\\_downloads/info/references/ADP\\_3-0\\_ULO\\_Oct\\_2011\\_APD.pdf](https://www.army.mil/e2/rv5_downloads/info/references/ADP_3-0_ULO_Oct_2011_APD.pdf).
48. Kaplan, *Dark Territory*, 160–61.
49. John Norton Moore, “Solving the War Puzzle,” *American Journal of International Law* 97, no. 2 (April 2003): 285, <http://www.jstor.org/stable/3100103>.
50. Moore, “Solving,” 286.
51. Moore, 286.
52. Henry Kissinger, *World Order* (New York: Penguin Press, 2014), 344–45.
53. Kissinger, 344–45.
54. Kissinger, 346.
55. Kissinger, 347.
56. Kevin Chilton and Greg Weaver, “Waging Deterrence in the Twenty-First Century,” in *Proceedings: Deterrence in the Twenty-First Century*, ed. Anthony C. Cain (Maxwell AFB, Alabama: Air University Press, 2016), 72.
57. Chilton and Weaver, “Waging Deterrence.”
58. Jon R. Lindsay, “Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack,” *Journal of Cybersecurity* 1, no. 1 (September 2015): 3, <https://doi.org/10.1093/cybsec/tyv003>.
59. Helmuth Moltke and Daniel J. Hughes, *Moltke on the Art of War: Selected Writings* (Novato, CA: Presidio Press, 1993), 257.
60. Defense Science Board, “Technology and Innovation Enablers for Superiority in 2030” (Washington, DC: Defense Science Board, 2013), 78, <http://www.dtic.mil/dtic/tr/fulltext/u2/a608507.pdf>.
61. Azriel Lorber, *Misguided Weapons: Technological Failure and Surprise on the Battlefield* (Washington, DC: Brassey’s Inc., 2002), 229–30.
62. Lorber, *Misguided Weapons*, 230.
63. Kevin Kelly, *The Inevitable: Understanding the 12 Technological Forces that Will Shape Our Future* (New York: Viking, 2016), 46.
64. Jason Brown, “In the Information Age: Centers of Activity > Centers of Gravity,” *Medium*, 5 May 2015, <https://medium.com/@jasonmbro/in-the-information-age-c70622a61bc9>.

# Beyond the Tweets: President Trump's Continuity in Military Operations

*Peter Dombrowski*  
*Simon Reich*

## Abstract

Scholars and analysts continue reviewing and analyzing elements of change and continuity in President Trump's US national security policy. Voices within the media and policy community have often questioned whether it is descending into chaos.<sup>1</sup> Behind the focus of the daily news cycle is a more profound question: is President Trump's approach to the use of military force characterized more by change or continuity compared to his predecessors? The prevailing opinion has favored change. We argue that even the apparently confusing periods of the first year of the Trump administration have been characterized more by continuity in military force decisions than change. In this article, we outline the reasons for this claim and defend it through three examples involving military forces: anti-Islamic State operations in Syria and Iraq, combating the Taliban in Afghanistan, and confronting North Korea.

\* \* \* \* \*

With over a year having passed since Donald Trump's inauguration, American scholars and analysts have gone into overdrive in reviewing his record to date, both predicting and prescribing his administration's future national security policy. The daily tide of presidential tweets and

---

Peter Dombrowski is professor of strategy in the strategic and operational research department at the Naval War College. His most recent book, coauthored with Simon Reich, is *The End of Grand Strategy: US Maritime Operations in the Twenty-first Century* (Cornell, 2018). He is also coauthor with Catherine McCardle Kelleher of the edited volume *Regional Missile Defense from a Global Perspective* (Stanford, 2015).

Simon Reich is professor in the division of global affairs and department of political science at Rutgers University. Reich was formerly director of The Ford Institute for Human Security and director of research and analysis at the Royal Institute of International Affairs (Chatham House) in London. He can be reached at [Reichs@Rutgers.edu](mailto:Reichs@Rutgers.edu).

occasional interviews on Fox TV has often been regarded as the primary indicator of the president's thinking. Trump's grand strategy has been characterized as "hard-nosed and realistic—and less ambitious and idealistic than prior efforts . . . a 'corrective' to the past 16 years of American foreign and security policies that overestimated America's influence and importance, and lost track of priorities."<sup>2</sup> His senior staff has labeled it "pragmatic realism."<sup>3</sup> And it has generally been assumed by policy scholars and media that the president's outpouring of often contentious comments is indicative of both American foreign policy and the country's evolving military strategy.<sup>4</sup> To date, a variety of views have been expressed about President Trump's approach to foreign and security policies, that it: is nonexistent; is haphazard and chaotic, and thus incoherent; is "transactional" and pragmatic; or is ideological—an "America First" approach interpreted by some as isolationist but better understood as Jacksonian populism.<sup>5</sup> But the widespread consensus is that chaos rules and the president is fickle, often undermining his staff's comments on a variety of issues spanning from Afghanistan to North Korea, NATO, and various conflicts in the Middle East. The successive firings of both Rex Tillerson and H. R. McMaster, to be replaced by more hawkish appointees Mike Pompeo and John Bolton, respectively, have amplified that view. Moreover, President Trump's cabinet officials have chosen to gut the departments they lead by firing or not replacing departing staff. Indeed, by 1 December 2017, the Trump administration was estimated to have filled only 26 of 54 of its top Department of Defense jobs and 55 of 153 Department of State positions.<sup>6</sup> This indicates there may be elements of truth to the criticisms. Certainly, the 2017 *National Security Strategy* did nothing to dispel the confusion, with its focus on China and Russia as strategic competitors, in contrast to the president's favorable comments about the leadership of both, and an emphasis on a multilateral approach, versus the president's occasional unilateral decisions.<sup>7</sup>

But behind the focus of the daily news cycle, the firings and hirings, and official publications is a more profound question: is the administration's approach to actual military operations characterized more by continuity or change compared to his immediate predecessors? The prevailing opinion among elites to date, suggesting change, is based on the president's rhetoric and policy statements. That opinion is understandable. President Trump appears at times to be the "anti-Obama" in his

castigation of NATO allies; coddling of Saudi Arabia; blatant snubbing of Angela Merkel; demonization of London mayor Sadiq Khan; laudatory characterization of Vladimir Putin, Rodrigo Duterte, and Tayyip Erdogan; and willingness to launch Tomahawk missiles against the Syrian government. Except for the missile strike, none of these examples entail military operations.

We dissent from the popular judgment that focuses predominantly on chaos and change when it comes to the critical realm of national security by examining the conduct of military operations. Our optic thus moves beyond the tweets by surveying what American military forces have done in the administration's first year. We suggest that, given his rhetoric, President Trump's influence to date in shifting the contours of America's existing or potential military operations has been more modest than might be expected. We contend that President Trump's campaign promises to initiate larger, radical military changes have gone unfulfilled. Rather than his spoken threats to unleash "fire and fury" on North Korea's regime, his speeches proclaiming a new strategy in Afghanistan, or his tweets about launching a larger war that would "bomb the hell out of ISIS" and then seize Iraq's oil fields, the administration's behavior to date has predominantly had the hallmarks of continuity, not change.<sup>8</sup>

Recognizing that the churning of senior appointments may change this pattern, we nonetheless defend our claim and explain the reasons for the disjuncture between President Trump's radical rhetoric and the general continuity demonstrated by his administration's ongoing and prospective military operations. The reasoning includes how military operations are constrained by local conditions and reinforced by domestic and leadership constraints. We then provide three high-profile examples to substantiate our position, specifically chosen because of both their size and significance and the fact that they have received significant media attention since the inauguration: anti-Islamic State operations in Syria and Iraq, efforts to combat the Taliban in Afghanistan, and the military movements and potential consequences of the ongoing nuclear crisis with North Korea. In the first two scenarios, the circumstances have remained consistent and so have the operations. In the North Korean case, a change in military operations has occurred, but it has been influenced by changing circumstances in the theater of war and so remains a deterrent approach coupled with an offer to negotiate consistent with the behavior of his predecessors. Pointedly, the ramping up of North

Korean aggression has resulted in a comparable increase in American operational deployment and preparedness. Collectively, these three geographically diverse cases focus on priority areas most scholars and analysts regard as the priorities of contemporary national security strategy: counterterrorism, counterinsurgency, and preventing nuclear conflict.

### **Drivers of Continuity in Military Operations**

American military operations in the twenty-first century must adapt to local conditions and a dynamically evolving environment.<sup>9</sup> This is because local military operations are conditioned by the answers to three questions. First, what type of actors do US forces face? During the Cold War, American planners largely (although not exclusively, as the Viet Cong demonstrated) had to strategize against adversarial states or state proxies. They still exist—from Iran to North Korea—as the recent *National Security Strategy* stressed. But now the US must also contend with a variety of nonstate actors, stretching from transnational terrorist groups and criminal organizations to pirates and even private corporations who participate, for example, in money laundering.

Second, what type of threat does the US face? As the number and types of strategic actors have proliferated, so have the forms of threats. The Cold War concentrated the minds of American strategic planners on narrowly defined military threats, notably the Warsaw Pact and assorted client nationalist proxy groups (for example, in Angola or Mozambique). In the twenty-first century, however, the American public and thus American strategic planners have expanded the definition of a security threat to incorporate a variety of illicit flows: of people, of drugs, of nuclear and fissile materials and parts, and even of viruses.<sup>10</sup> Relatedly, the geographic source of the threat has also expanded. It now includes a vast expanse of scattered ungovernable zones we now call “failed and fragile states,” whereas it used to be primarily focused on Europe.

Third, what forms of conflict does the US face, or potentially face, in a particular theater? The focus of the Cold War remained squarely on interstate forms of conflict such as conventional and nuclear war.<sup>11</sup> To that has now been added both asymmetric warfare (in fighting a succession of irregular wars in fragile states) and, more recently, hybrid conflicts that combine aspects of the first two with novel technological elements

that include cyber instruments, as the Russians vividly demonstrated in Eastern Ukraine.

American forces now face varying configurations of all three, depending on local conditions in a theater of conflict. They contend with pirates off the Somali coast and criminal gangs seeking to smuggle drugs into the United States, who both use asymmetric means and are motivated by little more than theft. They combat jihadists in the Middle East who are engaged in an ideological struggle and use asymmetric and hybrid means. And they oppose a North Korean state that poses (at least potentially) an existential threat to US territory. Furthermore, many strategists believe that a new era of great power conflict has already begun with China or Russia. In summary, the combinations abound.

By focusing on continuity, we are not suggesting that operational changes in strategy never occur. In practice, as we demonstrate, these factors can and do change in theaters of conflict. The character of the opposition can evolve, as was the case when the Revolutionary Armed Forces of Columbia (FARC) morphed from a revolutionary group into a transnational criminal organization. The nature of a threat can change, as North Korea's recent development of intercontinental ballistic missiles (ICBM) that threaten American territory highlights. And the form of warfare can alter, as the Islamic State (IS) shifting from employing conventional and irregular warfare tactics in a territorial conflict to transnational terrorism using asymmetric tactics illustrates. Strategies therefore change to meet local conditions.

Nonetheless, although operational circumstances may evolve over time, presidents generally inherit the same or similar ones of their predecessors. President Trump—despite his forthright approach—is as much of a captive to these constraints as were his predecessors, George W. Bush and Barack Obama. Despite the president and his advisors' proclamation that they will pursue different approaches than those of previous administrations, circumstances generally limit their degrees of freedom in the prosecution of military operations.

### **Domestic Bureaucratic and Leadership Constraints on Military Operations**

Furthermore, presidents inherit both the domestic political, bureaucratic, and historical capabilities and constraints of the American political system and national security state. Incoming presidents invariably de-

pend on a national security structure developed over decades. It includes, below the level of political appointees, many of the same personnel and, of course, standard operating processes, budgetary claims made by powerful congressional constituencies, legal constraints, administrative traditions, and institutional cultures. The size and structure of the national security apparatus by default reinforces a propensity for continuity and can therefore often undermine the grand promises of politicians.

As many journalists and scholars have documented, especially in the wake of 9/11, the national security state has inexorably grown, with a base budget increase of more than 50 percent between 2001 and 2016.<sup>12</sup> With that has come an increase in the size of its bureaucracy. That bureaucracy, broadly defined, now includes the Department of Homeland Security and the various intelligence agencies, those responsible for managing the massive growth of government contractors and private security services, and departments specifically created to address new forms of conflict across the entire electromagnetic spectrum (including cyber and space). Pointedly, national security professionals, regardless of their personal views and even any political differences, cannot simply be ignored; they are necessary for policy and strategy implementation. Indeed, they are more valuable than ever in the absence of more than half the number of key appointees. Furthermore, entirely consistent with the classic scholarship on bureaucratic and organizational behavior, their familiarity with ongoing operations and standard operating procedures generally reinforces the strategic status quo rather than radical change, often for fear of the unknown consequences of any major shift.<sup>13</sup> Complete withdrawal from Afghanistan, for example, sounds good on a bumper sticker, but the long-held concern of thereby giving terrorists a base from which to attack the United States suggests otherwise.

President Trump's choice of leadership has reinforced this trend. The incoming leaders of national security departments often arrive intent on instituting dramatic strategic changes. Sometimes they even succeed in some aspects, a notable example being the changes in immigration policy instituted by the Trump administration's Departments of Justice and Homeland Security to date.<sup>14</sup> President Trump chose, however, to install three distinguished career military personnel at the apex of his administration: Lt Gen H. R. McMaster as his second National Security Advisor, Gen James Mattis as secretary of Defense, and Gen John F. Kelly, initially as secretary of Homeland Defense and now chief of staff. Their extensive

and distinguished military careers socialized them to view strategic challenges from a pragmatic, operational perspective rather than a dogmatic one. McMaster's studious personal manner reputedly grated the president, eventually leading to his departure. But if reports are to be believed, President Trump regards Mattis and Kelly as credible and authoritative to the point where he routinely delegates strategy to them.<sup>15</sup> It is not surprising, therefore, to discover that they reputedly favor institutionally and culturally embedded conventions, abjuring many of the president's more radical proposals (as McMaster did) when it comes to force deployment.<sup>16</sup> In effect, they recognize the contextual factors that operate in differing theaters of war—such as Secretary Mattis' insistence on sustaining troop deployments in Eastern Europe—that often reinforce the propensity for continuity.<sup>17</sup> Commentators, such as George Will, expressed an early concern that Trump's third national security advisor, John Bolton, may adopt a more aggressive approach to force deployment.<sup>18</sup> At this point, however, there is no evidence by which to measure the relationship between Bolton's fiery rhetoric and his prescriptions when it comes to deployments. Time will tell if Bolton will be willing and able to impose new deployment patterns on both his more cautious colleagues and a possibly recalcitrant bureaucratic apparatus.

Thus, while sounding a cautious note, the available evidence to date has generated an ironic paradox in President Trump's case. The vacuum created by his administration's lack of senior appointments, coupled with the training of many of those he has appointed to leadership roles, has collectively reinforced the natural tendency to be circumspect in instigating any major operational changes.

### **From Top-Down to Bottom-Up in the Calibration of Military Operations**

In effect, our approach reverses the focus of analysis usually employed by scholars, politicians, and many pundits: from the deductive, top-down approach inherent in most discussions of national security (reflected in the most recent *National Security Strategy* and *National Defense Strategy*) to a bottom-up one that examines what the US military does on a daily basis. High-profile debates aside, operations are calibrated to deal with local conditions and continuity is reinforced by domestic constraints.<sup>19</sup>



Such an approach clearly has its advocates. Senior military leaders like calibrated approaches because they often correspond to what combatant commanders tell them needs to be done. Bureaucrats in Washington like calibrated approaches because they generally conform to the standard operating procedures used in the Pentagon when the military encounters specific challenges—and are thus the default position when faced with the jostling and infighting common to Washington. And despite their best efforts, political leaders often abandon their commitment to their chosen electoral promises and succumb to the need to address a problem this way because of the exigencies of responding to a vocal media and an anguished public about an imminent threat.

Strategy is distinct from policy, and both are distinct from field operations. What we describe links both to military operations: what the military, diplomats, and senior policy makers do rather than what politicians say or what official documents, spokespeople, or even public statements claim. Our view is that, given the often-contradictory statements of President Trump and his closest staff members, it is important to ignore the tweets and focus on how operational imperatives constrain the strategic choices of the president and other senior policy makers. Actions speak far louder than words—and the deployment of resources portrays those actions.

Admittedly, 12 months is a relatively limited timeframe on which to evaluate the new administration's record. But from our perspective, it is not surprising to read headlines such as "Trump Embraces Pillars of Obama's Foreign Policy,"<sup>20</sup> "Trump's 'Secret Plan' to Defeat ISIS Looks a Lot Like Obama's,"<sup>21</sup> "Clinton and Obama Laid the Groundwork for Donald Trump's War on Immigrants,"<sup>22</sup> or, as we discuss below, the suggestion that "Trump's Afghanistan Strategy Is Simply Old Wine in a New Bottle."<sup>23</sup> Certainly, there are individual foreign policy decisions that rise to the level of categorical and profound changes, like the decision to withdraw from the Paris Climate Change Agreement. But we argue it is hard to find evidence of any major shifts in military operations. And when they occur, those shifts are driven more by changes in the actors, threats, and potential form of warfare than by the president's preferences.

In the brief examples that follow, we illustrate our claims of a surprising propensity for continuity when it comes to core deployments despite President Trump's avowed pledge to reverse Obama's approach.

Our examples are clearly not comprehensive. But they share important qualities. First, we examine three of the most prominent national security disputes in the last year. Second, they are all cases where candidate Trump promised radical change but then, as president, he subsequently admitted that “it’s complicated.” And finally, they are cases that are of the greatest security concern to national security scholars, the administration, and the public, involving the issues of terrorism and nuclear conflict.<sup>24</sup>

### **Combating the Islamic State in Syria and Iraq**

The Obama administration’s approach to the fight against IS was a strategy of sponsorship, often derided as “leading from behind.” This approach generally entails the United States abdicating a leadership role while bolstering and subsidizing allies who share America’s interests and are motivated to implement them.<sup>25</sup> President Obama self-consciously—and at some political cost—resisted calls for greater engagement. Notably, he reneged on his threat to take the initiative and launch a military offensive if the Assad regime in Syria continued to use chemical weapons against civilians. But consistent with a sponsorship strategy, the new administration did logistically support the Kurds, Iraqi government forces, and various rebel groups in Syria in their general campaign to repel IS and Assad in both countries, even as Kurdish involvement raised the ire of Turkey, America’s NATO ally.

In practice, the US contribution under Obama was largely limited to providing materiel and training while standing by with airpower, providing intelligence and, on occasion, forward support to these proxy forces. This strategy saved American lives and helped avoid the messy domestic politics of again escalating the US role in the region. Conversely, of course, it also exposed Obama to accusations of inaction and inconstancy in the struggle against the Islamic State.

As a candidate, Trump excoriated President Obama, claimed that Hillary Clinton would continue this strategy, and claimed to have a “secret plan” to destroy IS.” More remarkably, the candidate vowed “I would bomb the s\*\*\* out of them.”<sup>26</sup> In that vein, the new administration’s early decisions were well publicized. The Trump administration instituted a policy shift by loosening the rules of engagement to allow larger and more risky strikes in Syria, effecting the one possible area of operational change. It also initially appeared markedly more open to col-

laborating with Russia to address the Syrian war, before later launching air strikes against an airfield used by the Assad regime and shooting down a Syrian MIG, actions that led to fears of direct conflict with Russian forces.

Administratively, a key decision by President Trump was that the formulation and supervision of operational strategy (and related troop levels) would be delegated to the military command, whether a sign of Trump's faith in Mattis, intended to dampen some of the initial infighting amongst his national security and political aides, or as a way of politically distancing himself from any responsibility if things eventually go awry. Civilian leadership had maintained a tight control over military strategy in the two prior administrations. But in the Trump administration the locus of decision making has firmly shifted to the military, generating attendant fears of an abrupt change in strategy and thus operations.

From our perspective, however, the key question concerns whether these policy and potential strategic shifts have resulted in major operational changes. Yes, the Trump administration has undertaken several high-profile military strikes in Syria and employed harsher rhetoric about destroying the Islamic State, which is fairly easy to do given the IS retreat throughout 2017. Yet, any operational changes have been nominal. As one commentator suggested, Trump "mainly accelerated a battle plan developed by President Obama."<sup>27</sup> There has been no large-scale recommitment of US forces. Instead, just as during the Obama administration, the fighting against IS has predominantly been left to proxies, including Kurds, rebel forces in Syria, and what passes for central government troops and militias in Iraq. As before, the US contributes training, logistics, intelligence, and occasional air strikes. It is not a frontline state in either theater, and there are no tangible signs to date that it intends to become one. The theaters where the battle against IS will be won or lost have been fought without a significant American presence.<sup>28</sup>

Developments in the summer of 2017 suggested that the American-led coalition may be "nearing the endgame with ISIS."<sup>29</sup> Bryan McGurk, the special presidential envoy for the Global Coalition to Counter IS (a rare appointment by Obama retained by President Trump<sup>30</sup>), argued that the changes in approach authorized by President Trump have "dramatically accelerated" the demise of IS.<sup>31</sup> But these strategic and policy changes—more autonomy for local commanders and increased burden

sharing with international stakeholders—appear to have resulted in few operational changes.

This continuity works in diametrically opposed ways in terms of either possible “proclaimed” strategy. As far as is publicly known, the administration has no plans to de-escalate the anti-IS fight, as might be expected from “America First” rhetoric. Nor, on the other hand, has it undertaken new military, diplomatic, political, or economic initiatives that might result in differing or greater deployments on the ground, as might be expected from a more muscular or primacist approach to countering terrorism. Rather, adjustments to the strategy and operations initiated by Obama have borne fruit under President Trump, who in claiming victory nonetheless put his own spin on counterterror operations.<sup>32</sup> But the evidence suggests that little has altered in terms of trajectory.

### **Doubling Down on Afghanistan**

The United States launched Operation Enduring Freedom against the Taliban and those al-Qaeda members sheltering in Afghanistan under the Taliban’s protection weeks after the 9/11 attacks. The American strategy was consistent with a liberal one of multilateral leadership of NATO forces, with the goal of conquest and reconstruction. In the words of Barack Obama, George W. Bush’s “good war” eventually became a “forever” one, with his promise of a complete withdrawal being overtaken by circumstances.<sup>33</sup> The logic for continued engagement in Afghanistan is simple and apparently compelling for American strategists. Daniel Byman and Will McCants offer a critical assessment while helping to locate the Afghan conflict within the wider context of US global counterterrorism efforts: “Fear of safe havens and the politics that undergird it are misplaced. Safe havens can be dangerous, and at times it is vital for the United States to use force, even massive force, to disrupt them. Yet not all safe havens—and not all the groups in the havens—are created equal.”<sup>34</sup>

In a world of unequal safe havens, Afghanistan has proven itself to be an exceptionally problematic one for American strategists. Withdrawal has become inconceivable as long as the threat of a Taliban resurgence is tangible. And the existence of a continued threat is undeniable, with tangible costs. In the past 16 years, more than 2,300 Americans have been killed and over 17,000 wounded. Yet neither the US, its NATO allies, nor the Afghan government has been able to defeat the Taliban or

allied Islamist forces. Subjugation has always been temporary, followed by resurgence.

As a private citizen, long before he began campaigning for the Republican presidential nomination, Donald Trump largely ignored this logic. He explicitly favored jettisoning a multilateral leadership strategy in favor of one of retrenchment when he tweeted, “We have wasted an enormous amount of blood and treasure in Afghanistan. Their government has zero appreciation. Let’s get out!”<sup>35</sup>

But that abrupt change in strategy has not materialized. Secretary Mattis set the stage for a continuation in America’s “forever war” strategy when he acknowledged in testimony before the Senate Armed Services Committee that “we are not winning in Afghanistan, right now, and we will correct this as soon as possible.”<sup>36</sup> And four months into the new administration, McMaster, who served in Afghanistan, and Mattis advocated committing an additional 3,000–5,000 American troops.<sup>37</sup> Notably, such figures would not be enough to destroy the Taliban and its allies but perhaps might be enough to staunch further losses, signaling little discernable shift in strategy from the Obama administration.

The future of US involvement in Afghanistan depends on the implementation of the general “South Asia Strategy” review commissioned by Mattis. It included changes in tactics within Afghanistan (more trainers and higher troop limits), greater pressure being exerted against Pakistan to stop any support for terrorist groups, and closer relations with India as a regional counterweight to both Pakistan and China.<sup>38</sup> Most publicly, and perhaps surprisingly, Mattis revealed before the Senate Armed Services Committee that US forces are operating under more aggressive rules of engagement: “You see some of the results of releasing our military from, for example, a proximity requirement—how close was the enemy to the Afghan or the U.S.-advised Special Forces.”<sup>39</sup> As a result, new reports suggest that “U.S. forces are no longer bound by requirements to be in contact with enemy forces in Afghanistan before opening fire.”<sup>40</sup> But the only tangible effect of any change to date has been an increase in the number of civilian casualties—reputedly rising by more than 50 percent—to record levels, as a result of the administration’s policy change.<sup>41</sup> That’s because, as a practical matter, while the reputed increase in the actual number of US troops on the ground has not been substantial (from 11,000 to 14,000), the increase in air strikes has been.<sup>42</sup> In September 2017, the United States conducted 751 air-

strikes in Afghanistan, a 50 percent increase over August's figures.<sup>43</sup> As always in counterinsurgency operations and civil wars, specialists endlessly debate whether it is possible to kill one's way to victory. The new administration has made it marginally easier to strike enemies from the air but not, yet, found a comparable foundation for a military victory or lasting political settlement. Operationally, in effect, the new administration has done more of the same.

Indeed, it appears that the administration's comprehensive position largely echoes the Afghanistan-Pakistan (AFPAK) strategy associated with Richard Holbrooke and announced 27 March 2009 by the Obama administration. As then-national security advisor Gen James Jones briefed, "The cornerstone of this strategy, I think, is that it's a regional approach. And for the first time, we will treat Afghanistan and Pakistan as two countries, but . . . with one challenge in one region."<sup>44</sup> It also coincided with a surge (a la 2007 Iraq<sup>45</sup>) of American troops and, given the Obama administration's preference for multilateralism, increased troop contributions to the International Security Assistance Force (ISAF) from other NATO members.<sup>46</sup> The surge, of course, resulted in greater presence and a larger number of kinetic operations. President Obama did eventually de-emphasize the term AFPAK in 2010 because it was deeply unpopular with Pakistan.<sup>47</sup> But many academics, military experts, and government officials recognized the importance of thinking in broad, multifaceted regional terms in combating insurgents and terrorists in South Asia.<sup>48</sup> Secretary Mattis has offered the same.

President Trump undoubtedly faces the same domestic pressures to remain tough on terrorism faced by his predecessors. As such, the United States currently leads a coalition capable of propping up the Afghan central government and periodically sortieing against jihadists. The forever war in Afghanistan will likely continue indefinitely, with the United States sharing the burdens with NATO and local allies, even as political leaders preach an America First strategy.<sup>49</sup> Despite the end of the ISAF combat operations mission in 2014, NATO Secretary General Jens Stoltenberg is considering a request from Gen John Nicholson, commander of US Forces Afghanistan, to commit more forces from non-American members. The new troops will join NATO's Resolute Support mission to, in words predating President Trump's inauguration, "provide further training, advice and assistance for the Afghan security forces and institutions."<sup>50</sup>

On 20 August 2017, President Trump delivered a major policy speech on the way ahead for American involvement. In it, the president acknowledged his longstanding criticisms of his predecessors before offering two major adjustments: a “shift from a time-based approach to one based on conditions” and “the integration of all instruments of American power—diplomatic, economic, and military—toward a successful outcome.”<sup>51</sup> As many critics have suggested, neither adjustment seems transformational nor likely to improve the prospects of stabilizing Afghanistan.<sup>52</sup> Rather, the new administration appears to be traveling down a well-trodden road. As President Trump conceded in a *New York Times* interview when discussing Afghanistan, “My original instinct was to pull out . . . and, historically, I like following my instincts. But all my life I’ve heard that decisions are much different when you sit behind the desk in the Oval Office.”<sup>53</sup> It remains to be seen whether the reintroduction of these 3,500 troops will change the dynamic of the last 16 years.<sup>54</sup>

### **North Korea and the Game of Nuclear Chicken**

Long-standing tensions with North Korea (DPRK), dating to the 1953 armistice ending the Korean War, flared even before President Trump assumed office. As president-elect, apparently in response to provocative statements by Supreme leader Kim Jong Un, he tweeted that “North Korea just stated that it is in the final stages of developing a nuclear weapon capable of reaching parts of the U.S. It won’t happen!”<sup>55</sup> News accounts had suggested that, having offered a barrage of increasingly incendiary ballistic missile tests and defiant language over the past 12 months, North Korea was planning further tests and to restart its Yongbyon plutonium reactor.<sup>56</sup> North Korea’s technological advances have been impressive. And the tests themselves have often been confrontationally timed, beginning in February 2017, when North Korea tested the Pukguksong-2, reportedly a solid-fueled, medium-range system, while Mattis was on his first official tour of Asia as the newly appointed secretary of defense. This pattern continued. By the end of the first year of the Trump administration, “Pyongyang ha[d] successfully tested two different types of intercontinental ballistic missiles, a new intermediate-range ballistic missile, a solid-fuel missile based off a submarine-launched design, and its most powerful nuclear device.”<sup>57</sup>

President Trump had offered inconsistent positions on the North Korea nuclear program when a private citizen and then a presidential candi-

date. Almost two decades ago he appeared to favor a preemptive strike against the regime. But on the campaign trail he mused that China should take care of the problem and/or Japan should develop its own nuclear weapons.<sup>58</sup>

In contrast to these shifts in position, his approach in the opening months of his administration remained consistent. He was quick to threaten military action and quick to resist calls, both from inside his administration and from the international community, to attempt further diplomacy to achieve a political solution (although subsequently, by March 2018, the prospect of Trump meeting with Kim Jong Un was raised as an option). Furthermore, the president pressured allies to both condemn the Kim regime and impose stronger sanctions on the North Korean government and its key leaders.<sup>59</sup>

The crisis escalated not simply because of the North Korean missile tests and inflammatory language but also because of President Trump's public responses. One notable example was his claim in an interview with Fox Business News that "we are sending an armada. Very powerful. We have submarines, very powerful, far more powerful than an aircraft carrier, that I can tell you."<sup>60</sup> McMaster made clear in an interview that "all our options are on the table," although he also emphasized that he hoped there would not be a need for military action.<sup>61</sup> And Trump's own senior military leadership argued that a ground invasion would be required to eliminate the prospects of a nuclear attack but was not feasible, in part because of the enormous cost it would entail in terms of South Korean civilian casualties—reinforcing what his predecessors had learned over the last two decades.<sup>62</sup>

The Trump administration has also undertaken a wide variety of military operational responses. Specifically, it initiated several demonstrations of power, including a rare multilateral exercise involving three aircraft carriers: the USS *Ronald Reagan*, the USS *Nimitz*, and the USS *Theodore Roosevelt*. The exercises, which included elements of the Japanese Maritime Self Defense Force and the South Korean navy, was officially intended to "conduct air defense drills, sea surveillance, replenishments at sea and other training in international waters."<sup>63</sup> In a speech while visiting South Korea, President Trump himself made his main point clear: "We sent three of the largest aircraft carriers in the world and they're now positioned. We have a nuclear submarine, we



have many things happening that we hope—we hope to God we never have to use.”<sup>64</sup>

In addition to a military demonstration of offensive power, the Trump administration hastened deployment of the terminal high altitude defense (THAAD) missile defense system to South Korea. In theory, it could provide a modest level of defense against the DPRK's large number of intermediate missiles. But this move itself generated controversy. News reports suggest that South Korean citizens believe the THAAD deployment signifies that the Trump administration is preparing for a preemptive attack.<sup>65</sup> Moreover, in an incident highlighting the tensions between crisis management and the administration's unilateralism, many South Korean were offended by President Trump's off-the-cuff suggestion that South Korea should pay \$1 billion for the system's deployment. Amid protests in South Korea, on 30 April 2017, McMaster reaffirmed the details of an earlier agreement on THAAD in which South Korea bore no financial burden.<sup>66</sup>

In North Korea, the Trump administration confronts a state actor armed with a large conventional military and a growing array of ballistic missiles capable, once engineering and operational challenges are resolved, of carrying nuclear warheads and reaching key treaty allies like Japan and now, potentially, American territory in Guam and the mainland. A preemptive strike involving American forces, of dubious legality under international law unless an attack was deemed imminent, is one of the military options under discussion.<sup>67</sup> Indeed, administration officials including the president and then-Secretary of State Rex Tillerson have indicated that, in Tillerson's words, “If they elevate the threat of their weapons program to a level that we believe requires action then that [military] option is on the table.”<sup>68</sup>

Journalists and former Obama administration officials have publicly suggested that some Trump officials, part of an informal “war party,” are advocating limited attacks sometime in 2018.<sup>69</sup> These officials argue that the character of the North Korean threat has swiftly changed. The first, most prominent factor is the DPRK's rapid upgrading of new missile and nuclear technology. The second is the increased volubility, and now feasibility, of their threats against the American homeland. While North Korea's leadership has threatened the US before, its existential character is novel.<sup>70</sup> Yet, the specific challenges facing US or allied forces in taking offensive action against North Korea remain unchanged. As Tom Ricks

reminded us, the United States has been preparing for a North Korean military crisis since the cease-fire concluded the Korean War—and preparing intensively since Pyongyang threatened military action over 20 years ago.<sup>71</sup> North Korea's conventional forces, while out-of-date and, in some cases, poorly maintained, are formidable. The Council on Foreign Relations summarizes the weapons systems maintained by the North Korean 1.1 million-man armed forces as having “more than 1,300 aircraft, nearly 300 helicopters, 430 combatant vessels, 250 amphibious vessels, 70 submarines, 4,300 tanks, 2,500 armored vehicles, and 5,500 multiple-rocket launchers. Experts also estimate that North Korea has upwards of one thousand missiles of varying ranges.”<sup>72</sup> Perhaps most importantly, even if North Korea cannot yet reach the American mainland with nuclear armed warheads,<sup>73</sup> its nuclear weapons pose threats to American forces (not to mention allies) in theater, some accounts suggest it may possess biological and chemical weapons, and cyberattacks attributed to North Korean actors have disrupted commerce and could do so again.<sup>74</sup>

President Trump's retaliatory threats invoking “fire and fury” against an enemy (the DPRK) and criticism of an ally (South Korea) may not have helped.<sup>75</sup> Indeed, it might have been tactically naïve, as some critics contend, because it has boxed the United States into an unfavorable position with regard to future negotiations.<sup>76</sup>

Nonetheless, to suggest that any operational changes are a product of President Trump's ill-judged statements is mistaken. That is because, when it comes to military operations related to the current North Korean crisis and preparations for a potential war, it is hard to argue that either President Bush or President Obama could have done much else under these circumstances.<sup>77</sup> Obama's efforts with Iran suggest he might well have first tried to negotiate. But his offers to talk to the DPRK when they conducted cyber hacking and espionage operations did not prove notably more effective.<sup>78</sup> Furthermore, it is hard to argue that the changing military circumstances—a growing existential threat coupled with virulent rhetoric from Kim Jong Un—would not dictate the installation of THAAD missile systems and the assemblage of what President Trump referred to as a powerful “armada,” regardless of who was president.<sup>79</sup> Any operational changes therefore represent the culmination of a long-held position and have been prompted more by dynamic local conditions than any major shift. America has adopted a deterrent military strategy

against North Korea for six decades. The current conflict is its latest manifestation of that strategy. Rhetoric aside, by the early months of 2018, it is therefore hard to imagine an alternative operational response.

### **President Trump and Future Military Operations?**

On 19 January 2018, Mattis presented to the public an unclassified summary of the Trump administration's long-awaited *National Defense Strategy*, the DOD's counterpart to the National Security Council's *National Security Strategy* released in December 2017.<sup>80</sup> It clarified some but not all of the outstanding questions regarding the administration's broad strategy.<sup>81</sup> On the one hand, it confirmed the *NSS* focus on preparing for great power competition; on the other, it left unresolved how the United States military would extricate itself from Afghanistan, Syria, and Iraq. Further, while the *NDS* summary argues that "[e]ffectively expanding the competitive space requires combined actions with the U.S. interagency to employ all dimensions of national power," it remains silent on how this will be successful given budgetary limits on foreign operations spending.


The new *NDS* has already provided more fodder for academics, pundits, and the media.<sup>82</sup> So has Trump's replacement of senior appointees with more hawkish officials like Pompeo at State and Bolton as national security advisor. But neither the new document nor the new appointments are likely, at least in the short run, to substantially alter the military's implementation of any overarching American national security strategy. To understand whether the Trump *NDS* has altered US strategic behavior, commentators will have to analyze military operations rather than speeches, outbursts on social media, or even planning documents. Given the evidence of the first 12 months of the Trump administration, we expect that any such analysis will reveal far more continuity with the recent past than many expected from a president who relentlessly criticized the choices of his predecessors and called for radical change.

We do not suggest that operational change cannot occur. It can and does. The admixture of shifts in the external environment and even possibly the relentless pursuit of preferences among domestic leaders can eventually overcome bureaucratic inertia. Furthermore, the increase in resources and eventually military capabilities may contribute to change, especially when any threat's scope rapidly increases.

Yet the evidence to date regarding this administration is significant and possibly generalizable: even those that promise and pursue acute shifts in operations encounter the constraints imposed by the theater of war. The Afghan and IS conflicts have evolved incrementally over several years. Little fundamentally has changed on the ground since President Trump took office. The North Korean case has done so more rapidly, even though Mattis conceded that the new North Korean ICBMs have “not yet shown to be a capable threat against us right now.”<sup>83</sup> In each case, within reasonable parameters, the requisites of military operations now largely generally mirror those of President Trump’s predecessors. Even the acceleration in deployments we note in the North Korean case is consistent with the historical trajectory. As Jacqueline Klimas suggests, despite all this pre-positioning of military resources, President Trump’s approach to North Korea to date still looks a lot like President Obama’s, a mixture of deployments and offers to negotiate.<sup>84</sup> Of course, the crisis is taking place with North Korea as we write in early 2018. It could abate or escalate at any point. Miscalculation or arrogance could trigger a military conflict verging from military skirmishes to the truly catastrophic.

No doubt, broader changes in the external environment, further replacements in cabinet-level leadership, and even congressional politics will help reshape strategic documents such as the *National Security Strategy*, the *National Defense Strategy*, and the *Nuclear Posture Review* over the lifetime of the Trump administration. There are already signs of an emerging Trumpian grand strategy that focuses on strategic competition with revisionist great powers—Russia and China—and “rogue” states—North Korea and Iran. But as we have argued elsewhere, “in the absence of radical changes in culture, institutional decision-making and in resources . . . the United States will muddle along, pursuing calibrated strategies by default, despite the intellectual effort and ink spilled in an effort to develop a coherent grand strategy.”<sup>85</sup>

Nonetheless, the nature of the adversaries, the character of the threats, and the potential forms of conflict themselves, varying in different regions of the globe, will determine what military operations are possible given the capabilities available to combatant commanders. To an extent alarming to his supporters and consoling to his critics, the evidence to date suggests that President Trump’s military leadership has adopted, and will continue to adopt, what President Obama disparagingly referred to

as “the Washington Playbook”—notably the propensity to pursue “militarized responses”—when it comes to facing national security challenges. The United States, furthermore, is likely to continue to do so in the foreseeable future.<sup>86</sup> 

## Notes

1. Cf. the comments of Stephen Hadley, former National Security Advisor, “Is Trump’s Foreign Policy Descending into Chaos,” MSNBC, 2 February 2017, <https://www.msnbc.com/mtp-daily/watch/is-trump-s-foreign-policy-descending-into-chaos-868859459603>; Susan B. Glasser, “Donald Trump’s Year of Living Dangerously,” *Politico Magazine*, January/February 2018, <https://www.politico.com/magazine/story/2018/01/02/donald-trump-foreign-policy-analysis-dangerous-216202>; and Adam Taylor, “Ditching Deals Has Become Trump’s Main Foreign Policy,” *Washington Post*, 13 October 2017, [https://www.washingtonpost.com/news/worldviews/wp/2017/10/13/ditching-deals-has-become-trumps-main-foreign-policy/?utm\\_term=.c16620d236bc](https://www.washingtonpost.com/news/worldviews/wp/2017/10/13/ditching-deals-has-become-trumps-main-foreign-policy/?utm_term=.c16620d236bc).

2. Jonathan Swan, “Scoop: Trump Approves National Security Strategy,” *Axios*, 3 December 2017, <https://www.axios.com/scoop-trump-approves-national-security-strategy-2514637164.html>.

3. Josh Delk, “McMaster: Trump’s Foreign Policy Approach Is Out of my ‘Comfort Zone,’” *The Hill*, 28 December 2017, <http://thehill.com/blogs/blog-briefing-room/366731-mcmaster-trumps-foreign-policy-approach-is-out-of-my-comfort-zone>.

4. Cf. Max Fisher, “Trump’s Military Ambition: Raw Power as a Means and an End,” *New York Times*, 3 March 2017, <https://www.nytimes.com/2017/03/03/world/americas/donald-trump-us-military.html?smprod=nytcore-ipad&smid=nytcore-ipad-share>; Colin Kahl and Hal Brands, “Trump’s Grand Strategy Train Wreck,” *Foreign Policy*, 31 January 2017, <https://foreignpolicy.com/2017/01/31/trumps-grand-strategic-train-wreck/>; Stephen M. Walt, “America’s New President Is not a Rational Actor,” *Foreign Policy*, 25 January 2017, <http://foreignpolicy.com/2017/01/25/americas-new-president-is-not-a-rational-actor/>; David Rothkopf, “Trump’s Pox Americana,” *Foreign Policy*, 26 January 2017, <http://foreignpolicy.com/2017/01/26/trumps-pox-americana-the-retreat-of-the-indispensable-nation/>; and Frank Hoffman, “The Case for Strategic Discipline during the Next Presidency,” *War on the Rocks*, 10 January 2017, <https://warontherocks.com/2017/01/the-case-for-strategic-discipline-during-the-next-presidency/>.

5. See, respectively, Micah Zenko and Rebecca Friedman Lissner, “Trump Is Going to Regret Not Having a Grand Strategy,” *Foreign Policy*, 13 January 2017, <http://foreignpolicy.com/2017/01/13/trump-is-going-to-regret-not-having-a-grand-strategy/>; Stephen Sestanovich, “The Brilliant Incoherence of Trump’s Foreign Policy,” *The Atlantic*, May 2017, <https://www.theatlantic.com/magazine/archive/2017/05/the-brilliant-incoherence-of-trumps-foreign-policy/521430/>; Leon Hadar, “The Limits of Trump’s Transactional Foreign Policy,” *National Interest*, 2 January 2017, <http://nationalinterest.org/feature/the-limits-trumps-transactional-foreign-policy-18898>; Dan De Luce, “Trump Sticks to a Protectionist, Isolationist Script in First Big Speech,” *Foreign Policy*, 1 March 2017, <http://foreignpolicy.com/2017/03/01/trump-sticks-to-a-protectionist-isolationist-script-in-first-big-speech/>; and Walter Russell Mead, “The Jacksonian Revolt: American Populism and the Liberal Order,” *Foreign Affairs*, March/April 2017, <https://www.foreignaffairs.com/articles/united-states/2017-01-20/jacksonian-revolt>.

6. For details on confirmations, see “Tracking How Many Key Positions Trump Has Filled so Far,” *Washington Post*, last updated 7 March 2018, [https://www.washingtonpost.com/graphics/politics/trump-administration-appointee-tracker/database/?tid=a\\_inl&utm\\_campaign=New%20Campaign&utm\\_medium=email&utm\\_source=Sailthru](https://www.washingtonpost.com/graphics/politics/trump-administration-appointee-tracker/database/?tid=a_inl&utm_campaign=New%20Campaign&utm_medium=email&utm_source=Sailthru).

7. Office of the President, *National Security Strategy of the United States* (Washington, DC: The White House, December 2017), 40, 45, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

8. Cf. C. Eugene Emery Jr., “Joe Biden Wrong to Say Donald Trump Has Called for Carpet Bombing,” *Politifact*, 2 August 2016, <http://www.politifact.com/truth-o-meter/statements/2016/aug/02/joe-biden/joe-biden-wrong-say-donald-trump-has-called-carpet/>.

9. The theme of this section is developed in our book, Simon Reich and Peter Dombrowski, *The End of Grand Strategy: U.S. Maritime Operations in the Twenty-First Century* (Ithaca, NY: Cornell University Press, forthcoming 2018), 13–27.

10. Cf. the variety of threats listed in the *National Security Strategy of the United States 2015* (Washington, DC: The White House, February 2015), [https://obamawhitehouse.archives.gov/sites/default/files/docs/2015\\_national\\_security\\_strategy\\_2.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf).

11. Colin S. Gray, “How Has War Changed since the End of the Cold War?,” *Parameters* (Spring 2005): 14–26, <http://ssi.armywarcollege.edu/pubs/parameters/articles/05spring/gray.htm>. The discussion emphasizes that while in the post–Cold War period “war, let alone ‘decisive war,’ between major states currently is enjoying an off-season,” it will return once the disparity in military power between the United States and its great power competitors diminishes.

12. See, for example, among many others, David Rothkopf, *National Insecurity: American Leadership in an Age of Fear* (New York: Public Affairs, 2014); and Michael J. Glennon, *National Security and Double Government* (London: Oxford University Press, 2014). For figures, see “Defense Spending Chart,” US Government Spending, accessed 8 March 2018, [http://www.usgovernmentpending.com/spending\\_chart\\_2000\\_2016USb\\_18s2li111mcn\\_30t\\_30\\_Defense\\_Spending\\_Chart](http://www.usgovernmentpending.com/spending_chart_2000_2016USb_18s2li111mcn_30t_30_Defense_Spending_Chart).

13. See new editions of such classics as Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. (New York: Pearson, 1999); Priscilla Clapp and Morton Halperin with Arnold Kanter, *Bureaucratic Politics and Foreign Policy*, 2nd ed. (Washington, DC: Brookings Institution Press, 2006); and Roger Hilsman, *The Politics Of Policy Making In Defense and Foreign Affairs: Conceptual Models and Bureaucratic Politics*, 3rd ed. (Saddle River, NJ: Prentice Hall, 1993). Other important contributions include Jerel A. Rosati, “Developing a Systematic Decision-Making Framework: Bureaucratic Politics in Perspective,” *World Politics* 33, no. 2 (January 1981): 234–52, <http://www.jstor.org/stable/2010371>; Daniel W. Drezner, “Ideas, Bureaucratic Politics, and the Crafting of Foreign Policy,” *American Journal of Political Science* 44, no. 4 (October 2000): 733–49, <http://www.jstor.org/stable/2669278>; and Barry R. Posen, “The Sources of Military Doctrine,” in *Military Power and International Politics*, 8th ed., ed. Robert J. Art and Kelly M. Greenhill (Lanham, MD: Rowman and Littlefield, 2009), 28–45.

14. For a discussion of this point, see Peter Dombrowski and Simon Reich, “Does Donald Trump Have a Grand Strategy?” *International Affairs* 93, no. 5 (September 2017): 1023–26, <https://doi.org/10.1093/ia/iix161>.

15. Cf. Missy Ryan, Philip Rucker, and Thomas Gibbons-Neff, “Among Trump Aides, Mattis Emerges as a Key Voice on National Security Issues,” *Washington Post*, 28 April 2017, [https://www.washingtonpost.com/world/national-security/among-trump-aides-mattis-emerges-as-a-key-voice-on-national-security-issues/2017/04/28/3c9f0760-25ea-11e7-a1b3-faff0034e2de\\_story.html?tid=ss\\_mail&utm\\_term=.d67266355d3f](https://www.washingtonpost.com/world/national-security/among-trump-aides-mattis-emerges-as-a-key-voice-on-national-security-issues/2017/04/28/3c9f0760-25ea-11e7-a1b3-faff0034e2de_story.html?tid=ss_mail&utm_term=.d67266355d3f); and Dexter Filkins, “James

Mattis, A Warrior in Washington," *New Yorker*, 29 May 2017, <http://www.newyorker.com/magazine/2017/05/29/james-mattis-a-warrior-in-washington>.

16. Cf. Max Fisher, "Stephen K. Bannon's CPAC Comments, Annotated and Explained," *New York Times*, 24 February 2017, [https://www.nytimes.com/2017/02/24/us/politics/stephen-bannon-cpac-speech.html?\\_r=0](https://www.nytimes.com/2017/02/24/us/politics/stephen-bannon-cpac-speech.html?_r=0).

17. Cf. Jim Garamone, "Mattis Pleased with NATO Progress Deterring Russia, Combating Terror," *Defense.gov*, 29 June 2017, <https://www.defense.gov/News/Article/Article/1234053/>; and Ewen MacAskill, "Russia Is a 'Strategic Competitor' to the West, Says James Mattis," *The Guardian*, 31 March 2017, <https://www.theguardian.com/world/2017/mar/31/russia-strategic-competitor-to-west-james-mattis>.

18. George F. Will, "The Second Most Dangerous American," *Washington Post*, 23 March 2018, [https://www.washingtonpost.com/opinions/the-second-most-dangerous-american/2018/03/23/90751d80-2ec6-11e8-8688-e053ba58f1e4\\_story.html?utm\\_term=.5e0150a9fd1d](https://www.washingtonpost.com/opinions/the-second-most-dangerous-american/2018/03/23/90751d80-2ec6-11e8-8688-e053ba58f1e4_story.html?utm_term=.5e0150a9fd1d).

19. Reich and Dombrowski, *End of Grand Strategy*.

20. Mark Landler, Peter Baker, and David E. Sanger, "Trump Embraces Pillars of Obama's Foreign Policy," *New York Times*, 2 February 2017, <https://www.nytimes.com/2017/02/02/world/middleeast/iran-missile-test-trump.html>.

21. Brian P. McKeon, "Trump's 'Secret Plan' to Defeat ISIS Looks a lot like Obama's," *Foreign Policy*, 31 May 2017, <http://foreignpolicy.com/2017/05/31/trumps-secret-plan-to-defeat-isis-looks-a-lot-like-obamas/>.

22. Aviva Chomsky, "Clinton and Obama Laid the Groundwork for Donald Trump's War on Immigrants," *The Nation*, 25 April 2017, <https://www.thenation.com/article/clinton-and-obama-laid-the-groundwork-for-donald-trumps-war-on-immigrants/>.

23. Michael Kugelman, "Trump's Afghanistan Strategy Is Simply Old Wine in a New Bottle," *National Interest*, 16 July 2017, <http://www.nationalinterest.org/feature/trumps-afghanistan-strategy-simply-old-wine-new-bottle-21549>.

24. For some recent polling, see Andrew Arengue, Hannah Hartig, and Stephanie Perry, "NBC News Poll: American Fears of War Grow," *NBC News*, 18 July 2017, <https://www.nbcnews.com/politics/national-security/nbc-news-poll-american-fears-war-grow-n783801>.

25. Peter Dombrowski and Simon Reich, "The Strategy of Sponsorship," *Survival: Global Politics and Strategy*, 57, no. 5 (October–November 2015): 121–148, <http://doi.org/ck8c>.

26. Tim Lister, "Is Bombing the S\*\*\* out of ISIS a Strategy?," *CNN*, 15 November 2016, <http://www.cnn.com/2016/11/15/middleeast/donald-trump-isis-strategy/index.html>.

27. Linda Qiu, "Can Trump Claim Credit for a Waning Islamic State?" *New York Times*, 17 October 2017, <https://www.nytimes.com/2017/10/17/us/politics/trump-islamic-state-raqqa-fact-check.html>.

28. Michael R. Gordon, "In a Desperate Syrian City, a Test of Trump's Policies," *New York Times*, 1 July 2017, <https://www.nytimes.com/2017/07/01/world/middleeast/syria-raqqa-tabqa.html>.

29. Robin Wright, "Are We Nearing the Endgame with ISIS?," *New Yorker*, 27 July 2017, <https://www.newyorker.com/news/news-desk/are-we-nearing-the-endgame-with-isis>.

30. Thomas Gibbons-Neff, "Trump Keeps Obama Appointee Tasked with Helping Run the War against ISIS," *Washington Post*, 19 January 2017, [https://www.washingtonpost.com/news/checkpoint/wp/2017/01/19/trump-keeps-obama-appointee-tasked-with-helping-run-the-war-against-isis/?utm\\_term=.348c516de848](https://www.washingtonpost.com/news/checkpoint/wp/2017/01/19/trump-keeps-obama-appointee-tasked-with-helping-run-the-war-against-isis/?utm_term=.348c516de848).

31. Karen DeYoung, "Under Trump, Gains against ISIS Have 'Dramatically Accelerated,'" *Washington Post*, 4 August 2017, [https://www.washingtonpost.com/world/national-security/under-trump-gains-against-isis-have-dramatically-accelerated/2017/08/04/8ad29d40-7958-11e7-8f39-eeb7d3a2d304\\_story.html?utm\\_term=.773aa591b188](https://www.washingtonpost.com/world/national-security/under-trump-gains-against-isis-have-dramatically-accelerated/2017/08/04/8ad29d40-7958-11e7-8f39-eeb7d3a2d304_story.html?utm_term=.773aa591b188).

32. Cf. Qiu, “Can Trump Claim Credit?”
33. Mark Landler, “The Afghan War and the Evolution of Obama,” *New York Times*, 1 January 2017, [https://www.nytimes.com/2017/01/01/world/asia/obama-afghanistan-war.html?\\_r=0](https://www.nytimes.com/2017/01/01/world/asia/obama-afghanistan-war.html?_r=0).
34. Daniel Byman and Will McCants, “Fight or Flight: How to Avoid a Forever War against Jihadists,” *Washington Quarterly* 40, no. 2 (Summer 2017): 67–77, <http://doi.org/ck8b>.
35. Donald Trump (@realDonaldTrump), “We have wasted an enormous amount of blood and treasure in Afghanistan,” Twitter, 21 November 2013, 12:06 pm, <https://twitter.com/realDonaldTrump/status/403615352338128896>.
36. Phil Stewart and Idrees Ali, “U.S. ‘Not Winning’ in Afghanistan, Defense Secretary Tells Congress,” Reuters, 13 June 2017, <http://www.reuters.com/article/us-usa-afghanistan-idUSKBN1941Y1>.
37. Mark Landler and Eric Schmitt, “Trump Administration Is Split on Adding Troops in Afghanistan,” *New York Times*, 23 May 2017, <https://www.nytimes.com/2017/05/23/world/europe/saudi-arabia-arms-deal-nato.html>.
38. Barbara Starr, “Mattis on New Afghanistan Strategy: ‘We are Pretty Close,’” CNN, 14 July 2017, [www.cnn.com/2017/07/14/politics/trump-thinking-mattis-afghanistan-pakistan/index.html](http://www.cnn.com/2017/07/14/politics/trump-thinking-mattis-afghanistan-pakistan/index.html).
39. Thomas Gibbons, “Mattis Discloses Part of Afghanistan Battle Plan, but It Hasn’t Yet Been Carried Out,” *New York Times*, 6 October 2017, <https://www.nytimes.com/2017/10/06/world/asia/mattis-afghanistan-rules-of-engagement.html>.
40. Aaron Mehta, “Mattis Reveals New Rules of Engagement,” *Military Times*, 3 October 2017, <https://www.militarytimes.com/flashpoints/2017/10/03/mattis-reveals-new-rules-of-engagement/>.
41. Josh Smith, “UN: Civilian Casualties in Afghanistan from US Air Strikes Have Risen more than 50% since Last Year,” Reuters, 12 October 2017, <https://www.reuters.com/article/us-afghanistan-casualties/afghan-civilian-casualties-from-air-strikes-rise-more-than-50-percent-says-u-n-idUSKBN1CH1SZ>.
42. Missy Ryan, “As Advisory Role Grows in Afghanistan, so Does Risk to U.S. Troops,” *Washington Post*, 28 November 2017, [https://www.washingtonpost.com/news/checkpoint/wp/2017/11/28/as-advisory-role-grows-in-afghanistan-so-does-risk-to-u-s-troops/?utm\\_term=.dcd25b25e37f](https://www.washingtonpost.com/news/checkpoint/wp/2017/11/28/as-advisory-role-grows-in-afghanistan-so-does-risk-to-u-s-troops/?utm_term=.dcd25b25e37f).
43. Harriet Sinclair, “Trump’s Military Dropped 751 Bombs on Afghanistan in September, Highest Number in Seven Years,” *Newsweek*, 9 October 2017, <http://www.newsweek.com/trumps-military-dropped-751-bombs-over-afghanistan-september-highest-number-681208>.
44. James Jones, “President Obama’s Afghanistan-Pakistan (AFPAK) Strategy” (briefing, Foreign Press Center, Washington, DC, 27 March 2009), <https://2009-2017-fpc.state.gov/120965.htm>.
45. Thomas E. Ricks, *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006–2008* (New York: Penguin Press, 2009).
46. Daniel Korski, *Transatlantic “AfPak” Policy: One Year Later*, FRIDE Policy report no. 10 (February 2010), [http://fride.org/uploads/PB40\\_Transatle\\_afpk\\_korski\\_ENG\\_feb10.pdf](http://fride.org/uploads/PB40_Transatle_afpk_korski_ENG_feb10.pdf).
47. Josh Rogin, “Team Obama Scuttles the Term ‘AfPak,’” *Foreign Policy*, 20 January 2010, <http://foreignpolicy.com/2010/01/20/team-obama-scuttles-the-term-afpak/>.
48. Cf. C. Raja Mohan, “South Asian Views on America’s Role in Asia,” in *Asian Views on America’s Role in Asia: The Future of the Rebalance* (San Francisco: The Asia Foundation, 2016), 1–12.
49. Dexter Filkins, *The Forever War* (New York: Alfred A. Knopf, 2008).
50. Radio Free Europe/Radio Liberty, “NATO Chief Says Alliance Could Increase Troops in Afghanistan in Face of Intensifying Insurgency,” Radio Free Europe/Radio Liberty, 1 May 2017, <https://www.rferl.org/a/nato-stoltenberg-afghanistan-troop-levels-taliban/28461034.html>. For



quote and details, see “Resolute Support Mission in Afghanistan,” NATO, updated 10 November 2017, [http://www.nato.int/cps/en/natohq/topics\\_113694.htm](http://www.nato.int/cps/en/natohq/topics_113694.htm).

51. Donald Trump, “Remarks by President Trump on the Strategy in Afghanistan and South Asia” (speech, Fort Myer, VA, 21 August 2017), <https://www.whitehouse.gov/the-press-office/2017/08/21/remarks-president-trump-strategy-afghanistan-and-south-asia>.

52. Lawrence J. Korb, “10 Fatal Flaws in Donald Trump’s Afghanistan Plan,” *National Interest*, 23 August 2017, <http://nationalinterest.org/feature/10-fatal-flaws-donald-trumps-afghanistan-plan-22021>.

53. Quoted in Mark Landler, “Trump, the Insurgent, Breaks with 70 Years of American Foreign Policy,” *New York Times*, 30 December 2017, [https://www.nytimes.com/2017/12/28/us/politics/trump-world-diplomacy.html?smprod=nytcore-ipad&smid=nytcore-ipad-share&\\_r=0](https://www.nytimes.com/2017/12/28/us/politics/trump-world-diplomacy.html?smprod=nytcore-ipad&smid=nytcore-ipad-share&_r=0).

54. Thomas Gibbons-Neff and Dan Lamothe, “3,500 More U.S. Troops Headed to Afghanistan, Officials Say,” *Washington Post*, 6 September 2017, [https://www.washingtonpost.com/news/checkpoint/wp/2017/09/06/3500-more-u-s-troops-headed-to-afghanistan-officials-say/?utm\\_term=.fa3bee37694b](https://www.washingtonpost.com/news/checkpoint/wp/2017/09/06/3500-more-u-s-troops-headed-to-afghanistan-officials-say/?utm_term=.fa3bee37694b).

55. Julia Manchester and Olivia Beavers, “Trump and North Korea: A Timeline on Escalating Tensions,” *The Hill*, 3 September 2017, <http://thehill.com/homenews/administration/349088-timeline-trumps-relationship-with-north-korea>.

56. Joshua Berlinger, “As Secretary Mattis Prepares for Asia Visit, North Korea Starts Reactor,” CNN, 30 January 2017, <http://www.cnn.com/2017/01/29/asia/north-korea-secretary-mattis-asia-visit/>.

57. Eric Gomez, “Explained: Why America’s North Korea Strategy Is Failing,” *National Interest*, 26 December 2017, <http://nationalinterest.org/blog/the-skeptics/explained-why-americas-north-korea-strategy-failing-23805>.

58. Cf. M. J. Lee, “Trump: North Korea Is China’s Problem to Fix,” CNN, 6 January 2016, <https://www.cnn.com/2016/01/06/politics/donald-trump-north-korea-china-ted-cruz-immigration/index.html>; and Andrew Rafferty, “Donald Trump Has History of Contradictory Statements on Nuclear Weapons,” NBC News, 11 October 2017, <https://www.nbcnews.com/news/all/donald-trump-has-history-contradictory-statements-nuclear-weapons-n808466>.

59. John Bowden, “Trump Admin Sanctions Two Senior North Korean Officials,” *The Hill*, 26 December 2017, <http://thehill.com/policy/international/366536-trump-sanctions-two-senior-north-korean-officials>.

60. “Trump: ‘Armada’ Heading toward North Korea,” CNN, 4 April 2017, <http://www.cnn.com/videos/world/2017/04/12/trump-armada-north-korea-fox-news-sje-orig.cnn>.

61. “U.S. National Security Adviser H. R. McMaster: All Options on The Table for North Korea,” *War Defence and News* (blog), 16 April 2017, [http://wardefencenews.blogspot.com/2017/04/us-national-security-adviser-h-r\\_16.html](http://wardefencenews.blogspot.com/2017/04/us-national-security-adviser-h-r_16.html).

62. John Haltiwanger, “U.S. Must Invade North Korea to Wipe Out Kim Jong Un’s Nuclear Weapons, Military Leaders Say,” *Newsweek*, 5 November 2017, <http://www.newsweek.com/us-must-invade-north-korea-wipe-out-kim-jong-uns-nuclear-weapons-military-701713>.

63. Carla Babb, “3 US Aircraft Carriers to Start Joint Exercise in Western Pacific,” *VOAnews.com*, 8 November 2015, <https://www.voanews.com/a/three-us-aircraft-carriers-join-exercises-western-pacific/4107534.html>.

64. Sofia Lotto Persio, “U.S. Aircraft Carriers Show Off ‘Unparalleled Strength’ in First Three Way Joint Drills in the Pacific in a Decade,” *Newsweek*, 9 November 2017, <http://www.newsweek.com/us-nuclear-powered-aircraft-carriers-hold-first-three-way-joint-drills-pacific-706398>.

65. Kim Tong Hyung, "Anger Grows in South Korea over US Anti-Missile System," *ABC News Online*, 2 May 2017, <http://abcnews.go.com/International/wireStory/anger-grows-south-korea-us-anti-missile-system-47169679>.

66. Associated Press, "The Latest: US Won't Seek South Korean Money for THAAD," *ABC News Online*, 30 April 2017, <http://abcnews.go.com/International/wireStory/latest-us-look-south-korean-money-thaad-47114076>.

67. Bruce Klinger, "Save Preemption for Imminent North Korean Attack," Heritage Foundation Report, 1 March 2017, <http://www.heritage.org/missile-defense/report/save-preemption-imminent-north-korean-attack>.

68. Alexander Smith, "Rex Tillerson: Military Action against North Korea Is 'on the Table,'" NBC News Online, 17 March 2017, <http://www.nbcnews.com/news/north-korea/rex-tillerson-military-action-against-north-korea-table-n734771>.

69. Jeffrey Lewis, "Trump Is Bluffing about Attacking North Korea in 2018," *Foreign Policy*, 28 December 2017, <http://foreignpolicy.com/2017/12/28/trump-is-bluffing-about-attacking-north-korea-in-2018/>.

70. For a brief overview, see Russell Goldman, "How Trump's Predecessors Dealt with the North Korean Threat," *New York Times*, 17 August 2017, [https://www.nytimes.com/2017/08/17/world/asia/trump-north-korea-threat.html?\\_r=0](https://www.nytimes.com/2017/08/17/world/asia/trump-north-korea-threat.html?_r=0).

71. Thomas E. Ricks, "Why '5027' Is a Number You Should Know: How War in Korea might Unfold," *Foreign Policy*, 1 May 2017, <http://foreignpolicy.com/2017/05/01/why-5027-is-a-number-you-should-know-how-war-in-korea-might-unfold/>.

72. Eleanor Albert, "Backgrounder: North Korea's Military Capabilities," CFR, updated 30 November 2017, <https://www.cfr.org/backgrounder/north-koreas-military-capabilities>.

73. Choe Sang-Hun, "North Korea Won't Stop Its Arms Tests Anytime Soon, South Korea Warns," *New York Times*, 26 December 2017, <https://www.nytimes.com/2017/12/26/world/asia/north-korea-nuclear-missile-tests.html>.

74. Cf. Joby Warrick, "Microbes by the Ton: Officials See Weapons Threat as North Korea Gains Biotech Expertise," *Washington Post*, 10 December 2017, [https://www.washingtonpost.com/world/national-security/microbes-by-the-ton-officials-see-weapons-threat-as-north-korea-gains-biotech-expertise/2017/12/10/9b9d5f9e-d5f0-11e7-95bf-df7c19270879\\_story.html?utm\\_term=.daec680102bf](https://www.washingtonpost.com/world/national-security/microbes-by-the-ton-officials-see-weapons-threat-as-north-korea-gains-biotech-expertise/2017/12/10/9b9d5f9e-d5f0-11e7-95bf-df7c19270879_story.html?utm_term=.daec680102bf); and Isabella Steger, "North Korea Was Behind the WannaCry Cyberattacks, Says the White House," *Government Executive*, 19 December 2017, <http://www.govexec.com/technology/2017/12/north-korea-was-behind-wannacry-cyberattacks-says-white-house/144674/>.

75. Glenn Thrush and Mark Lander, "Why Trump, After North Korea's Test, Aimed His Sharpest Fire at the South," *New York Times*, 3 September 2017, [https://www.nytimes.com/2017/09/03/us/trump-north-south-korea-nuclear.html?\\_r=0](https://www.nytimes.com/2017/09/03/us/trump-north-south-korea-nuclear.html?_r=0).

76. Interpreting the Trump administration's thinking on the relationship between diplomatic negotiations with North Korea, military threats, and actual military operations is worthy of an article on its own. Suffice to say that the president is not necessarily on the same page as his own appointees in his administration. In October, when then-Secretary Tillerson offered the possibility of negotiations, the president promptly tweeted, "I told Rex Tillerson, our wonderful Secretary of State, that he is wasting his time trying to negotiate with Little Rocket Man." Max Kutner, "Will Trump Negotiate with North Korea? Russia Offers Help with Talks," *Newsweek*, 25 December 2017, <http://www.newsweek.com/trump-negotiate-north-korea-jong-un-russia-758492>.

77. Amanda Erickson, "The Last Time the U.S. Was on 'the Brink of War' with North Korea," *Washington Post*, 9 August 2017, <https://www.washingtonpost.com/news>

/worldviews/wp/2017/08/09/the-last-time-the-u-s-was-on-the-brink-of-war-with-north-korea/?utm\_term=.5c35cab7637d.

78. Mark Bowden, "How to Deal with North Korea," *The Atlantic*, July/August 2017, <https://www.theatlantic.com/magazine/archive/2017/07/the-worst-problem-on-earth/528717/>.

79. CNN, "Trump: 'Armada' Heading toward North Korea."

80. John Grady, "McCain: Where's the Strategy? Mattis: 'We're Working It,'" USNI News, 14 June 2017, <https://news.usni.org/2017/06/14/mccain-wheres-strategy-mattis-working>; and James Mattis, *Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 19 January 2018), <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

81. Simon Reich and Peter Dombrowski, "Has a Trumpian Grand Strategy Finally Stepped into The Light?," *War on the Rocks*, 29 January 2018, <https://warontherocks.com/2018/01/trumpian-grand-strategy-finally-stepped-light/>.

82. For a range of academic and policy practitioner responses, see "Policy Roundtable: A Close Look at the 2018 *National Defense Strategy*," *Texas National Security Review*, 26 January 2018, <https://tnsr.org/roundtable/policy-roundtable-close-look-2018-national-defense-strategy/>.

83. Max Greenwood, "Mattis: North Korean Ballistic Missile Doesn't Pose Immediate Threat to US," *The Hill*, 15 December 2017, <http://thehill.com/policy/defense/365193-mattis-north-korean-ballistic-missile-does-not-yet-pose-immediate-threat-to-us>.

84. Jacqueline Klimas, "Trump's North Korea Strategy: A Lot like Obama's," *Politico*, 8 August 2017, <http://www.politico.com/story/2017/08/08/trump-obama-north-korea-241389>.

85. Reich and Dombrowski, "Has a Trumpian Grand Strategy?"

86. Barack Obama, quoted in Jeffrey Goldberg, "The Obama Doctrine," *The Atlantic*, April 2016, <http://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/>.

# A New Security Framework for Geoengineering

*Elizabeth L. Chalecki*

*Lisa L. Ferrari*

## Abstract

As the national security ramifications of climate change grow more pronounced, climate manipulation technologies, called geoengineering, will become more attractive as a method of staving off climate-related security emergencies. Geoengineering includes methods of carbon dioxide removal and/or solar radiation management and can theoretically achieve significant reductions in warming-related environmental changes, but they are scientifically untested. Geoengineering technologies have the potential to disrupt the global ecological status quo and mount a potentially coercive threat with implications as serious as those in wartime. Several of these technologies can be deployed from the global commons, but international law provides no more than indirect guidance as to how they should be governed as a matter of international security. We argue that, lacking explicit scientific or legal guidance, just war theory provides a useful normative framework for restraining the use of environmental force. Modifying just war theory into “just geoengineering theory” will provide ethical standards for security decision makers as they consider whether or how geoengineering should be used.



---

Elizabeth L. Chalecki is assistant professor of international relations at the University of Nebraska–Omaha and a nonresident research fellow in environmental security at the Stimson Center. Dr. Chalecki has published over 20 books, articles, and book chapters on diverse environmental topics. She holds a PhD in international relations from the Fletcher School of Law and Diplomacy at Tufts University, an MS in environmental geography from the University of Toronto, and an MA in international affairs from Boston University.

Lisa L. Ferrari is associate professor of international relations and ethics in the department of politics and government at the University of Puget Sound. She holds a PhD in government from Georgetown University.

Academics, military practitioners, think tanks, and international organizations—even the UN Security Council—are increasingly concerned about the national security ramifications of a changing climate.<sup>1</sup> These range from direct physical effects such as loss of territory due to sea level rise, to higher order effects such as greater spread of infectious disease, geopolitical instability in a thawing Arctic, and climate change-driven migration. The increasing security toll of climate change is clearly recognized as a significant driver of civil unrest and conflicts such as the Arab Spring.<sup>2</sup> The US military has addressed climate change in both the 2010 and 2014 editions of the Quadrennial Defense Review, and other states around the world are likewise concluding that climate change is a threat multiplier.<sup>3</sup> Even the Intergovernmental Panel on Climate Change (IPCC) now recognizes the human security impacts of climate change and has addressed security in its Working Group II report.<sup>4</sup> With NASA's announcement that 2016 and 2017 will likely be the two hottest years ever recorded, it is clear that the international community is failing to control climate change at the global level.<sup>5</sup> Atmospheric concentration of carbon dioxide has reached a new high of 405 parts per million (ppm) and continues to climb.<sup>6</sup> The emissions restrictions and other climate change mitigation actions contained in the multilateral agreement signed in Paris in December 2015, even if fully implemented, will only result in limiting any global temperature increase to 3.5°C above pre-industrial levels, rather than the recommended 2°C target.<sup>7</sup> The Trump administration has now withdrawn the United States, one of the largest emitters, from the Paris Agreement, placing even the 3.5°C result in jeopardy. Such ongoing and future security concerns will lead policy makers' attention to climate-modifying technologies, which are beginning to appear in scientific and policy discussions as viable alternatives to climate mitigation.

Considerations of the scientific, technological, financial, and ethical implications of geoengineering technologies have appeared in various reports since 2009,<sup>8</sup> but the implications of such technologies for security and defense have not been part of any recent analyses. However, geoengineering on any but the smallest scale means that one state may be able to substantially change the material conditions in another state or even globally on a unilateral basis. Given the lack of any specific laws, treaties, or norms governing planetary technologies of this type, states must look elsewhere for guidance on whether, when, and how

to use them in the interest of national security. A modification of just war theory will serve as a framework for restraining the use of environmental force by states and provide guidance in setting ethical norms and standards for the deployment of climate-altering technologies. This article first explains the types of geoengineering technologies considered feasible for altering the climate. Next it analyzes existing legal guidance. Finally, the article presents a “just geoengineering theory” for considering deliberate climate modification.

## **Geoengineering Technologies**

Currently, we have three options to address the changing climate and its second- and third-order environmental and security effects: adapt to the changes with improved infrastructure and other technologies, mitigate the phenomenon through global greenhouse gas (GHG) emissions reductions, or geoengineer the climate in an attempt to offset or “undo” the damage. Adaptation is the path of least resistance regarding climate change. However, this option requires states rethink the many climatic assumptions, such as stable temperatures and regular precipitation, upon which their economy, their culture, and their infrastructure are based. This type of fundamental change presents huge political and logistical challenges for large and small states.

Mitigation would provide the greatest long-term climate stability, but GHG emission reductions could be economically costly because they would require a massive shift away from fossil fuel use.<sup>9</sup> States have attempted to create a global climate change mitigation regime but have only generated piecemeal agreements, such as the Reducing Emissions from Deforestation and Forest Degradation in Developing Countries plan and the intended nationally determined contributions contained in the Paris accord.<sup>10</sup> Meanwhile, sovereign governments will continue to act in their own best economic and political interests rather than in a generalized global interest.

If the security problems resulting from climate change are severe enough, and if both mitigation and adaptation are seen as undesirable for time or cost reasons, then geoengineering may emerge as a credible method of responding to a national security threat. Geoengineering technologies fall into two distinct types, carbon dioxide removal (CDR) and solar radiation management (SRM). CDR includes any method of removing carbon dioxide, and possibly additional gases, from the ambient air with the inten-

tion of reducing the greenhouse effect and allowing more heat to escape the atmosphere. SRM methods attempt to bounce sunlight away from the earth before it has the chance to be absorbed and re-radiated from the surface as infrared heat, becoming trapped in the atmosphere and contributing to the greenhouse effect.<sup>11</sup> Most methods of SRM or CDR can be deployed from land and so would fall under laws and norms of national governance. However, three of the current CDR/SRM methods must be deployed from the global commons (oceans or atmosphere) and would require novel changes to our ideas of international governance because they cannot be implemented under current assumptions of international sovereignty and security. Those global commons three include:

### **1. Ocean Iron Fertilization (OIF)**

Carbon dioxide can be pulled from the air and sequestered by natural processes in the ocean. Seeding high-nutrient, low-chlorophyll areas of the ocean with nutrients such as iron can stimulate plankton growth, which then absorb carbon dioxide via photosynthesis from the ocean. When the plankton die, the carbon sinks to the ocean floor. This method is estimated to capture between one and four gigatons of carbon dioxide per year, though it would take decades to scale up to that level of capture, and more still would be needed to achieve a 1.5°C climate target.<sup>12</sup>

### **2. Sulfur Aerosol Dispersal**

Dispersal of sulfur dioxide particulates into the upper atmosphere is the most commonly discussed SRM method. Using airplanes, high-altitude balloons, airships, or other means, injected aerosol particulates would then create a global haze that would reflect sunlight, limiting the solar energy reaching the earth's surface and thereby cooling the planet. By way of example, the 1991 eruption of Mount Pinatubo in the Philippines spewed approximately 20 million tons of sulfur and other particulates into the atmosphere, resulting in a global average temperature drop of 1°C for about a year.<sup>13</sup> The equivalent of approximately one Pinatubo every four years would be needed to counteract the effects of climate change over the next few decades.<sup>14</sup>

### **3. Marine-Based Cloud Brightening**

Since clouds are a natural method of reflecting sunlight, the stimulation of cloud formation may serve to reduce incoming solar radiation.

Using sea salt particles as cloud condensation nuclei could encourage clouds to form and reflect sunlight without the use of sulfur dioxide.<sup>15</sup> This method would require approximately 1,500 unmanned ships called Flettner spray vessels to release seawater micro-droplets into the lower atmosphere.<sup>16</sup> These ships could operate on the high seas, thus removing them from territorial interference from other states, and would be unmanned and unfueled, using wind power for motion. Since the cloud-brightening effect requires a constant input of sea spray, the process can be turned off relatively quickly if adverse effects appear.<sup>17</sup>

### **Costs and Implications**

In terms of security-related changes to the environment, ecological collateral damage during combat is one of the most significant costs of war, because disruption or destruction of the environment and its resources hinders the recovery of the civilian population. The UN Environment Programme has conducted postconflict environmental assessments in Afghanistan, Iraq, Gaza, and Sudan. Sometimes the ecosystem can recover from the effects of a conflict, sometimes it does not.<sup>18</sup> Subsequent estimates of the ecological, economic, and human health costs of recent wars include \$450 million to clean up dioxin in certain areas of Vietnam, \$6.5 billion to fight fires and make repairs to oil infrastructure in Kuwait after the First Gulf War and \$27 billion in lost oil/gas profit, and approximately \$44 million in environmental damage in Gaza since the escalation of conflict in 2009.<sup>19</sup>

Any geoengineering technology on a scale large enough to shift the global climate has the potential to inflict damage of the same magnitude. Since these technologies have not been tested to scale, direct cost comparison can be difficult, but by way of proxy data, the eruption of the Eyjafjallajökull volcano in 2010 cost the Icelandic government \$7.5 million in cleanup and repairs, and the global economy experienced an estimated \$5 billion in lost airfare, tourism, and perishable consumer goods.<sup>20</sup> The total costs of the 1980 Mount St. Helens eruption in Washington State and the 1991 Mount Pinatubo eruption in the Philippines were estimated to be \$1.1 billion (1980 dollars) and \$700 million (1991 dollars), respectively.<sup>21</sup> Since governments have limited abilities to calculate ecosystem losses, there may be extended or synergistic damages that are not captured.<sup>22</sup>



Furthermore, this damage would be perpetrated knowingly upon other states without their consent. Global commons-based geoengineering is not synonymous with the use of violent force. But, depending upon the type of technology used, it could incur the same level of cross-border environmental destruction and loss of sovereignty as a war. War is waged with intent to harm; geoengineering might be deployed without that intent, but we argue that—when speaking of that scale of involuntary environmental change—that is a distinction without a difference. Since the global ecosystem and atmosphere are indivisible, one state can cause material changes in the environment of another that have the possibility to negatively affect the territory, economy, and security of that state. These changes would affect the security and material well-being of states, just as the use of violent force does. Thus, rules and norms about geoengineering have their parallels in rules and norms about use of force. Deploying geoengineering technologies raises issues of both national security and ethical treatment of the global environment.

### **Ecological and Economic Risks to Geoengineering**

Research on these methods of geoengineering is not well developed, and it is easy to spot both ecological and economic risks. While OIF may have a positive effect on fish stocks, it may also result in changes to the structure of the marine food web and possible reduction of subsurface oxygen.<sup>23</sup> Previous OIF experiments have resulted in the production of greenhouse-enhancing gases such as dimethylsulfide, nitrous oxide, and methane.<sup>24</sup> Any type of geoengineering that does not remove carbon will allow for the continued acidification of the oceans.<sup>25</sup> Such effects will vary depending on where on the ocean and at what time of year the Flettner ships are deployed.<sup>26</sup>

The ecological risks of aerosol deployment are significant. Net primary productivity is a measure of the amount of chemical energy produced by plants and is directly related to the amount of sunlight they receive. If SRM reduces the amount of sunlight reaching the earth, then plants from crops to forests may become less productive.<sup>27</sup> Also, with a 3 percent drop in incoming sunlight under an SRM scheme, solar power from photovoltaic panels and dish collectors would become less effective.<sup>28</sup> Sulfur aerosols in particular may accelerate depletion of the stratospheric ozone layer, and since sulfur dioxide is the main corrosive component in acid precipitation, any sulfur artificially added to the

atmosphere via geoengineering will eventually rain out in some form, causing localized ecosystem damage and human health concerns.<sup>29</sup> Additionally, early computer models suggest that cloud brightening may interfere with existing precipitation patterns.<sup>30</sup> If global GHG emissions are not reduced, then any method of SRM would have to be continued indefinitely once it is begun. If SRM is stopped and the full complement of sunlight reaches the earth through an atmosphere thick with GHGs, the global temperature would rapidly spike upward, a phenomenon known as the termination effect. This carries the more-than-likely risk of abrupt and dangerous warming, well outside twentieth-century climate variability bounds.<sup>31</sup> It should be noted that the potential benefits of geoengineering on the climate could also be significant, but just as in war, they would be unevenly distributed.

Perhaps the greatest concern regarding geoengineering is the moral hazard. Any type of geoengineering method could incur a moral hazard, but SRM is particularly dangerous; because SRM methods have the potential to work quickly, their effects can be felt quickly. This may lead the public to conclude that the global warming problem has been “fixed” and that the difficult and disruptive work of de-carbonizing the world’s energy supply need not continue. Without public pressure, policy makers are unlikely to pursue further climate change mitigation measures, particularly if they are costly compared to an SRM regime. Already, with US participation in the Paris agreement stalled, lawmakers in Congress have introduced a bill to formulate a research agenda for “albedo modification strategies that involve atmospheric interventions” (SRM), citing the effects that climate change has on US national security!<sup>32</sup>

## **Existing Legal Guidance**

Since there are no international instruments that deal explicitly with geoengineering, international law only provides limited guidance to security policy makers. However, several environmental treaties and war conventions may have ancillary relevance.

### **Environmental Laws**

International environmental laws assign responsibility and regulate behavior with respect to the environment as well as describe the norms and conventions that govern our relationship to the natural environ-

ment. Many of these laws address issues that arise in the global commons (ocean and atmosphere), and several may apply to geoengineering processes and technologies. The 1972 London Dumping Convention and the 1982 UN Convention of the Law of the Sea (UNCLOS) both contain provisions to address marine pollution; depending on the attempt, this may include iron particles used for OIF.<sup>33</sup> UNCLOS Article 140 states that activities carried out in the high seas area shall be for the benefit of mankind as a whole, irrespective of the geographical location of states. Although the article is intended to address the disposition of minerals and other resources on the ocean floor, it is relevant to our discussion because the exclusionary nature of security actions automatically prejudices the interests of one state over another. One state wishing to employ a marine-based geoengineering strategy may therefore have to demonstrate that the climate benefits they intend to bring about are intended to improve the climate generally and not merely for their own individual state. The 1979 Convention on Long Range Transboundary Air Pollution addresses air pollution and may outlaw the use of sulfur aerosols for SRM. The 1992 Convention on Biological Diversity addresses any process that affects ecological biodiversity; in 2010, the tenth conference of the parties issued a statement calling for states to abstain from attempts at geoengineering until further research into their effects on biodiversity might be assessed.<sup>34</sup> By 2016, the subsidiary body on scientific, technical, and technological advice issued an updated analysis pointing out the environmental and governance uncertainties still inherent in these technologies and noting that they are yet ungoverned.<sup>35</sup>

## **Laws of War**

Legal agreements concerning norms of wartime behavior can also shed light on the security, political, and ethical implications of geoengineering in two ways. First, a few of those agreements directly address treatment of the environment during wartime. Second, since geoengineering technologies have the potential to disrupt the global physical status quo, they mount a potentially coercive threat with implications as serious as those in wartime. Thus, any review of the security ramifications of geoengineering technology warrants consideration of legal norms and agreements regarding war.

## **1977 Environmental Modification Convention**

The 1977 Environmental Modification Convention (ENMOD) specifically prohibits “military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party.”<sup>36</sup> This leaves open the possible argument that ENMOD is not applicable to geoengineering because it does not qualify as warfare since it has no stated intent to destroy, cause damage to, or injure any other state.

The prohibition of “military use” of environmental modification techniques appears to apply to the conduct of warfare only and leaves open to interpretation whether or not peaceful use could be carried out by military personnel or equipment.<sup>37</sup> Some of the atmospheric or ocean-based schemes would require substantial logistical capability to deploy successfully, and the national military may be the only state agency with the wherewithal to perform such a mission. Most state militaries are allowed and even expected to assist civil authorities when officially requested to do so; this includes carrying out disaster relief operations such as provision of emergency aid and evacuation of civilians. If deployment of a geoengineering scheme becomes a matter of national economic or scientific policy, then military involvement would be governed by the relevant national laws.

## **1977 Geneva Protocol I**

Protocol I pursuant to the Geneva Conventions of 1949 addresses the protection of victims of international armed conflict, and several articles specifically address protection of the natural environment. Article 35 employs similar language to ENMOD in that parties are prohibited from employing methods and means of warfare that cause “widespread, long-term, and severe” damage to the natural environment. Though the two conventions use similar terms to describe prohibited environmental damage, ENMOD assumes “long-lasting” to mean a few months to a season, whereas “long-term” in Protocol I is understood to refer to decades.<sup>38</sup> Article 54 prohibits parties from attacking objects necessary for the survival of the civilian population, including food, water, and agricultural land and resources. Article 55 enjoins parties to protect the environment from widespread, long-lasting and severe collateral damage during war. Article 56 prohibits attacks on works and installations that

contain dangerous forces (usually read to mean the built environment, such as dams and power plants).<sup>39</sup> The reasoning behind both ENMOD and Protocol I is that the health of the natural environment is critical to the survival of the civilian population and should not be prejudiced by war. If this injunction is significant enough to warrant consideration during warfare, when states are customarily granted the greatest legal and operational leeway in national security operations, then it should warrant consideration during peacetime when states have the ability to reflect and consult.

### **Geoengineering in International Legal Limbo**

Of the three technologies that would be deployed from the global commons, each suffers from a certain kind of legal neglect. For example, nothing prohibits peacetime use of environmental modification technologies such as aerosol dispersal or cloud brightening. This means that any state or nonstate actor deploying such technology could claim (truthfully or not) that they were acting for the good of their country or of humankind and consequently had no hostile intent. Such a claim would render laws such as ENMOD or Geneva Protocol I inapplicable. These same actions might be illegal under domestic law, but since domestic laws differ in scope and specificity from international treaties, a particular technology such as ocean iron fertilization that may be illegal in territorial waters may not automatically contravene international law if deployed from the high seas. Consequently, any one of the Global Commons 3 technologies could be considered legal from a positivist perspective.

Finally, nothing in any law, convention, treaty, or custom prohibits a state from defending itself and its territory from a real threat to its national security. As disruption from climate change becomes more pronounced, and the international security threats arising from these effects become more apparent, a state may find itself considering an attempt at geoengineering for its own protection or preservation.

### **Just Geoengineering Theory**

Under every accepted theory of modern international relations, a state is allowed, even obligated, to protect its national security. If the physical effects of anthropogenic climate change produce or contribute

to threats to national security, then abating it or offsetting its negative consequences may be viewed as a necessary security requirement, maybe even on a pre-emptive or preventive basis. Already, military forces from countries around the world are taking steps to address climate-related threats. The mounting security threats from climate change have been likened to World War III, and the need to mobilize on a nation-changing footing to produce renewable energy technology likened to the American industrial run-up to defeat the Axis Powers.<sup>40</sup> If geoengineering is to be considered as a defense option, and international law provides no specific prohibition, we can look to just war theory for further guidance.

Just war theory provides ethical guidance for decision making about the destructive forces of war. It helps define the concepts of “right” and “wrong” in warfare and made customary the idea that warfare is limited in scope and method.<sup>41</sup> Therefore, just war criteria can illuminate important ethical and security considerations for deploying geoengineering technology. Using geoengineering for defense and security means one of two things: either a state is manipulating the climate as “offense,” as a means of war; or the national security problems engendered by the changing climate have become so severe that policy makers have begun to see geoengineering as a possible means of “defense.” If the former, such actions are clearly prohibited by ENMOD and Geneva Protocol I. If the latter, decision making becomes a bit murkier. Consequently, we can view potential “defensive” attempts at geoengineering through the lens of just war theory and ask ourselves whether or not such attempts could be both ethically acceptable and a net security gain. In doing so, we make use of both *jus ad bellum* (law of resort to force) and *jus in bello* (law of war fighting) criteria. While not all the elements of just war theory relate directly to consideration of geoengineering, three of the criteria shed useful light on its utility as a possible option for national self-defense.

### **Competent Authority**

This *jus ad bellum* criterion is generally understood to mean that war cannot be undertaken justly without the permission of a publicly recognized authority acting in accordance with the rule of law, divine right, or other relevant source of political legitimacy. Early Western notions of just war were articulated through Christian theology, but just war thinking has grown beyond that foundation. On questions of war, states share with

intergovernmental organizations (IGO) such as the United Nations and NATO the ability to speak authoritatively about when the use of force is and is not permitted. Therefore, it is reasonable that states and IGOs, in consultation with climate experts, can speak with authority on the use of force through geoengineering.<sup>42</sup>

However, sovereign states, individually or in groups, are still the only actors that can legitimately use force in international relations, ostensibly in defense of their citizens. Therefore, they must make a significant and allied commitment to prevent any illegitimate geoengineering deployment by rogue or unauthorized actors.<sup>43</sup> Then, if geoengineering is deployed, it is done as part of a considered national plan, not from a grudge, hostile intent, or a misplaced sense of experimentation.

### **Proportionality**

This same requirement for expert scientific judgment informs the *jus ad bellum* and *jus in bello* principles of proportionality. Here, proportionality means that the ecological good that the acting state intends to achieve through its use of geoengineering must outweigh any negative ecological consequences it brings about. Consideration of proportionality in geoengineering is complicated both because the changing climate is a moving ecological target and because meaningful tests of the technology are currently ineffective or impossible. This means that a “just” deployment would need to be reassessed regularly over its duration, because changing environmental conditions over time mean that geoengineering can make things worse, not better.

### **Discrimination**

Finally, the principle of discrimination distinguishes between morally acceptable and unacceptable targets: combatants are legitimate targets; noncombatants are not. This distinction is not always easy to make, since guerrilla and insurgent warfare frequently involve irregular troops, civilians who willingly or unwillingly serve as weapons platforms, and tactics such as improvised explosive devices that can be difficult to attribute to a specific source. In such cases, it is difficult to discriminate between legitimate and illegitimate targets because the line has blurred between who is a combatant and who is not. The old categories do not easily fit the new reality of warfare, though the moral imperative of discrimination remains. However, there are two points to consider when

applying this principle to geoengineering: how to identify “combatants” in this case, and whether global geoengineering technologies raise collateral damage questions similar to those raised by weapons of mass destruction (WMDs).

In considering geoengineering as a use of force, the principle of discrimination forces us to redefine who are considered combatants and noncombatants. Combatants are generally the armed forces of two or more warring nations, and are legitimate targets under just war theory; noncombatants are not legitimate targets. However, when the proper authority of a state is considering geoengineering, this policy is intended to benefit the government and its citizens. Since they are the ones taking the proposed action for their own benefit, they can be loosely termed to be the “combatants” in this parallel to war. Conversely, “noncombatants” are normally those civilians who are not party to the conflict; in this parallel, we might term everyone else on Earth to be the non-combatants, since the action is not taken for their benefit, nor are they necessarily even considered.

### **Climate Change for National Defense**

War involves unleashing powerful forces not only on the target population but also on the non-target population as well. Current norms of war permit some level of collateral damage during combat, but combatants must reasonably foresee and minimize such damage. While geoengineering technologies and WMDs differ in important ways, they are both instruments of force that cannot be targeted precisely. Furthermore, commons-based geoengineering will not be effective unless tested or deployed on a global scale, which adds another level of ecological uncertainty to any attempt to minimize collateral damage. Customary international law, as stated by the International Committee of the Red Cross and reaffirmed in the 1998 Rome Statute of the International Criminal Court, holds both that indiscriminate attacks are prohibited and that the use of indiscriminately targeted weapons constitutes a war crime.<sup>44</sup> It stands to reason, then, that a similar precaution would pertain to indiscriminately targeted instruments of massive environmental change. If states do consider geoengineering from the global commons as a method of national defense, we can construct a new framework to function in geoengineering decision making as just war theory functions in conflict decision making. Because of the global and possibly irreversible



effects, all precautions must be taken by the decision makers to maximize transparency and represent all stakeholder views.

### **Jus ad climate**

The state must be facing a major climate change–related security emergency in order to justify using geoengineering. In the same way that self-defense is an agreed-upon indicator of a just war, a major climate emergency would function as an agreed-upon precondition for geoengineering deployment. However, as in just war theory, this criterion is extremely subjective. While no financial or mortality estimates have been agreed upon as to what constitutes a major emergency, what would be a small scale natural disaster for one state might be an existential threat to another. Hence, geoengineering technology would be deployed when the damage became “bad enough,” presumably as determined by the competent national authority. Such an estimation could include costs from drought, floods and storms, crop failures, heat deaths, and so forth.

We propose consideration of several additional factors for determining whether a situation is “bad enough.” First, the estimated damage must meet some threshold in lives or dollars. There is no specific number to attach to such a factor, since relative damage varies by state, but the competent national authority should think about what those numbers might be and presume to set them high so geoengineering does not become the option of first resort. Second, the security threat must be publicly attributable to climate change. If policy makers want to geoengineer the climate, they need to admit that the security threat the state is facing stems from a climate change–related problem and not some random force majeure event. In this way, mitigation and adaptation measures are brought back into the discussion and not automatically dismissed in favor of the technological option.

Third, the real or assumed cost of equivalent climate change mitigation or adaptation efforts must be “too high” to afford or take “too long” to be effective. Meeting this threshold would permit the just use of geoengineering rather than, or in addition to, mitigation or adaptation measures. However, this is where the greatest moral hazard trap appears. As environmental conditions further degrade and the need to respond grows increasingly urgent, it will be easy for international actors to see geoengineering as a technological quick fix for the climate. This would be a grave error for two reasons. First, most of the technologies

are in the early stages of research and development, so confidence in their effectiveness is low. Second, field testing the technologies at the planetary level will have the same impact as actual deployment, thus eliminating the option of experimentation. This greatly reduced margin of error argues for caution even beyond the normal level for scientific investigation.

Some analysts have argued for the preemptive early use of SRM, well before any such emergency threshold is reached. Such argument is usually attached to the justification that this use would temporarily stabilize the climate and buy the world's states enough time to switch from fossil fuels to noncarbon energy sources. However, the danger of preemptive use lies in its very potential for short-term success. The deployment of atmospheric sulfur may indeed lower global temperature a measurable 1.5°C for the span of a few years, similar to the eruption of Mount Pinatubo, but this veneer of success removes the urgency for making the switch; as most energy infrastructures and systems are path-dependent with a high level of technological lock-in, discouraging any shift to other modes of production as too expensive.<sup>45</sup>

Any decision to deploy geoengineering from the global commons (atmosphere or seas) must be made at the national level first, then subject to international consent. To guard against rogue actors, any decision to deploy geoengineering must be made by the competent national authority, presumably in conjunction with scientific advisors. This guarantees that such a decision represents the will of the nation, or at least its government, and not merely one faction or one individual. However, since the ecological changes brought about by geoengineering are global in scope and the likelihood of undesirable collateral environmental damage is high, there must be some level of international approval for an individual state's decision.

National decisions concerning evaluation of just war criteria, and determination of national security in general, are not usually subject to international discussion before they are implemented. But geoengineering technologies are not like other weapons due to their unique combination of global reach, potential for nonlinear effect, and fundamental implications for the livability of our planet.<sup>46</sup> Any type of weapon used in modern conflict can be subject to the just war constraints of proportionality and discrimination; geoengineering technologies should be as well. Barring formation of a new body, the only standing body

that could provide such consent, and hence legitimacy under our just geoengineering theory criteria, is the UN Security Council. This means that any discussion of deployment would be subject to the veto of the five permanent members, which may act as a restraining force on states seeking approval for deployment. However, if the UN or any agency it designates to make such decisions were to assess the risk of a proposed attempt and determine it to be acceptable, then such an action would have earned international approval and would not be considered “hostile” per ENMOD.

Any geoengineering attempt must have a reasonable chance of success, according to the best scientific and economic knowledge available at the time. If a particular method of geoengineering has some negative ecological consequences that in itself does not make it unjust. Rather, the competent national authority must clearly demonstrate how the ecological and financial good outweighs the bad, based on the best scientific knowledge available at the time the decision is made. This could be measured in a number of ways: temperature lowered, lives saved, money saved, disasters avoided. If this cannot be determined, then the precautionary principle applies: put down the sulfur and step away. The intent of the state deploying the technology is key: only defensive deployment aimed at avoiding or mitigating a security threat is permitted. Any attempt to use geoengineering for offensive purposes (to manipulate or threaten another state) would be considered hostile use and subject to the terms of ENMOD.<sup>47</sup>

Any geoengineering attempt must meet the double effect criteria: only the good result is intended, the bad result is not a means to the good result, and the actor foresees greater good than bad resulting from the deployment. In war, double effect is a matter of both *jus ad bellum* and *jus in bello*. An actor’s reason for resorting to force may or may not violate the principle, though the actor’s means of fighting incur a double effect. In either case, actors must ensure that they are not engaging in harm for harm’s sake. In geoengineering, double effect is primarily a question of resorting to use, rather than one of using the technology once it is deployed. This is because effective geoengineering will alter the global climate, and any change on that scale will almost certainly have both good and bad results. In other words, it would be impossible to deploy geoengineering technology without incurring double effect. Therefore, the question of double effect arises in assessing not the use

of force but rather in determining the ethics of resorting to using geo-engineering force at all. This suggests that any decision-making about geoengineering should proceed with a high level of caution.

### **Jus in climate**

The method chosen must be the least environmentally harmful one within the necessary time frame and designed to achieve the minimum ecological disruption necessary to offset climate change effects. This criterion echoes the just war criteria of proportionality and comparative justice, since it posits that just actors may use only the amount of force necessary to achieve their goal. However, this criterion also includes elements of the need for proper authority, because understanding the available time frame and levels of ecological disruption will require input from scientists and stakeholders. We caution that extreme care should be taken with the implementation of this criterion, since it relies heavily on subjective scientific and environmental judgment. If done hastily or with no ecological care, a reckless deployment attempt could be perceived as an act of war by one aggrieved or desperate nation or party against the rest of humanity or the earth. Therefore, transparency of negotiation, goals, and possible outcomes will be paramount to ethical geoengineering.

The method chosen must yield greater good than harm globally, not just to the country deploying it, and from the first year of deployment. If not, it must be discontinued as ineffective or unjust. Again relying on the obligation to refrain from transboundary environmental harm, not only the deploying state but also the world community must measure the effects of geoengineering for its benefits for the combatants and its harm to the noncombatants. The applicability of the double effect principle here in jus in climate means that both proportionality and discrimination must be reassessed on an annual basis for the duration of the deployment, and a workable regime must produce greater environmental good than harm.

A short time threshold to prove the viability of geoengineering technology is critical for jus in climate, because unjust or unworkable strategies that linger can cause significant environmental and economic damage on top of the climate change effects they are trying to mitigate. The important second-order effects of climate change are availability of fresh water, amount of agricultural output, and prevalence of infectious dis-

ease. Food and water security are significantly affected by climate-dependent conditions such as temperature and precipitation, and climate change results in outbreaks of infectious diseases due to shifting disease vectors.

Most states that avail themselves of a modicum of international trade can recover from a one-year disruption in agricultural output, water supplies (though this is harder), and food and resource markets. Aid agencies such as the World Food Programme or Oxfam can make accommodations for one year, and the WHO and other international medical authorities can get medicines and personnel in place within one year, should they need to respond to an outbreak. However, for food and water constraints or disease outbreaks lasting longer than that, adaptation becomes more problematic. Consequently, for a geoengineering method that is expected to take longer than one year to provide benefits, we should assume that the net environmental effect will be neutral, pending a positive outcome. Otherwise, insisting against evidence that a technique will work in the undetermined future can become a cover for faulty technology, scientific experimentation, or profit seeking.

### **Jus post climate**

The third category of just geoengineering theory, what we might call *jus post climate*, would have as its equivalent principles those of ending the geoengineering deployment as soon as possible and restoring the ecosystem to its previous state. However, elucidating this further would be premature at this point due to the specific technological nature of geoengineering. If the technology deployed is a type of SRM, then not only can it not be stopped without concomitant removal of atmospheric GHGs, in fact it must be continued indefinitely in order to provide the desired global cooling effect. Otherwise the temperature would rise rapidly, the previously mentioned termination effect. This means that regardless of what SRM methods are used, the world community must work to reduce GHG concentrations in the atmosphere at the same time. Additionally, the process of geoengineering is not designed to restore the climate and the environment to its original state but merely to hold off damage and buy time until noncarbon forms of energy have replaced fossil fuels. Since the climate always exhibits some degree of variability, knowing when a particular deployment had “reset” the climate would be near impossible.

Jus post bellum does include a principle stating that those individuals guilty of war crimes and crimes against humanity perpetrated in the course of a war should be tried in accordance with international law. In parallel, states embracing jus post climate could also consider rogue geoengineers to be guilty of crimes against humanity. This is not a completely new concept. The 1998 Rome Statute of the International Criminal Court (ICC) includes environmental damages as outlined in the Geneva Protocol I as a possible war crime.<sup>48</sup> Until now, the ICC has not pursued environmental crimes, though the current prosecutor may expand the range of the court's cases.<sup>49</sup> Although geoengineering is not explicitly enumerated among customary crimes against humanity or war crimes, the extensive environmental alteration inherent in any scale geoengineering attempt could easily result in "widespread, long-lasting, and severe" damage if it has unintended effects.

### **Conclusion: It's Not Nice to Fool Mother Nature**

States that are threatened by the security effects of climate change and considering geoengineering as a result face an unpalatable choice: refrain from deploying and run a dangerous or even ruinous security risk or deploy some method of geoengineering, gamble that it will not result in a climate catastrophe, and face criticism from the international community if this decision does not have UN approval. Either of these choices entails risks for a state, since climate change-driven security threats are often multiyear, multisystem hazards that are not easily quantifiable and may not result from a direct adversary.

If addressing climate change-related threats has become part of the security decision-making process, does it make sense to try to operationalize the principles behind just geoengineering theory? In traditional defense and security decision making, the principles behind just war theory are formalized in treaties such as the Geneva Conventions and in customary international law, and put into practice in the form of rules of engagement (ROE) that military forces must follow in combat. Since international law does not address geoengineering as a security measure, could we build an international convention on climate manipulation technologies and construct the relevant ROEs from there? This is problematic for two reasons.

First, there would likely be resistance from the scientific community, which has argued for experimentation on the grounds that, should this

be needed in an emergency, we would be unwise to deploy untested technology.<sup>50</sup> It is true that small-scale experiments may yield valuable local data on how particular technologies perform, but these results may not scale up to planetary level. If a larger-scale deployment were attempted under the guise of “experimentation,” the data yielded might be more useful, but the risk to the ecosystem is proportionally greater. To this end, there would be no justifiable distinction between experimentation and actual use.

Second, the growing strain of nationalism in the world is pointing toward fewer treaties and less cooperation on global issues and signals a retreat from the liberal international order needed to make a geoengineering convention work. What we hope to achieve with this development of just geoengineering theory is to create a set of norms and customs that can be used to guide decision making by states and the international community in the absence of explicit international law.

Right now, climate change–related security threats are increasing, while mitigation and adaptation efforts are not keeping pace. Eventually, geoengineering (especially the three global commons methods discussed herein) will start to look like viable climate manipulation measures cloaked in national security. However, law and custom require states to keep environmental harm from negatively affecting other states, and these three methods of geoengineering offer no possibility of limiting effects to one country or region. These methods are indiscriminate, nonproportional, and possibly irreversible, and the global environmental stakes are too high for anything less than deliberate ethical decision making. Consequently, we offer these just geoengineering guidelines as essential to deployment. ■■■

## Notes

1. See Center for Naval Analyses (CNA), *National Security and the Accelerating Risks of Climate Change* (Washington, DC: CNA, 2014), [https://www.cna.org/CNA\\_files/pdf/MAB\\_5-8-14.pdf](https://www.cna.org/CNA_files/pdf/MAB_5-8-14.pdf); CNA, *National Security and the Threat of Climate Change* (Washington: CNA, 2007), [https://www.cna.org/CNA\\_files/pdf/National%20Security%20and%20the%20Threat%20of%20Climate%20Change.pdf](https://www.cna.org/CNA_files/pdf/National%20Security%20and%20the%20Threat%20of%20Climate%20Change.pdf); Elizabeth L. Chalecki, *Environmental Security: A Guide to the Issues* (New York: Praeger, 2013); Christian Parenti, *Tropic of Chaos: Climate Change and the New Geography of Violence* (New York: Nation Books, 2011); Carolyn Pumphrey, ed., *Global Climate Change: National Security Implications* (Carlisle, PA: US Army War College Strategic Studies Institute, 2008); UN Security Council, “Maintenance of International Peace and Security, Impact of Climate Change,” in *Part V: Consideration of the Functions and Powers of the*

Security Council S/PV.6587 (Resumption 1), 20 July 2011, 393–95, [http://www.un.org/ga/search/view\\_doc.asp?symbol=S/PV.%206587%20\(Resumption%201\)&Lang=E](http://www.un.org/ga/search/view_doc.asp?symbol=S/PV.%206587%20(Resumption%201)&Lang=E).

2. Caitlin E. Werrell and Francesco Femia, eds., *The Arab Spring and Climate Change: A Climate and Security Correlations Series* (Washington, DC: Center for American Progress, February 2013).

3. US Department of Defense, 2014 Quadrennial Defense Review (Washington, DC: US Department of Defense, 2014), [archive.defense.gov/pubs/2014\\_Quadrennial\\_Defense\\_Review.pdf](http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf); 2010 Quadrennial Defense Review. [www.comw.org/qdr/fulltext/1002QDR2010.pdf](http://www.comw.org/qdr/fulltext/1002QDR2010.pdf). Lukas Rüttinger, Dan Smith, Gerald Stang, Dennis Tänzler, and Janani Vivekananda, *A New Climate for Peace: Taking Action on Climate and Fragility Risks, An Independent Report Commissioned by the G7 Members* (Berlin: Adelphi, Woodrow Wilson International Center for Scholars, European Union Institute for Security Studies, 2015); for a list of documents from governments around the world on the links between security and climate change, see the Center for Climate & Security, <http://climateandsecurity.org>.

4. Neil Adger, Juan Pulhin, Jonathon Barnett, Geoffrey D. Dabelko, Grete Kaare Hovelsrud, Marc Levy, Ursula Oswald-Spring, Coleen Vogel, Paulina Aldunce, and Robin Leichenko, “Human Security,” in *Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change*, ed. C. B. Field, et al (New York: Cambridge University Press, 2014), 755–91, [http://www.ipcc.ch/pdf/assessment-report/ar5/wg2/WGIAR5-Chap12\\_FINAL.pdf](http://www.ipcc.ch/pdf/assessment-report/ar5/wg2/WGIAR5-Chap12_FINAL.pdf).

5. Jonathan Erdman, “2017 Likely to Be Earth’s Second Warmest Year on Record, NASA Says,” Weather.com, 17 November 2017, <https://weather.com/news/climate/news/2017-11-17-earth-second-warmest-year-october-nasa-noaa>.

6. Ed Dlugokencky and Pieter Tans, “Trends in Atmospheric Carbon Dioxide: Recent Global Monthly Mean CO<sub>2</sub>,” Earth System Research Laboratory / National Oceanic and Atmospheric Administration, last updated 5 February 2018, <https://www.esrl.noaa.gov/gmd/ccgg/trends/global.html>.

7. The 2°C limit was recommended by the IPCC and committed to by the parties to the Cancun Agreements of 2010. See “Summary for Policymakers,” Intergovernmental Panel on Climate Change (IPCC), *Climate Change 2014: Mitigation of Climate Change. Working Group III Contribution to the Fifth Assessment Report of the IPCC* (New York: Cambridge University Press, 2014), 10, [http://www.ipcc.ch/pdf/assessment-report/ar5/wg3/ipcc\\_wg3\\_ar5\\_summary-for-policymakers.pdf](http://www.ipcc.ch/pdf/assessment-report/ar5/wg3/ipcc_wg3_ar5_summary-for-policymakers.pdf). For a brief and interesting discussion of how the international climate regime arrived at the 2°C target, see “Two Degrees: The History of Climate Change’s Speed Limit,” Carbon Brief, 12 August 2014, <https://www.carbonbrief.org/two-degrees-the-history-of-climate-changes-speed-limit>. Also see UN Framework Convention on Climate Change (UNFCCC), “The Cancun Agreements,” accessed 20 November 2017, <http://cancun.unfccc.int/cancun-agreements/significance-of-the-key-agreements-reached-at-cancun/>.

8. Royal Society, *Geoengineering the Climate: Science, Governance, and Uncertainty* (London: The Royal Society, 2009); Asilomar Scientific Organizing Committee, *The Asilomar Conference Recommendations on Principles for Research into Climate Engineering Techniques: Conference Report* (Washington, DC: Climate Institute, 2010); Bart Gordon, “Engineering the Climate: Research Needs and Strategies for International Coordination,” Report to the 111th Congress, Second Session, October 2010, [www.science.house.gov](http://www.science.house.gov); National Research Council (NRC), *Climate Intervention: Carbon Dioxide Removal and Reliable Sequestration* (Washington, DC: The National Academies Press, 2015), <https://doi.org/10.17226/18805>;



and NRC, *Climate Intervention: Reflecting Sunlight to Cool Earth* (Washington, DC: The National Academies Press, 2015), <https://doi.org/10.17226/18988>.

9. International Energy Agency (IEA), *Real World Policy Packages for Sustainable Energy Transitions: Shaping Energy Transition Policies to Fit National Objectives and Constraints* (Paris: IEA, 2017); see also Mark Z. Jacobson and Mark A. Delucchi, "Providing All Global Energy with Wind, Water, and Solar Power, Part I: Technologies, Energy Resources, Quantities and Areas of Infrastructure, and Materials," *Energy Policy* 39, no. 3 (March 2011): 1154–1169, <https://doi.org/10.1016/j.enpol.2010.11.040>.

10. See UNFCCC, Reducing Emissions from Deforestation and Forest Degradation in Developing Countries (website), <http://redd.unfccc.int/>. For a list of intended nationally determined contributions and progress towards their achievement, see [http://unfccc.int/focus/indc\\_portal/items/8766.php](http://unfccc.int/focus/indc_portal/items/8766.php).

11. The scientific definitions of CDR and SRM can be found at NRC, *Carbon Dioxide Removal and Reliable Sequestration*, 2, and NRC, *Reflecting Sunlight to Cool Earth*, 28, respectively.

12. Phil Williams, "Emissions Reduction: Scrutinize CO<sub>2</sub> Removal Methods," *Nature* 530 (11 February 2016): 153, <http://doi.org/ck64>; see also NRC, *Carbon Dioxide Removal and Reliable Sequestration*, 72.

13. Robert Kunzig, "A Sunshade for Planet Earth," *Scientific American* 299 (2008): 46–55, <http://www.jstor.org/stable/26000882>.

14. Alan Robock, Martin Bunzl, Ben Kravitz, and Georgiy L. Stenchikov, "A Test for Geoengineering?," *Science* 327 (29 January 2010): 530–31, <http://www.jstor.org/stable/40510171>.

15. John Latham and M. H. Smith, "Effect on Global Warming of Wind-Dependent Aerosol Generation at the Ocean Surface," *Nature* 347 (1990): 372–73, <http://doi.org/d6m455>.

16. Jack Chen, Alan Gadian, John Latham, Brian Launder, Armand Neukermans, Phil Rasch, and Stephen Salter, "Stabilization of Global Temperature and Polar Sea-ice Cover via Seeding of Maritime Clouds," *European Geosciences Union (EGU) General Assembly Conference Abstracts* (Vienna: EGU, 2–7 May 2010), 11364, <http://adsabs.harvard.edu/abs/2010EGUGA..1211364C>; and Andrew Moseman, "How Geoengineering Works: 5 Big Plans to Stop Global Warming" *Popular Mechanics* (30 September 2009), <http://www.popularmechanics.com/science/environment/a3719/4290084/>.

17. Chen, et al, "Stabilization."

18. UN Environment Programme (UNEP), "Disasters and Conflicts" (website), accessed 16 October 2017, [www.unep.org/disastersandconflicts/](http://www.unep.org/disastersandconflicts/); see also Jay E. Austin and Carl E. Bruch, *The Environmental Consequences of War: Legal, Economic, and Scientific Perspectives* (New York: Cambridge University Press, 2000).

19. Charles Bailey, *Agent Orange in Vietnam Program 2012 Report* (New York: Aspen Institute, 2013), <http://www.aspeninstitute.org/sites/default/files/content/upload/Agent%20Orange%20in%20Vietnam%202012%20Report%20-%20EN.pdf>; Ali Mohamed Al-Damkhi, "Kuwait's Oil Well Fires, 1991: Environmental Crime and War," *International Journal of Environmental Studies* 64, no. 1 (2007): 31–44, <http://doi.org/dq88cc>; Tahir Husain, *Kuwaiti Oil Fires: Regional Environmental Perspectives*, 1st ed. (New York: Pergamon, 1995); and UNEP, *Environmental Assessment of the Gaza Strip Following the Escalation of Hostilities in December 2008–January 2009* (Nairobi: UNEP, September 2009), [http://wedocs.unep.org/bitstream/handle/20.500.11822/8736/UNEP\\_Gaza\\_EA.pdf?sequence=2&isAllowed=y](http://wedocs.unep.org/bitstream/handle/20.500.11822/8736/UNEP_Gaza_EA.pdf?sequence=2&isAllowed=y).

20. "Ask IR: How Much Did the Volcanic Eruptions in Iceland in 2010 Cost?," Iceland Review, last updated 30 January 2014, <http://icelandreview.com/stuff/ask-ir/2010/12/06/how-much-did-volcanic-eruptions-iceland-2010-cost>; and Oxford Economics, *The Economic*

*Impacts of Air Travel Restrictions Due to Volcanic Ash* (New York: Oxford Economics, 2010), <http://www.oxfordeconomics.com/publication/open/240242>.

21. Remigio T. Mercado, Jay Bertram T. Lascamana, and Greg L. Pineda, "Socioeconomic Impacts of the Mount Pinatubo Eruption," in *Fire and Mud: Eruptions and Lahars of Mount Pinatubo, Philippines*, ed. Christopher G. Newhall and Raymundo S. Punongbayan (Seattle: University of Washington Press, 1999), <https://pubs.usgs.gov/pinatubo/mercado/>.

22. Eric Feldman, "Introduction to Part IV," in *The Environmental Consequences of War: Legal, Economic, and Scientific Perspectives*, ed. Jay E. Austin and Carl E. Bruch (New York: Cambridge University Press, 2000).

23. Doug W. R. Wallace, Cliff S. Law, Philip W. Boyd, Yves Collos, Peter Croot, Ken Denman, Phoebe J. Lam, Ulf Riebesell, Shigenobu Takeda, and Phil Williamson, *Ocean Fertilization: A Scientific Summary for Policymakers* (Paris: Intergovernmental Oceanographic Commission, 2010), 3; and Canadian Science Advisory Secretariat, *Ocean Fertilization: Mitigating Environmental Impacts of Future Scientific Research* (Ottawa: Fisheries and Oceans Canada, 2010), 2.

24. Wallace et al., *Ocean Fertilization: A Scientific Summary*, 8, 11.

25. NRC, *Reflecting Sunlight to Cool Earth*, 6.

26. Meinhard Doelle, "Climate Geoengineering and Dispute Settlement under UNCLOS and the UNFCCC: Stormy Seas Ahead?" in *Climate Change Impacts on Ocean and Coastal Law: U.S. and International Perspectives*, ed. Randall A. Abate (New York: Oxford University Press, 2015), 345–65.

27. Sirisha Kalidindi, Govindasamy Bala, Angshuman Modak, and Ken Caldeira, "Modeling of Solar Radiation Management: A Comparison of Simulations Using Reduced Solar Constant and Stratospheric Sulphate Aerosols," *Climate Dynamics* 44, nos. 9–10 (2014): 2909–2925, <http://doi.org/f66wcd>; and Nir Y. Krakauer and James T. Randerson, "Do Volcanic Eruptions Enhance or Diminish Net Primary Production? Evidence from Tree Rings," *Global Biogeochemical Cycles* 17, no. 4 (16 December 2003): 29-1–29-11, <http://doi.org/cpkxq6>. For conflicting model results see Daniel S. Cohan, Jin Xu, Roby Greenwald, Michael H. Bergin, and William L. Chameides, "Impact of Atmospheric Aerosol Light Scattering and Absorption on Terrestrial Net Primary Productivity," *Global Biogeochemical Cycles* 16, no. 4 (19 November 2002): 37-1–37-12, <http://doi.org/dpwjrt>.

28. Daniel M. Murphy, "Effect of Stratospheric Aerosols on Direct Sunlight and Implications for Concentrating Solar Power," *Environmental Science & Technology* 43, no. 8 (2009): 2784–2786, <http://doi.org/cw4fqm>.

29. Patricia Heckendorn, D. Weisenstein, S. Fueglistaler, B.P. Luo, E. Rozanov, M. Schraner, L. W. Thomason, and T. Peter, "The Impact of Geoengineering Aerosols on Stratospheric Temperature and Ozone," *Environmental Research Letters* 4, no. 4 (2009): 11, <http://doi.org/b6x4v8>; see also Bijal Trivedi, "Hacking Earth Against Warming, Scientists Favor Fake Volcanoes," *Popular Mechanics*, 30 September 2009, [www.popularmechanics.com/science/environment/4267288](http://www.popularmechanics.com/science/environment/4267288); Kunzig, "Sunshade"; and Utibe Effiong and Richard L. Neitzel, "Assessing the Direct Occupational and Public Health Impacts of Solar Radiation Management with Stratospheric Aerosols," *Environmental Health* 15, no. 7 (2016): <http://doi.org/f76tb9>.

30. E. Baughman, Anand Gnanadesikan, Arthur T. Degatano, and Alistair Adcroft, "Investigation of the Surface and Circulation Impacts of Cloud-Brightening Geoengineering," *Journal of Climate* 25 (2010): 7527–7543, <http://doi.org/ck66>.

31. Kelly E. McCusker, Kyle C. Armour, Cecilia M. Bitz, and David S. Battisti, "Rapid and Extensive Warming Following Cessation of Solar Radiation Management," *Environmental Research Letters* 9 (2014), <http://doi.org/ck67>.

32. The Geoengineering Research Evaluation Act of 2017, H.R. 4586, 115th Cong., 1st sess. (7 December 2017), <https://www.congress.gov/bill/115th-congress/house-bill/4586/text?r=1>.
33. International Maritime Organization, "Marine Geoengineering: Guidance and Amendments under the London Convention/Protocol," accessed 28 February 2018, <http://www.imo.org/en/OurWork/Environment/LCLP/EmergingIssues/geoengineering/Pages/default.aspx>. For information on the 2009 LOHAFEX experiment, see "The Law of the Sea," Editorial, *Nature Geoscience* 2 (March 2009): 153, <http://doi.org/dhppwm>; and Richard Black, "Setback for Climate Technical Fix," BBC News, 23 March 2009, <http://news.bbc.co.uk/go/pr/fr/-/2/hi/science/nature/7959570.stm>.
34. Convention on Biological Diversity (COP), "Decision X/33: Biodiversity and Climate Change" (Tenth Meeting of the Conference of the Parties to the COP, Nagoya, Japan, 18–29 October 2010), <https://www.cbd.int/decision/cop/?id=12299>.
35. Secretariat of the Convention on Biological Diversity (SCBD), *Update on Climate Geoengineering in Relation to the Convention on Biological Diversity: Potential Impacts and Regulatory Framework* (Montreal: SCBD, 2016), <https://www.cbd.int/doc/publications/cbd-ts-84-en.pdf>.
36. UN, Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification (ENMOD) Techniques, Article I, accessed 7 March 2018, <http://www.un-documents.net/enmod.htm>.
37. For expectations of weather-related warfare and now-irrelevance of the ENMOD, see Robert A. Francis and Krishna Krishnamurthy, "Human Conflict and Ecosystem Services: Finding the Environmental Price of Warfare," *International Affairs* 90, no. 4 (2014): 853–69, <http://doi.org/f598mx>.
38. Nils Melzer, *International Humanitarian Law: A Comprehensive Introduction* (Geneva: International Committee of the Red Cross, August 2016), 96–97; see also International Committee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Norwell, MA: Kluwer Academic Publishers, 1987).
39. ICRC, "Treaties, State Parties and Commentaries, Protocol Additional to the Geneva Conventions of 12 August 1949 and Relation to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977," <https://www.icrc.org/ihl.nsf/INTRO/470>.
40. Bill McKibben, "A World at War," *New Republic*, 15 August 2016, <https://newrepublic.com/article/135684/declare-war-climate-change-mobilize-wwii>.
41. See, for example, Thomas Aquinas, *Summa Theologiae*, pt. II-II, questions 40, 64; Francisco de Vitoria, "On the Law of War," in *Vitoria: Political Writings*, ed. Anthony Pagden and Jeremy Lawrance (New York: Cambridge University Press, 1991): 295–327; Hugo Grotius, *The Rights of War and Peace* [De Jure Belli ac Pacis], trans. A. C. Campbell (Washington, DC: M. Walter Dunne, 1901), particularly bk. 2, chap. 22, and bk. 3, chap. 1; Samuel Pufendorf, "On the Law of Nature and of Nations," in *The Political Writings of Samuel Pufendorf*, ed. Craig L. Carr, trans. Michael J. Seidler (New York: Oxford University Press, 1994), particularly bk. 8, chap. 6; National Conference of Catholic Bishops (NCCB), *The Challenge of Peace: God's Promise and Our Response* (Washington, DC: NCCB, 1983); Michael Walzer, *Just and Unjust Wars: a Moral Argument with Historical Illustrations*, 3rd ed. (New York: Basic Books, 2000); Brian Orend, *War and International Justice: A Kantian Perspective* (Waterloo, ON: Wilfrid Laurier University Press, 2000).
42. Mark Douglas, "Changing the Rules: Just War Theory in the Twenty-First Century," *Theology Today* 59, no. 44 (January 2003): 529–45, <http://doi.org/d2gc3v>.
43. In July 2012, a geoengineer named Russ George conducted an independent OIF experiment off the coast of British Columbia. Canada claimed this was illegal, while George maintains it was proper. David Biello, "Pacific Ocean Hacker Speaks Out," *Scientific Ameri-*

can 307, no. 4 (24 October 2012), <https://www.scientificamerican.com/article/questions-and-answers-with-rogue-geoengineer-carbon-entrepreneur-russ-george/>.

44. Rules 11 and 12 prohibit indiscriminate attacks, and Rule 71 describes weapons that are by nature indiscriminate. For a full discussion of international humanitarian law (IHL) rules, see International Committee of the Red Cross (ICRC), “IHL Database: Customary IHL,” accessed 6 March 2018, <https://ihl-databases.icrc.org/customary-ihl/eng/docs/home>; on the role of the International Criminal Court (ICC) in IHL, see ICRC, “International Criminal Court,” accessed 6 March 2018, <https://www.icrc.org/en/war-and-law/international-criminal-jurisdiction/international-criminal-court>.

45. Clive Oppenheimer, “Climatic, Environmental, and Human Consequences of the Largest Known Historic Eruption: Tambora Volcano (Indonesia) 1815,” *Progress in Physical Geography* 27, no. 2 (2003): 230–59, <https://doi.org/10.1191/0309133303pp379ra>; and Gregory C. Unruh, “Understanding Carbon Lock-In,” *Energy Policy* 28, no. 2 (September 2000): 817–30, <http://doi.org/fj28sw>.

46. Angus J. Ferraro, Eleanor J. Highwood, and Andrew Charlton-Perez, “Weakened Tropical Circulation and Reduced Precipitation in Response to Geoengineering,” *Environmental Research Letters* 9 (2014), <http://iopscience.iop.org/article/10.1088/1748-9326/9/1/014001>; McCusker et al, “Rapid and Extensive Warming”; Heckendorn et al, “Impact of Geoengineering Aerosols”; Alan Robock, Luke Oman, and Georgiy L. Stenchikov, “Regional Climate Responses to Geoengineering with Tropical and Arctic SO<sub>2</sub> Injections,” *Journal of Geophysical Research* 113 (2008): D16101, <http://doi.org/ct2dcq>; D. L. Lunt, A. Ridgwell, P. J. Valdes, and A. Seale, “Sunshade World: A Fully Coupled GCM Evaluation of the Climatic Impacts of Geoengineering,” *Geophysical Research Letters* 35 (2008): L12710, <http://doi.org/b6v8t8>; and for conflicting model results, see Long Cao, Lei Duan, Govindasamy Bala, and Ken Caldeira, “Simulated Long-Term Climate Response to Idealized Solar Geoengineering,” *Geophysical Research Letters* 43 (2016): 2209–2217, <http://doi.org/f8fzgm>.

47. Whether or not the environmental protection norms contained in ENMOD are considered customary international law, and hence automatically binding on all states, is an open question and beyond the scope of this paper.

48. UN, *Rome Statute of the International Criminal Court* (Rome: UN Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court, 17 July 1998), [https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome\\_statute\\_english.pdf](https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_english.pdf). The 1998 Statute Article 8, Para 2(iv) states, “For the purposes of this statute, war crimes means . . . intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment that would be clearly excessive in relation to the concrete and direct overall military advantage anticipated.”

49. Adam Taylor, “Is Environmental Destruction a Crime Against Humanity? The ICC May Be about to Find Out,” *Washington Post*, 16 September 2016, <https://www.washingtonpost.com/news/worldviews/wp/2016/09/16/is-environmental-destruction-a-crime-against-humanity-the-icc-may-be-about-to-find-out/>.

50. Jane C. S. Long, Frank Loy, and M. Granger Morgan, “Policy: Start Research on Climate Engineering,” *Nature* 518 (5 February 2015): 29–31, <http://doi.org/ck3g>; and NRC, *Carbon Dioxide Removal and Reliable Sequestration and Reflecting Sunlight to Cool Earth*.

# Space Arms Control: A Hybrid Approach

*Brian G. Chow*

## Abstract

Space arms control proposals such as the Prevention of the Placement of Weapons in Outer Space (PPWT) have failed to become treaties in spite of countless efforts over the past 50 years. These proposals will not work in the emerging space proximity-operations era. This article proposes a hybrid approach to space arms control based on restricting the locations in space of some potential space weapons while banning other types of space weapons outright. The core of any hybrid space arms control (HSAC) treaty should prohibit satellites, whether for antisatellite (ASAT) or peaceful purposes, from positioning too close to more than an innocuous threshold number of another country's satellites and authorize preemptive self-defense as a last resort countermeasure. This article also proposes a comprehensive list of space arms control measures, which can be added to the core proposal to more effectively manage both traditional and emerging space weapons.

\*\*\*\*\*

In June 2018, the United Nations Office for Outer Space Affairs will celebrate the 50th anniversary of the first United Nations Conference on the Exploration and Peaceful Uses of Outer Space. The conference is an opportunity “for the international community to gather and consider the future course of global cooperation for the benefit of humankind.”<sup>1</sup> Indeed, there is much to celebrate since the space age began because the world has reaped abundant benefits from satellites. We have established five treaties and a number of transparency and confidence-building measures for space activities.<sup>2</sup> But, in spite of countless efforts,

---

Brian G. Chow is an independent policy analyst with over 25 years as a senior physical scientist specializing in space and national security. He holds a PhD in physics from Case Western Reserve University and an MBA with distinction and PhD in finance from the University of Michigan. This piece builds on Chow's previous *Strategic Studies Quarterly* article, “Stalkers in Space: Defeating the Threat,” Summer 2017. Contact at: [brianchow.sp@gmail.com](mailto:brianchow.sp@gmail.com).

these treaties and measures focus on civil and commercial activities and cannot control space weapons other than weapons of mass destruction in orbit. One of the greatest emerging threats in space comes from unmanned proximity operations. These operations require maneuvering a spacecraft close enough to another object in space to make physical contact with the other object or affect the object in some way.<sup>3</sup> To date, the intent of unmanned proximity operations has been for peaceful purposes such as active debris removal (ADR) or on-orbit servicing (OOS). However, a spacecraft that can perform ADR or OOS can also be readily commanded to grapple and destroy an adversary's satellite. Currently the United States, China, Russia, the European Union, and other countries are pursuing R&D programs for satellites to perform ADR and OOS. Each nation is planning to provide such services in early 2020 and beyond. To perform these peaceful services, a country needs to master the skill of unmanned proximity operations.

In a 2017 *Strategic Studies Quarterly* article, I argued that antisatellite weapons (ASAT), called space stalkers, could be placed on orbit in peacetime and maneuvered to tailgate US satellites during a crisis and attack from such close proximity that the United States would not have time to prevent damage.<sup>4</sup> I further argued that deterring and defending against space stalkers would require prohibiting satellites, whether for antisatellite or peaceful purposes, from being too close to more than an innocuous threshold number of another country's satellites. Today, more arms control measures should be implemented to further improve effectiveness and affordability in dealing not only with space stalkers, but other emerging space weapons as well. Without successful arms control, our continued "peaceful uses of outer space" will be in jeopardy. During 2018, the international community should take advantage of the seriousness and enthusiasm of the momentous 50th anniversary to establish an initiative for a new approach to space arms control. A hybrid space arms control (HSAC) treaty is needed because current proposals have not worked and will not work in the future. Moreover, implementing effective space arms control is urgent because by early 2020, ADR and OOS demonstrations will be completed, regular services will begin, and these spacecraft can be used as space stalkers.

This article first describes the emerging proximity operations era and the problems with traditional space arms control. Then, it presents the core of a hybrid space arms control treaty. Next it proposes additional

HSAC measures to complement the core proposal. Finally, the article arrays space weapons into six categories that could help manage space weapons, creating the ultimate hybrid space arms control. Taken together, the hybrid approach proposed here will help expand the peaceful benefits from space without the threat of space weapons in the emerging proximity-operations era.

## **The Emerging Proximity-Operations Era and Traditional Space Arms Control**

Since 2007, the United Nations Committee on the Peaceful Uses of Outer Space has adopted a set of space debris mitigation guidelines.<sup>5</sup> These guidelines are important and necessary but not sufficient to deal with the growing space debris problem. Following the well-accepted Kessler Syndrome theory,<sup>6</sup> NASA scientist J.-C. Liou found that, if active debris removal starts in 2020 with an annual removal rate of 5 massive intact objects (such as decommissioned satellites and derelict rocket bodies), debris population in the low Earth orbits (LEO) would stabilize over the next 200 years.<sup>7</sup> Space scientist Nicholas Johnson concluded that “in the long term, the removal of large orbital debris will be essential to the sustainability of space operations.”<sup>8</sup> Studies at the European Space Agency arrived at a rate “on the order of 5-10 objects” per year.<sup>9</sup> A report based on the Third International Interdisciplinary Space Debris Congress arrived at a rate of 9.1 objects per year.<sup>10</sup> Thus, all these major studies are consistent that roughly a high single-digit number of massive intact objects per year needs to be removed.

However, these studies did not consider the recent dramatic growth of 14,000 to 16,000 small satellites to be launched into LEOs over the next 10 years—in contrast to merely 1,071 LEO satellites of any size worldwide as of 31 August 2017.<sup>11</sup> Extrapolating from the estimate by scientist H. G. Lewis and his team that about one additional intact object needs to be removed per year for the additional 1,080 small LEO satellites they analyzed, I estimate that about 14 additional removals are required for the additional 14,000 to 16,000 small satellites.<sup>12</sup> Adding this to the earlier single-digit removal produces the need to remove about two dozen massive intact objects every year to keep space debris from increasing and to ensure the debris environment remains suitable for peaceful uses. However, uncertainties in prediction and provision of

a safety margin could increase debris removal demand, which in any case should be monitored and updated regularly.

In June 2016, Xinhua, the official press agency of China, reported that onboard the inaugural launch of a new generation carrier rocket Long March-7 was an “Aolong-1” spacecraft, which was a demonstrator of space debris cleaning.<sup>13</sup> It re-entered the atmosphere on 27 August 2016 after completing a short-duration demonstration mission.<sup>14</sup> Spaceflight 101.com reported “according to Chinese space officials, Aolong-1 is only the first in a series of satellites tasked with the collection of space debris as the country develops the technology needed to retrieve small debris up to [the size of an] entire spacecraft to be safely brought to a destructive re-entry.”<sup>15</sup> The European Union also has a program to demonstrate the removal of space debris and aims to remove the defunct 8-ton remote-sensing satellite Envisat from LEO around 2023.<sup>16</sup> In essence these developments and others by major spacefaring nations mean that the space will be weaponized by early 2020, even if we do not count demonstrators as weapons.

In addition to debris removal, countries are pursuing on-orbit servicing. For example, the Defense Advanced Research Projects Agency (DARPA) Robotic Servicing of Geosynchronous Satellites R&D program aims to provide services including high-resolution inspection; correction of some types of mechanical anomalies, such as solar array and antenna deployment malfunctions; relocation and other orbital maneuvers; installation of attachable payloads to enable upgrades or new capabilities; and refueling to extend the service life of satellites.<sup>17</sup>

The United States and China will likely complete their developmental and demonstration OOS programs and provide services such as refueling also in the early 2020s. Once any country has such a spacecraft in orbit, there is no reason to deny other countries following suit for commercial and/or national security purposes. Since OOS spacecraft will have rendezvous and robotic capabilities even more advanced than those for ADR, they become even more threatening as space stalkers. In effect, weaponization of space will happen by default in the early 2020s and beyond and will be unavoidable and irreversible.

### **Traditional Space Arms Control Ineffective**

In the emerging space proximity-operations era, space weapons will be technically synonymous with ADR and OOS. The difference is in



the intent of whether such spacecraft are used for peaceful or ASAT purposes. Our space defense and deterrence cannot count on adversaries to always have peaceful intent. Also, in the emerging era, traditional space arms control will not be able to prevent weapons in space. Article IV of the Outer Space Treaty states that “State Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction.”<sup>18</sup> While it is critical to ban weapons of mass destruction in space, subsequent treaties and transparency and confidence-building measures have done little to control or ban the placement of conventional weapons in space. Treaty proposals under consideration by the United Nations are mainly those proposed by Russia and China.

Russia and China have been taking the lead to ban weapons in space. Their latest version of the draft Prevention of the Placement of Weapons in Outer Space treaty (PPWT, hereafter the Prevention Treaty) was issued 12 June 2014.<sup>19</sup> On 3 September 2014, the US analysis submitted to the Conference on Disarmament stated, “The draft PPWT (CD/1985) proposed by Russia and China, like the 2008 version, remains fundamentally flawed.” It concluded that “the United States has determined that the 2014 draft PPWT does not satisfy the President’s criteria in the 2010 US National Space Policy for considering space arms control concepts and proposals, namely, that they must be equitable, effectively verifiable, and enhance the national security of the United States and its allies.”<sup>20</sup> This conclusion is based on three major reasons.

First, the United States stated: “There is no integral verification regime to help monitor or verify the limitation on the placement of weapons in space. . . . Moreover, the United States has maintained that it is not possible with existing technologies or cooperative measures to effectively verify an agreement banning space-based weapons.”<sup>21</sup> Russia and China responded that “PPWT is similar to the provision of the Outer Space Treaty of 1967. . . . The Outer Space Treaty does not provide for any mechanism for verifying the fulfilment of this obligation and during the half a century that it has been in force no questions about verification have been raised.”<sup>22</sup> Basically, the United States insists on verification, but Russia and China argue that, if no country including the United States complains about the lack of verification for the Outer Space Treaty, the United States should not demand a verification regime for the Prevention Treaty. Russia and China actually do not object to

verification—if it is possible. As they stated: “However, we continue to believe that the development of a verification mechanism would be desirable for the subsequent full implementation of PPWT.”<sup>23</sup>

Second, the United States stated: “Typically, arms control treaties that prohibit the deployment of a class of weapon also prohibit the possession, testing, production, and stockpiling of such weapons to prevent a country from rapidly breaking out of such treaties. The PPWT contains no such prohibitions and thus a Party could develop a readily deployable space-based weapons break-out capability.”<sup>24</sup> Russia and China responded that:

The Russian Federation and the People’s Republic of China maintain that the prohibition against the possession, testing, production and stockpiling of space-based weapons does not contradict the purposes of PPWT. Furthermore, one of the principles that guided defining the scope of the treaty consisted in setting limitations that could be monitored. (Such monitoring capability is dealt with, for example, in document CD/1785 submitted by Canada in 2006.) Effective monitoring of ‘research, development, production, and terrestrial storage of space-based weapons’ — on which there is no prohibition, as is pointed out in the United States document — is not feasible in practical terms for objective reasons.<sup>25</sup>

Basically, Russia and China do not object to “prohibit the possession, testing, production and stockpiling of such weapons,” as the United States insists. Rather they are being practical “in setting limitations that could be monitored.” Thus, Russia and China should have no objection that the prohibition of tailgating another country’s satellites can be observed and thereby, monitored.

Third, the United States claimed: “The Treaty does not address the most pressing, existing threat to outer space systems: terrestrially-based anti-satellite weapon systems. There is no prohibition on the research, development, testing, production, storage, or deployment of terrestrially-based anti-satellite weapons; thus, such capabilities could be used to substitute for, and perform the functions of, space-based weapons.”<sup>26</sup> Russia and China responded that,

While anti-satellite weapons as a class of weapons are not prohibited under the draft PPWT, the proliferation of such weapons is restricted through a comprehensive ban on the placement in outer space of weapons of any kind, including anti-satellite weapons. A ban on ground-based anti-satellite (ASAT) weapon systems has been introduced into PPWT through the ban on the use of force, regardless of its source, against space objects.<sup>27</sup>

Russia and China argue that ground-based ASATs are covered in the draft Prevention Treaty “through the ban on the use of force.” They clarify their argument by stating that “Furthermore, we would like to emphasize that in acceding to PPWT . . . the placement of weapons of any kind in outer space and the use or threat of force are prohibited.”<sup>28</sup> Russia and China have made three additional important observations in their response to the US analysis of the Prevention Treaty:

1. There is a need for “reaching a common understanding of the right to self-defense under the Charter as regards outer space in the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS).”
2. “Furthermore, it is worth noting that the Charter was drafted before the space age had begun and, consequently, in our view, the unqualified and direct application of the provisions of the Charter to such a sensitive area of international relations as outer space development requires further elaboration and clarification through negotiation between States.”
3. There is “the need for clarification of the issue of the use of force in outer space on the grounds provided for under the Charter.”<sup>29</sup>

### **“No First Placement” Initiative Led by Russia**

On 7 December 2015, the United Nations General Assembly adopted Resolution 70/27 entitled “No first placement of weapons in outer space.” It “Encourages all States, especially spacefaring nations, to consider the possibility of upholding as appropriate a political commitment not to be the first to place weapons in outer space.”<sup>30</sup> Ambassador Robert Wood, US Permanent Representative to the Conference on Disarmament, explained that the resolution “does not adequately define space weapons, leaving the nonbinding resolution difficult to enforce, or for compliance with the agreed-upon measures to be verified.”<sup>31</sup> Indeed, space weapons undefined or ambiguously defined has been an ongoing problem in both the no first placement initiative and the proposed Prevention Treaty. Since the same spacecraft designed for debris removal or servicing can readily serve as a space weapon at a moment’s notice, no first placement of weapons in space would amount to no ADR and OOS, which is incompatible with reality. However, a hybrid space arms

control approach that allows ADR and OOS spacecraft but prohibits close proximity to another country's satellites offers a win-win solution. The common ground among the United States, Russia, and China can be used to form the basis for a hybrid approach.

### **The Core of Hybrid Space Arms Control**

While the Outer Space Treaty of 1967 bans weapons of mass destruction in space, there has been little success in controlling conventional space weapons in spite of substantial efforts led by Russia and China over the last 50 years. The United States has yet to offer a viable alternative proposal and has been relegated to a naysayer with diminishing support from other countries, including its allies and friends. For example, on 30 October 2014, the United Nations Disarmament Committee approved the text of a draft resolution to the General Assembly to urge an early start to substantive work on the 2014 updated draft Prevention Treaty. The recorded vote was 126 in favor to 4 against (Israel, Ukraine, United States, Georgia). The European Union, Australia, Japan, South Korea, and others totaled 46 abstentions. The committee also approved the draft resolution on No First Placement Initiative with identical recorded votes. Further, the committee approved the draft resolution on the Prevention of An Arms Race in Outer Space by a recorded vote of 180 in favor to none against, with 2 abstentions (United States and Israel).<sup>32</sup> By proposing and actively pursuing practical space arms control, the United States can regain leadership and worldwide support to ensure beneficial space activities without the dangerous side effects of space weapons.

The current US national space strategy cannot deal with the space stalker threat.<sup>33</sup> However, a new space arms control proposal can deter and defend against space stalkers, while the United States and other countries continue to use their existing and developing strategies and assets to deal with traditional threats such as ground-launched ASATs as well as other new threats such as cyberattack.

This new space arms control differs from traditional approaches such as those proposed by Russia and China, in four important ways:

1. Some space weapons cannot be banned.
2. Non-bannable space weapons can still be controlled.
3. Treaty verification is required.

4. Self-defense should be allowed after treaty violation before or after actual attack.

### **Non-Bannable Space Weapons in the Emerging Era**

The proposed Prevention Treaty defines weapon in outer space as “any outer space object or component thereof which has been produced or converted to destroy, damage or disrupt normal functioning of objects in outer space, on the Earth’s surface or in its atmosphere.”<sup>34</sup> According to the Prevention Treaty, space stalkers would be prevented from being placed in space. Unfortunately, once ADR or OOS spacecraft are deployed in space, the same spacecraft can be simply retasked, maneuver near any other country’s satellites for space stalking, and attack upon command. Therefore, abiding by the Prevention Treaty would imply banning the placement of ADR and OOS satellites.

There are three reasons the United States should not attempt to ban debris removal and servicing spacecraft to deal with space stalking threat. First, ADR spacecraft are necessary in the emerging era to prevent the space debris population from increasing and hindering the peaceful uses of space. Also, as space technologies continue to become more capable and less expensive, it is highly advantageous to have some satellite services performed in space. Second, as noted earlier, China will likely deploy both ADR and OOS spacecraft in the early 2020s and Russia is likely to follow suit in the 2020s. Even if the United States wanted to delay ADR and OOS deployment for the benefit of preventing space stalker threat, it could not dissuade China and Russia from such a deployment. Third, and most importantly, there is a way to both deter and defend against space stalkers and still be able to benefit from the presence of ADR and OOS spacecraft.

### **Controlling Non-Bannable Space Weapons**

Space weapons being non-bannable does not mean they are uncontrollable. Space stalkers can be controlled by prohibiting them from being simultaneously placed too close to and threatening another country’s satellites. For example, if the United States wants to deter and defend against simultaneous space-stalking attacks against geosynchronous Earth orbit (GEO) satellites, it could declare that any country positioning its space objects of any kind (i.e. whether space stalker or ordinary

satellite, as one cannot reliably distinguish them once they are in space) within 0.2 degree in longitude (148 km in minimum separation) or inclination of more than a threshold number of another country's satellites as an aggressor. The minimum degree separation requirement should be determined and approved by the DOD before State Department negotiations with the international community. The defender would also have the right to exercise self-defense as the last resort even before an actual attack. Additionally, countries should coordinate and limit the number of ADR and OOS spacecraft in space, as a larger number would increase the possible space stalker threat. It is feasible to arrive at both useful and practical limits. For example, both the United States and China need not reposition any of their operational satellites to observe the above suggested rule of 0.2 degree minimum satellite separation between any pair of US-China GEO satellites.<sup>35</sup>

In sum, China, Russia, and the United States likely agree that ADR and OOS will be needed for essential space missions in the 2020s and beyond. China and Russia will recognize that “a ban on the placement of weapons of any kind in outer space” is no longer possible since ADR and OOS spacecraft can be retasked as weapons.<sup>36</sup> Placing satellites—whether weapons or nonweapons—in space but restricting their locations may well be the only viable alternative to control them. This core or foundational proposal can keep the peaceful and important services of ADR and OOS spacecraft while not allowing them to morph into a space stalker threat. As any country can be threatened by space stalkers, all countries will benefit from controlling them.

### **Treaty Verification Required**

President Reagan's favorite adage, “Trust, but verify,” applies to space treaties as well. The United States insists on verification, while Russia and China do not include it in the proposed Prevention Treaty because verification is not possible in their formulation. However, Russia and China “believe that the development of a verification mechanism would be desirable.”<sup>37</sup> Since compliance and violation of a ‘no simultaneous tailgating’ provision can be detected and monitored, the United States, China, and Russia as well as other countries can find verification of this foundational proposal desirable and agreeable. The hybrid approach can resolve the verification issue by allowing certain weapons to be space based but prohibiting their being too closely placed (e.g. within 0.2

degree in longitude or inclination) to another country's satellites. By banning space weapons being too close instead of outright, the United States should find that it is "possible with existing technologies and/or cooperative measures," such as space surveillance systems and requiring ADR/OOS spacecraft to broadcast their positions 24/7, "to effectively verify an agreement banning space-based weapons" being too close to US satellites.<sup>38</sup> Thus, the US condition for verification is satisfied.

At the same time, the United States should understand that "the possession, testing, production, and stockpiling" of some weapons, such as space stalkers, does not lead to "rapidly breaking out of" the hybrid treaty since it is not broken (rather alerted) by the rapidly increased number of space stalkers present in space, but by space stalkers being too close to US satellites. Finally, compared to the current state of no space arms control, a hybrid approach that restricts placement locations would be far better.

### **Right of Self-Defense**

The international community is ambiguous whether a country is allowed to tailgate any number of another country's satellites. Also, the current US national security space strategy is ambiguous about preemptive self-defense, including when it faces a threat from space stalkers.<sup>39</sup> Under these two dangerous ambiguities, China could reason that space stalkers would be the best type of ASATs to present the United States with two bad choices. First, the United States could preemptively destroy the space stalkers to save the targeted satellites so as to maintain space support to military operations during crisis and war. However, without discussing and resolving these two ambiguities with the international community in peacetime, the United States could be condemned as the aggressor who fired the first shot, which led to a war in space possibly spreading to Earth—something both sides tried to avoid. Second, the United States could fight ineffectively without the support of some critical satellites. Facing these two bad choices, the United States might end up not intervening at all. This would be the perfect outcome for China, as it prevented US intervention without firing a single shot.

To attain space security in the emerging era, the world needs to remove these two ambiguities now. First, countries should agree and declare, in peacetime, that the country that positions real or plausible space stalkers to simultaneously threaten another country's satellites is

considered the aggressor. Second, the country whose satellites are under such a threat has the right of preemptive self-defense as a last resort to disable the threat.

So, what should be the common understanding of the right to self-defense under the charter as regards outer space? The self-defense doctrine for US policies in space and on Earth, as well as other nations' policies, has long been strongly influenced by Article 51 of the United Nations Charter: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if armed attack occurs against a Member of the United Nations."<sup>40</sup> Georgetown University professor of government and foreign service Anthony Arend stated, "Although the basic contours of Article 51 seem straightforward, its effect on the customary right of anticipatory self-defense is unclear."<sup>41</sup> There are two interpretations: restrictive and broad of "armed attack occurs" in Article 51. Legal scholars, who are proponents of a restrictive interpretation, allow self-defense only after attack has started. Other legal scholars take a broad view that the charter does not "impair the inherent right" embedded in the customary international laws, which allow anticipatory or preemptive self-defense if certain conditions are met. Typical conditions were suggested as far back as 1842 by US Secretary of State Daniel Webster in the Caroline case. Subsequently, jurists like Roberto Ago in 1980 came to a similar set of conditions: "necessity," "proportionality," and "immediacy."<sup>42</sup> The 9/11 terrorist attacks in 2001 confirmed the need of preemptive self-defense in specific situations and led to the 2002 US National Security Strategy: "For centuries, international law recognized that nations need not suffer an attack before they can lawfully take action to defend themselves against forces that present an imminent danger of attack."<sup>43</sup> This premise should apply to preemptive self-defense against space stalkers as well because Ago's three conditions are met.<sup>44</sup> Thus, preemption against space stalkers would comply with the broad view of Article 51. However, for those insisting on its restrictive interpretation, the United States should respond that such an interpretation drafted in October 1945 understandably could not anticipate and counter the space stalker threat seven decades later. As quoted earlier, Russia and China observed that "the [United Nations] Charter was drafted before the space age" and that the "application of the provisions of the Charter" to "outer space development requires further elaboration and clarification."<sup>45</sup> Article 51 was designed against armed attack that takes time



to prepare and gives warning by the massing of soldiers and weapon systems for an attack. The defender would have alternative responses, including the referral of the threat to the United Nations for peaceful resolution. Articles VI and VII of the Prevention Treaty also recommend “assistance of the executive organization of the Treaty, submitting relevant evidence for further consideration of the dispute, which includes the claim that a violation of the Treaty is taking place.”<sup>46</sup> However, in the case of space stalkers, there is no time for referral and no means other than preemption to neutralize the imminent threat.

In sum, the common understanding of the right to self-defense should include the preemption of space stalkers. Should Russia, China, and/or the United States reject such preemptive actions, they need to offer a viable alternative and explain why the alternative is more practical and effective than the one proposed here.

### **Benefits of the Hybrid Core**

The foundational or core proposal is a significant improvement in three ways. First, it is better than the status quo of no space arms control at all. Currently, the world is ambiguous whether space stalking is threatening or peaceful and whether preemption as last resort is defensive or a pretext for aggression. Consequently, a country could be tempted to use space stalkers to prevent a third country’s intervention in a conflict or intimidate its adversary into submission. The use of space stalking could create crisis instability and trigger a war in space and on Earth that could kill untold numbers of combatants and noncombatants. The core proposal clarifies and condemns space stalking as aggression and permits preemption. It unambiguously informs the aggressor that blackmailing with space stalkers is destabilizing and, in any case, futile.

Second, Russia and China stated that the purpose of the Prevention Treaty is “very specific: a ban on the placement of weapons of any kind in outer space and a ban on the use of force or threat of the use of force against outer space objects.”<sup>47</sup> Thus, the means is banning “placement of weapons,” while the goal is banning “the use of force or threat of the use of force.” However, the means of the Prevention Treaty is not possible in the presence of ADR and OOS satellites in the emerging era of proximity operations. Most interestingly, by replacing the means of outright banning with prohibiting the threatening configuration of space stalking, the foundational proposal can now attain the goal of PPWT.

China and Russia, as well as the United States, should find that the foundational proposal offers a viable new means to attain their ultimate goal of banning “the use of force or threat of the use of force against outer space objects.”

Third, if the foundational proposal fails to gain support from countries such as China and Russia, the proposal could still have a second chance to turn into a treaty. As long as the United States gains overwhelming support from its allies and friends, it can still declare that it will unilaterally observe the proposal, namely, that it will not pose a space stalking threat to another country’s satellites but that it will reserve the right of preemption as the last resort if its satellites are threatened by space stalkers. Once the United States adopts this policy, the space stalking threat would no longer deter US intervention. Naturally, China and Russia could have preferred no change in US space security strategy so as to maintain the potency and leverage of their space stalkers. However, once the foundational proposal rendered space stalkers ineffective, China and Russia could decide it would be better to join the proposed treaty. In sum, the foundational proposal deters and defends against space stalkers that cannot be banned from space in the emerging era of unmanned, close proximity operations.

### **Additional HSAC Measures**

Additional control measures can improve deterrence and defense against not only space stalkers but also many of the traditional and new threats. The United States and other countries need to consider and decide which ones should be added to the foundational or core proposal. Control measures described below start with those that are relatively easy then progress to those far more difficult to implement but which could control space weapons far more effectively and affordably.

### **Facilitating the Monitoring of ADR and OOS Spacecraft**

The following measures can make verification easier for any country that is concerned about an adversary’s ADR and OOS spacecraft being repurposed temporarily or permanently as space stalkers. First, each of these spacecraft, as well as its technical and performance description relevant to ascertaining potential ASAT capability, should be submitted to the secretary-general for inclusion in the United Nations Register, as

over 92 percent of all prior satellites have been.<sup>48</sup> However, this control measure should be made more acceptable to some countries by not allowing it to be used to reveal capabilities such as sensor resolution that are proprietary and/or military sensitive but not critical for determining a satellite's potential ASAT capability. Since the maintenance of the Register had been delegated to the United Nations Office for Outer Space Affairs (UNOOSA), these ADR and OOS data can be managed by the same office as well. Second, each ADR or OOS spacecraft should be required to make its location and orbital track known to the public and the spacecraft should be easily detectable 24/7 by broadcasting its position. Third, the service provider or owner will preannounce to the public the itinerary of any repositioning well before the journey starts so any country can prepare for defense accordingly, should the precaution be necessary. These measures to facilitate monitoring are consistent with, but go beyond, Guideline 6, "Enhance the Practice of Registering Space Objects," in "Guidelines agreed by the United Nations Working Group on the Long-term Sustainability of Outer Space Activities (UNWG Guidelines)" to "be used as the basis for producing the next official version of the guidelines for the long-term sustainability of outer space activities."<sup>49</sup>

Perhaps some countries and spacecraft owners prefer to keep some information such as a spacecraft's new destination private. One option is to exempt a pre-agreed number of ADR and OOS spacecraft from preannouncement and even registration. However, there seems little justification for any exemption as an ADR mission is for common good and should be public knowledge. As to OOS spacecraft, even if one wanted to keep the maintenance and repair record of a satellite, especially a military one, confidential, one could still preannounce the OOS spacecraft's new destination but mask the record by adding some unnecessary visits to the satellite being serviced.

### **Prohibiting Test of Simultaneous Unmanned Proximity Operations**

On-orbit testing and demonstration are required for the deployment and upgrades of proximity operations including robotics. However, there is little need over the next decade to test or perform multiple peaceful ADR or OOS missions simultaneously. Yet, such simultaneous activities would greatly facilitate these spacecraft being repurposed for simultaneous space stalking that any space arms control for the emerging era

would need to prevent. Should hybrid space arms control become a treaty and remain in place for several years, this testing prohibition can be relaxed to allow simultaneous ADR or OOS missions.

### **Prohibiting Ground-Launched Ballistic-Missile ASAT Tests**

As discussed, the United States stated, “The Treaty [PPWT] does not address the most pressing, existing threat to outer space systems: terrestrially-based anti-satellite weapon systems.”<sup>50</sup> Two possible control measures exist. First, countries may consider banning further ground-launched (i.e. terrestrially based) ballistic-missile ASAT tests. Since testing in space is observable and verifiable, the test ban can result in slower development or upgrade of such ASATs. But, since the United States withdrew from the 1972 Anti-Ballistic Missile Treaty on 13 June 2002, this control measure would also affect the testing of ground-launched ballistic-missile defense systems. One compromise is to take advantage of the fact that the maximum apogee altitude is around 1,300 km for a non-lofted ICBM with a range of about 10,000 km.<sup>51</sup> The apogee actually is lower for ranges greater than 10,000 km.<sup>52</sup> Thus, a control measure can prohibit all ballistic missile intercept tests against both real or virtual targets, whether for ASAT or any other purpose such as missile defense, above 2,000 km (the upper limit of LEOs).<sup>53</sup> This prohibition would reduce the ground-launched, ballistic-missile ASAT threat to medium Earth orbit (MEO) and GEO satellites yet would not prevent tests of ground-launched ballistic-missile defense system against ballistic missiles of any range.

Second, even if countries decide to remain silent about banning all ground-launched, ballistic-missile ASAT tests as in the Prevention Treaty, they can still consider banning simultaneous tests for the same reasons as the above measure for banning test of simultaneous proximity operations. However, countries that want to preserve the option for simultaneous ground-launched ballistic-missile defense intercept tests would have to identify some observables to distinguish ASAT flight-test profiles from those of ballistic-missile defense intercept.

### **Prelaunch Inspections Required for All Space Launches**

This measure calls for a series of inspections before the launch into orbit of any spacecraft from any member country. Clearly, delaying the adoption of a measure, such as prelaunch inspections, would require

grandfathering all space systems already in orbit and, thus, degrade the effectiveness of the measure. These inspections of every spacecraft are in addition to providing to the United Nations Register its registration and technical and performance specifications. All these data together are designed to discern, once any spacecraft is in orbit, its technical capability including convertibility to perform ASAT missions such as close-in attacks (e.g. space stalking) or attacks from far away. Before the United States proposes such a drastic but highly useful measure, it needs to carefully consider the benefits and costs to the United States as well as to other countries, especially China and Russia. Overly intrusive inspections could delay a launch, add costs, and, most critically, reveal trade secrets and military capability. On the other hand, without inspections, treaty members would have far less assurance that their satellites would not be attacked or would be protected.

During the early period of implementing this measure, the inspection team will include, but not be limited to, space experts from China, the United States, Russia, the European Union, and other major spacefaring nations. Their participation is needed to ensure that other countries' space systems would not have a potential ASAT capability that a given expert's country cannot deter or defend against. As the inspection procedure becomes objective and reliable in uncovering potential ASAT capability, trust among countries might eventually permit the inspection duty to be taken over by a third-party team under the auspices of the United Nations.

The number of spacecraft with exemptions from registration and/or specification can be negotiated. However, the number can be small or even zero especially when countries are willing to trade the sacrifice of some military expedience with the tremendous benefits of space arms control.

Article II of the Convention on Registration of Objects Launched into Outer Space stated that "when a space object is launched into earth orbit or beyond, the launching State shall register the space object by means of an entry in an appropriate registry which it shall maintain."<sup>54</sup> While Article II intends to make transparent what objects are in space, prelaunch inspections further this goal.

### **Acceptable and Effective Prelaunch Inspections**

The foundational proposal by itself is a significant improvement over the status quo of no agreement. However, if prelaunch inspections are

added to the foundational proposal, comprehensive space arms control on a wide variety of space weapons would become possible or far more effective. Discussed below are suggestions on how inspections can be designed to be acceptable to the international community and effective in maintaining a peaceful space environment.

First, business practices—particularly regarding exports—provide lessons learned on how to inspect space systems without exposing essential trade secrets. Military systems, which contain many proprietary and highly sensitive hardware and software, are exported to foreign entities including potential adversaries. The recipients can take their time to repeatedly open up, inspect, test, and reverse-engineer their acquired systems to learn about trade-secrets. Yet, the United States and others are capable of protecting these secrets and comfortable in exporting them. If countries can do so on these exported sensitive systems, they should be able to do the far easier job of protecting the secrets through only prelaunch inspections, which are far more time constrained and far less intrusive.

Second, gathering even general information through prelaunch inspections could adequately specify the designed or retasked ASAT capability of a space system. Take ADR or OOS spacecraft as an example. Knowing the type, number and power of thrusters; the type and dimensions of the solar panel; the dry mass of the spacecraft; and the amount of propellant could be adequate for assessing the maneuverability and speed capability of unmanned rendezvous proximity operations for ASAT. The availability of a robotic arm also shows the spacecraft's potential ASAT capability. Again, as for ADR and OOS spacecraft, the intent of both specifying technical and performance information during registration and the data obtained through prelaunch inspections on every space launch should exclusively focus on determining the potential ASAT capability, should the space system be retasked to do so. This focus should lessen the danger of revealing other sensitive information for non-ASAT purposes.

Third, prelaunch inspections can be designed so the revealed information does not lessen a country's capability or offer much help to adversaries. For example, one may be concerned that such inspections could degrade the benefits of using a potentially militarily sensitive reconnaissance, surveillance, or intelligence satellite such as a LEO imaging satellite or US Geosynchronous Space Situation Awareness Program satellite. A country may want to sneak in for a picture or close look of

a ground or space target in its unalerted and unconcealed state. However, prelaunch inspections would not reduce the satellite's ability to surprise, because inspection data offer little help to the targeted country in knowing whether the satellite is at a suitable location for such a peek. For the targeted country to prevent a surprise look, it would have to rely on direct observation of the location of the reconnaissance satellite, and prelaunch inspection data would be of little help.

Fourth, as discussed before, 14,000 to 16,000 small satellites are expected to be launched into LEOs over the next decade. They will add a significant burden to space tracking, because they are both numerous and small. Just like the control measure to facilitate the monitoring of the ADR and OOS spacecraft discussed above, these small satellites should have their locations as well as their repositioning plans known to the public and be easily detectable 24/7. Also, since they have no peaceful reason to be placed at or travel to GEOs or even high MEOs, they should stay at LEOs and low MEOs only. Without these requirements or restrictions, they could serve as numerous and hard-to-track space stalkers as well, making the defense against stalking more difficult. These measures can be used as "design solutions that increase the trackability of small-size space objects and all other space objects that are difficult to track" as described in Guideline 30 of the UNWG Guidelines.<sup>55</sup>

Fifth, there have been reports of stealth spacecraft such as *Misty*, which are supposed to be difficult to detect.<sup>56</sup> Should such spacecraft exist and be used for ASAT, they would make satellite defense far more difficult. Countries should consider whether to ban them outright. The risks of having stealth satellites may outweigh the benefits. Again, prelaunch inspections can prevent them from being placed into space and lurking for attacks.

Sixth, in the emerging era of proximity operations, space weapons cannot be banned. As space weapons will always be present in space, it would be foolish to ban the use of space weapons for defensive purposes.

Seventh, by seeing the interior of a spacecraft, one can inspect whether anything is hiding inside that could be a potential ASAT. It should be noted that the most important purpose of prelaunch inspections is to ensure there is no long-range ASAT capability hiding in the spacecraft, because any short-range ASAT including space stalker can be adequately handled by the foundational proposal. The subsection below further

explains that banning space-based long-range ASATs can pave the way for a truly comprehensive and effective space arms control.

## **Ultimate Space Arms Control**

Incorporating the foundational proposal and all of the above control measures that are compatible could be the basis of the ultimate space arms control treaty that the United Nations has been seeking since the Outer Space Treaty entered into force in 1967. The foundational proposal should be the core of any ultimate space arms control treaty. In addition to these two actions, space weapons should be arrayed into six categories to help manage them:

1. Space-based less-than-10km-range ASAT weapons. The final range demarcation is to be determined by DOD and the international community.
2. Space-based less-than-10km-range defensive weapons
3. Space-based 10km-or-more-range ASAT weapons
4. Space-based 10km-or-more-range defensive weapons
5. Ground-launch ASAT weapons
6. Space-based weapons against terrestrial targets

Since spacecraft such as those for ADR or OOS or even garden-variety satellites can be potential weapons, they either would be controlled as if they were weapons or could not be converted into weapons. In other words, the control measures for each weapon category should cover both weapons and potential weapons alike or prelaunched inspections should ensure the inconvertibility into weapons.

All category 1 space-based less-than-10km-range ASAT weapons and ASAT-capable spacecraft such as those for ADR and OOS will be controlled by prohibiting them from tailgating another country's satellites beyond a pre-agreed innocuous number.

Once weapons and potential weapons of the first category are present, it is far better to allow weapons of the second category for defense, because using "guns" to defend against "guns" in space is far more effective than using no "gun" to defend against "guns" especially in the proximity-operation era. On the other hand, since weapons and potential weapons of the first two categories cannot be observably distinguished from one



another, we should consider it a treaty violation if these defensive weapons and potential weapons are too close to more than the threshold number of an adversary's satellites. Also, whenever possible, defensive weapons that can produce reversible or soft kill are the first choice, while defensive weapons that result in hard kill but with little enduring space debris are the second choice.<sup>57</sup> For the latter, a defensive weapon with a robotic arm can disable a space stalker with little debris.

Space weapons of the third and fourth categories are banned outright. Prelaunch inspections are needed to ascertain their range or potential range and prevent such weapons and potential weapons from being launched into orbit. The foundational proposal works well when these long-range weapons and potential weapons are absent in space, because short-range space-based weapons can be kept from reaching satellites even when the satellite population is large. In contrast, if long-range space-based weapons were not banned, they could attack satellites far away. Then, the defensive weapons would be forced to be long-range as well. Alternatively, the number of short-range defensive weapons around each critical satellite would have to be greatly increased to counter the threat of multiple space-based long-range ASAT weapons because, even if they are far away from the target satellite, they can still quickly concentrate their attacks on the same target to overwhelm the defense. Longer range and/or increased numbers of weapons are major causes of a space arms race that should be prevented for more efficient space arms control.

Space weapons of the fifth category cannot be banned because the banning cannot be monitored. However, as discussed earlier, the testing of ground-launch ASAT weapons can be banned or restricted to LEOs only.

If countries agree to ban space weapons of the sixth category, prelaunch inspections will prevent them from being launched in orbit. But, if countries wanted to allow, a space-based missile defense system, some specific give-and-take would have to be worked out. For example, the system can be restricted to being located only in LEO. The range of the defensive missile can only be long enough to intercept incoming ballistic missiles but short enough to be unable to attack MEO and GEO satellites. It may even be possible to structurally fix the sensor, the firing mechanism, and the interceptor to only look and shoot downward and thus render the system incapable of attacking any satellite far above the system's altitude. The prelaunch inspections would have to be designed

to ensure that the system cannot be used or reconfigured in space to hit any satellite that the system has been designed and committed not to hit.

Finally, it would make satellite defense easier if the numbers of rendezvous proximity operation–capable spacecraft such as those for ADR or OOS are limited. Many of them can be controlled and managed by a United Nations organization so as to prevent any country from retasking its spacecraft controlled by a neutral independent party for space stalking or other offensive purposes.

## **Conclusion**

The 50th anniversary of the first United Nations Conference on the Exploration and Peaceful Uses of Outer Space in 2018 is a time to celebrate the establishment of the Outer Space Treaty and many other accomplishments, which guide the civil and commercial activities in providing peaceful benefits of space. It is also time for reflection on how we have failed to arrive at a treaty to control space weapons and the space arms race to ensure peace in space in spite of countless effort over the last 50 years. Space is irreversibly entering into an era of unmanned, rendezvous proximity operations, in which space weapons are inevitable and space will become weaponized. The world needs to face this reality. Fortunately, while space weapons cannot all be banned, they can still be effectively controlled. A foundational space arms control treaty would be better than the status quo of no space arms control or continuing the impossible tradition of banning weapons of any kind in outer space.

A core space arms control proposal that deals with space stalkers can be negotiated and established by itself. It can also be used as the core of a more comprehensive hybrid space arms control proposal as only some space weapons are banned outright while others are prohibited from being too close to an adversary's satellites. A comprehensive set of control measures can be added to the core proposal from the start or gradually over time after the core treaty is first established. These added measures will allow countries to better deter and defend against not only traditional threats and space stalkers but also emerging space threats. Both the foundational proposal and the additional measures aim to provide effective space arms control and are reasonable for adoption by countries. All suggested measures are verifiable, recognize the right of self-defense as the last resort after treaty violation, and most importantly, can lead to peace in space.

In the worst-case scenario where no space arms control comes out of this hybrid approach, the United States would still have acted in good faith for pursuing an international space arms control treaty. Consequently, the world would have more understanding and support toward the United States as it had no choice but to switch to unilateral space arms control measures to ensure space security and stability.

Space arms control permits the continued benefits from peaceful space activities yet prevents the horror of war in space. While the emerging era of proximity operations will be upon us in the early 2020s, space arms control is still within reach, provided countries are open to ideas new and old and are willing to promptly deliberate, negotiate, and compromise for the benefit of humankind. **SSQ**

## Notes

1. United Nations (UN) Office for Outer Space Affairs (UNOOSA), “Fifty Years since the First United Nations Conference on the Exploration and Peaceful Uses of Outer Space (1968–2018): UNISPACE+50,” accessed 2 September 2017, <http://www.unoosa.org/oosa/en/ourwork/unispaceplus50/>.

2. The treaties commonly referred to as the “five United Nations treaties on outer space” are the Outer Space Treaty, the Rescue Agreement, the Liability Convention, the Registration Convention, and the Moon Agreement. While the Outer Space Treaty includes a ban of weapons of mass destruction in outer space, the rest of this treaty and the other four treaties have little to do with controlling space weapons. UNOOSA, “Space Law Treaties and Principles,” accessed 9 February 2018, <http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html>.

3. In this article, “spacecraft” and “satellite” are the same and used interchangeably.

4. Brian G. Chow, “Stalkers in Space: Defeating the Threat,” *Strategic Studies Quarterly* 11, no. 2 (Summer 2017), 82–116, [http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11\\_Issue-2/Chow.pdf](http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-2/Chow.pdf).

5. UNOOSA, “Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space,” 2010, iii–iv, [http://www.unoosa.org/pdf/publications/st\\_space\\_49E.pdf](http://www.unoosa.org/pdf/publications/st_space_49E.pdf).

6. Donald J. Kessler and Burton G. Cour-Palais, “Collision Frequency of Artificial Satellites: The Creation of a Debris Belt,” *Journal of Geophysical Research* 83, no. A6 (1 June 1978): 2637–2646, <http://webpages.charter.net/dkessler/files/Collision%20Frequency.pdf>.

7. J.-C. Liou, “A Parametric Study of Using Active Debris Removal for LEO Environment Remediation,” NASA Johnson Space Center, 2010, 4, <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100033207.pdf>.

8. Nicholas L. Johnson, “Preserving the Near-Earth Space Environment with Green Engineering and Operations,” NASA Green Engineering Masters Forum, 30 September–1 October 2009, 31, <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20090032041.pdf>.

9. “Active Debris Removal,” European Space Agency, accessed 3 September 2017, [http://www.esa.int/Our\\_Activities/Operations/Space\\_Debris/Active\\_debris\\_removal](http://www.esa.int/Our_Activities/Operations/Space_Debris/Active_debris_removal).

10. UNOOSA, "Active Debris Removal—An Essential Mechanism for Ensuring the Safety and Sustainability of Outer Space," *A Report of the International Interdisciplinary Congress on Space Debris Remediation and On-Orbit Satellite Servicing*, 27 January 2012, [http://www.unoosa.org/pdf/limited/c1/AC105\\_C1\\_2012\\_CRP16E.pdf](http://www.unoosa.org/pdf/limited/c1/AC105_C1_2012_CRP16E.pdf).

11. The author tallied the planned small satellite launches from Boeing, WorldVu Satellites Ltd., SpaceX, Tilsit, and Kepler Communications by 2027. "Who Has Satellites? Then and Now," Union of Concerned Scientists, accessed 26 July 2017, <http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.Wat9DYWcFZU>.

12. H. G. Lewis, Jonas Radtke, Alessandro Rossi, James Beck, Michael Oswald, Pamela Anderson, Benjamin Bastida Virgili, and Holger Krag, "Sensitivity of the Space Debris Environment to Large Constellations and Small Satellites," Proceedings: 7th European Conference on Space Debris, Darmstadt, Germany, 18–21 April 2017, <https://conference.sdo.esoc.esa.int/proceedings/list>.

13. "China's New Orbital Debris Clean-Up Satellite Raises Space Militarization Concerns," Spaceflight 101, 29 June 2016, <http://spaceflight101.com/long-march-7-maiden-launch/aolong-1-asat-concerns/>.

14. "Re-Entry: Aolong-1 Space Debris Removal Demonstrator," Spaceflight 101, 28 August 2016, <http://spaceflight101.com/re-entry-aolong-1-space-debris-removal-demonstrator/>.

15. "China's New Orbital Debris Clean-Up."

16. Jesse Emspak, "How Can Humans Clean Up Our Space Junk?" 30 December 2016, The Verge, <https://www.theverge.com/2016/12/30/14116918/space-junk-debris-cleanup-missions-esa-astro-scale-removedebris>; and Tereza Pultarova, "Launch of Space-Debris-Removal Experiment Delayed Amid Safety Reviews," *SpaceNews*, 26 May 2017, <http://spacenews.com/launch-of-space-debris-removal-experiment-delayed-due-to-safety-reviews/>.

17. "DARPA Select SSL as Commercial Partner for Revolutionary Goal of Servicing Satellites in GEO," DARPA, 9 February 2017, <https://www.darpa.mil/news-events/2017-02-09>.

18. UN Treaties and Principles on Outer Space, ST/SPACCE/61, UNOOSA, 2013, 4, [http://www.unoosa.org/res/oosadoc/data/documents/2013/stspace/stspace61\\_0\\_html/st\\_space\\_61E.pdf](http://www.unoosa.org/res/oosadoc/data/documents/2013/stspace/stspace61_0_html/st_space_61E.pdf).

19. Permanent Representative of the Russian Federation and the Permanent Representative of China to the Conference on Disarmament (hereafter Permanent Representatives), "Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects," 12 June 2014, CD/1985, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/050/66/PDF/G1405066.pdf?OpenElement>.

20. Delegation of the United States of America to the Conference on Disarmament, The United States of America (hereafter Delegation of the US), "Analysis of the 2014 Russian-Chinese Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects; Conference on Disarmament," CD/1998, 3 September 2014, 2, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/007/57/PDF/G1500757.pdf?OpenElement>.

21. Delegation of the US, 2. On the other hand, the United States signed the Biological Weapons Convention, which does not have a verification protocol, on 10 April 1972, the opening day for signature. But, it and other countries have tried hard to add an agreeable protocol in ensuing years, although without success. Also, it does not mean that the United States does not require verification from the start for all agreements, especially when such a protocol is feasible.

22. Permanent Representatives, "Follow-Up Comments by the Russian Federation and China on the Analysis Submitted by the United States of America of the Updated Russian-

China Draft PPWT,” CD/2042, 14 September 2015, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/208/38/PDF/G1520838.pdf?OpenElement>.

23. Permanent Representatives, “Follow-Up Comments,” 5.
24. Delegation of the US, “Analysis of the 2014 Russian-Chinese Draft Treaty,” 2.
25. Permanent Representatives, “Follow-Up Comments.”
26. Delegation of the US, “Analysis of the 2014 Russian-Chinese Draft Treaty,” 2.
27. Permanent Representatives, “Follow-Up Comments.”
28. Permanent Representatives, “Follow-Up Comments.”
29. Permanent Representatives, “Follow-Up Comments,” 3.
30. UN General Assembly, 70th session, Agenda Item 95(b), No First Placement of Weapons in Space, A/RES/70/27, 7 December 2015, <https://www.un.org/en/ga/70/resolutions.shtml>; and UN General Assembly Plenary, 70th session, 67th meeting, GA/11735, 7 December 2015, 4, <https://www.un.org/press/en/2015/ga11735.doc.htm>.
31. Matthew Bodner, “UN Adopts Russian Initiative Restricting Space Weapons,” *DefenseNews*, 9 December 2015, <https://www.defensenews.com/air/2015/12/09/un-adopts-russian-initiative-restricting-space-weapons/>.
32. “Disarmament Committee Approves Drafts on No First Placement of Arms in Outer Space Ban on New Types of Mass Destruction Weapons,” UN General Assembly, 30 October 2014, <https://www.un.org/press/en/2014/gadis3514.doc.htm>.
33. Chow, “Stalkers in Space.”
34. Permanent Representatives, “Draft Treaty.”
35. Chow, “Stalkers in Space,” 116n48.
36. Permanent Representatives, “Follow-Up Comments.”
37. Permanent Representatives, “Follow-Up Comments,” 5.
38. See the quotes of “possible with existing technologies and/or cooperative measures” and “to effectively verify an agreement banning space-based weapons” in Delegation of the US, “Analysis of the 2014 Russian-Chinese Draft Treaty,” 2.
39. Secretary of Defense and Director of National Intelligence, *National Security Space Strategy*, Unclassified Summary, January 2011, 10, 13, [http://archive.defense.gov/home/features/2011/0111\\_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary\\_Jan2011.pdf](http://archive.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf).
40. Article 51 of the Charter of the UN, 3, accessed 20 August 2016, <http://www.un.org/en/sections/un-charter/chapter-vii/index.html>.
41. Anthony Clark Arend, “International Law and the Preemptive Use of Military Force,” *Washington Quarterly* 26, no. 2 (Spring 2003): 92, [http://www.cfr.org/content/publications/attachments/highlight/03spring\\_arend.pdf](http://www.cfr.org/content/publications/attachments/highlight/03spring_arend.pdf).
42. Roberto Ago, *Addendum: Eighth Report on State Responsibility by Mr. Roberto Ago, Special Rapporteur—the Internationally Wrongful Act of the State, Source of International Responsibility (Part 1)*, extract from the *Yearbook of the International Law Commission*, 1980, vol. II(1), Document: A/CN.4/318/Add.5-7, United Nations, 69, [http://legal.un.org/ilc/documentation/english/a\\_cn4\\_318\\_add5\\_7.pdf](http://legal.un.org/ilc/documentation/english/a_cn4_318_add5_7.pdf).
43. The White House, *The National Security Strategy of the United States of America*, September 2002, 15, <http://www.globalsecurity.org/military/library/policy/national/nss-020920.pdf>.
44. Chow, “Stalkers in Space.”
45. Permanent Representatives, “Follow-Up Comments,” 3.
46. Permanent Representatives, “Draft Treaty.”
47. Permanent Representatives, “Follow-Up Comments,” 2.
48. UNOOSA, United Nations Register of Objects Launched into Outer Space, 14 August 2017, <http://www.unoosa.org/oosa/en/spaceobjectregister/index.html>.

49. UN Committee on the Peaceful Uses of Outer Space, "Guidelines for the Long-Term Sustainability of Outer Space Activities," A/AC.105/L.308, 15 February 2017, 17–18, [http://www.unoosa.org/oosa/oesadoc/data/documents/2017/aac.105l/aac.105l.308\\_0.html](http://www.unoosa.org/oosa/oesadoc/data/documents/2017/aac.105l/aac.105l.308_0.html).
50. Delegation of the US, "Analysis of the 2014 Russian-Chinese Draft Treaty," 2.
51. Deane N. Morris, *Charts for Determining the Characteristics of Ballistic Trajectories in a Vacuum*, RM-3752-PR (Santa Monica, CA: RAND, April 1964), 37, figure 27, [https://www.rand.org/content/dam/rand/pubs/research\\_memoranda/2008/RM3752.pdf](https://www.rand.org/content/dam/rand/pubs/research_memoranda/2008/RM3752.pdf).
52. Morris, *Charts*, 39.
53. While lofted flight will result in maximum apogee higher than 1,300 km, the control measure can choose to prohibit ballistic missile intercept test far higher than 2,000 km but still protect important MEO satellites such as satellite navigation systems from the United States, Russia, European Union, and China, which are located at altitudes of 19,100 km and above.
54. Convention on Registration of Objects Launched into Outer Space, UNOOSA, accessed 16 September 2017, <http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/registration-convention.html>.
55. UN Committee on the Peaceful Uses of Outer Space, "Guidelines," 32.
56. Jesus Diaz, "Misty Stealth Satellite Hides Perfectly While Watching You," Gizmodo, 2 March 2009, <https://gizmodo.com/5162837/misty-stealth-satellite-hides-perfectly-while-watching-you>.
57. Chow, "Stalkers in Space," 106.

# Book Reviews

*The Logic of American Nuclear Strategy: Why Strategic Superiority Matters* by Matthew Kroenig. Oxford University Press, 2018, 280 pp.

In 1984, Robert Jervis published a wide-ranging critique of American nuclear strategy entitled *The Illogic of American Nuclear Strategy*, in which he argued that much of the thinking by nuclear strategists and decision makers within the US federal government had, over the previous decades, been based on a flawed understanding of the nature of both nuclear deterrence and strategic stability. He suggested that the United States need only possess the ability to retaliate against the Soviets to deter them from launching a surprise attack on the US or its allies. Any capability in excess of this was unnecessary and, even more problematically, destabilizing.

For both Thomas Schelling and Jervis, threats issued by a state with a numerical inferiority could also be viewed as equivalently credible as, if not more so than, those issued by a state with a larger and thus more destructive capability if the stakes involved were greater for the numerically inferior state. Matthew Kroenig's recently released work *The Logic of American Nuclear Strategy* is in many ways a direct rebuttal to Jervis, Schelling, and the many scholarly works published since that echo these sentiments. In it, he lays out a detailed argument as to why such an approach is at best incomplete, if not wholly misguided.

Kroenig begins by reviewing the classic logic of the brinkmanship game, which suggests that once each state in a two-player game possesses a second-strike capability, any additional capability should not affect the outcome. If both sides escalate to nuclear war, each player in the game is affected equally (destruction). The "winner" is thus determined not by whether one possesses more or less capability but by which one is more resolute and/or risk acceptant. Kroenig smartly points out, as he has in previous scholarship, that it is obviously not the case that two states with drastically different-sized nuclear arsenals would suffer in the same way in such a situation. Were such an exchange to occur between the United States and China, for example, the comparatively small size of the Chinese nuclear force combined with the US's ability to destroy much of the Chinese nuclear arsenal before its use would virtually guarantee a US victory.

To reflect this dynamic, Kroenig offers his "superiority-brinkmanship synthesis theory," which suggests that states with a superior destructive capability have a distinct advantage in crisis bargaining situations because the potential cost of escalating to nuclear war is less for them than it is for those with a numerically inferior force.

He tests the strength of this theory using both qualitative and quantitative analyses and finds that nuclear superiority bolsters both deterrence and coercion. Furthermore, he finds that the scale of these effects increases as the disparity in capability between the two parties in a nuclear crisis increases (a rather troubling conclusion for those interested in nuclear disarmament).

The second part of the book not only attempts to dispel the conventional wisdom that nuclear superiority is inherently destabilizing but also challenges the prevailing logic of the stabilizing influence of nuclear parity. Nuclear parity, he points out, was always considered tenuous because it relied on "mutual vulnerability" between adversaries. If either side in such a relationship ever felt that its adversary possessed or was developing a first-strike capability, the other side might be incentivized to preemptively strike or else risk losing the ability to respond. As a result, there were strong pressures on both sides to guarantee the ability to conduct a retaliatory strike. However, Kroenig argues that situations where preponderances of capability exist are not subject to such tenuous circumstances because it is much clearer at the outset of a nuclear crisis who the likely victor would be, regardless of who launches first or second. Thus this kind of

situation is inherently more stable than one in which parity exists. Kroenig further argues that many of the most often cited instability-inducing byproducts of nuclear superiority, including arms races and nuclear proliferation, are wholly unsupported by the empirical record.

Certain criticisms can be leveled at this book—including the brevity of the case studies and reliance on a dataset that Kroenig himself views as inherently flawed. Furthermore, chapter 2 appears least significant since its sole purpose is to empirically support the assertion that if a state has more or bigger bombs than an adversary it can inflict more damage than said adversary (hypothesis 1). Perhaps the most interesting aspect of this book is the questions it raises for both scholars and the strategic-planning community, the most obvious of which is why academics and those involved in US nuclear planning have been so at odds for so long. If Kroenig is correct that preponderances of nuclear capability create more stable relationships than those where capabilities are roughly equivalent, why is it that the opposite conventional wisdom among academics remains prevalent? One might wonder, for instance, whether it is more ideology than strategy.

While the academic community has been almost monotheistic in its reverence for the concepts associated with parity, including the oft-cited doctrine of mutually assured destruction (MAD), the US nuclear planning community has, by and large, endeavored to create the situation Kroenig advocates. MAD, as many have pointed out, was never a doctrine to adhere to but rather an unfortunate reality to be dealt with. If given the choice between parity and US numerical superiority over all potential adversaries, it is hard to imagine that even the most reverential of MAD supporters would choose the former over the latter.

Overall this book is a noteworthy and necessary contribution to the renewed debate on the utility and appropriate constitution of the US nuclear arsenal. Kroenig's preference for US strategic superiority seems to be echoed by the current presidential administration, a sharp departure from the past eight years. It will thus be interesting to see whether or to what extent his arguments filter into the narrative crafted by the administration to justify current and planned efforts toward force modernization. This volume may come to define the US approach to nuclear strategy for the foreseeable future—in which case, one can only hope that his assertions are correct.

**Todd C. Robinson**

*Air Command and Staff College*

***Strategic Cyber Deterrence: The Active Cyber Defense Option*** by Scott Jasper.  
Rowman & Littlefield, 2017, 255 pp.

The book *Strategic Cyber Deterrence: The Active Cyber Option* is particularly relevant today in the face of the continuing challenges for America from the Russians, the Chinese, the Iranians, and the North Koreans. While many feel cyber deterrence is unattainable, Professor Scott Jasper of the Naval Postgraduate School in Monterey, CA, shows quite clearly that we can in fact get there, if we open our intellectual aperture. This is a subject of ever increasing relevance to the physical and digital security of the nation, as well as America's wider national interests. It is tough ground to cover, filled with a great deal of technical information and international relations jargon, but it is a needful task and worth the intellectual effort.

Jasper has structured the book logically, into three parts. He begins with a section of solid introductory material covering the main theoretical areas that must be understood to address



deterrence. “Strategic Landscape” (chapter 1) covers all the preliminary concepts. It is heavy, but understandable. The next two chapters (“Cyber Attacks” and “Theoretical Foundations”) expand on the concepts introduced in the first and will satisfy those who may think chapter 1 covered too much ground, too fast.

In Part II, “Traditional Deterrence Strategies,” chapters 4–6 form an excellent primer on deterrence. Jasper categorizes deterrence three ways: retaliation, denial, and entanglement. Defining each, he means: deterrence because your opponent is worried about the backlash, deterrence because the opponent’s efforts will have no effect, and deterrence because the opposing system and your own are so intertwined that hostile attack becomes self-defeating. For readers with a scholastic background in deterrence, these three chapters are classic treatments and can be covered quickly. For other readers, this section offers solid background information and is well worth reading to grasp coverage of critical concepts.

Jasper finishes the book by investigating an active cyber defense strategy in two chapters (7 and 8): what it is, what it is not, why it can work, and why it may be our only real, effective choice while considering alternative strategy selection.

The book has many strengths. First, it is loaded with understandable definitions, especially helpful with terms that typically are misused or at least misunderstood. That alone would make it worth reading. Second, it challenges the intellectual status quo without dismissing traditional thought. He gives the traditional deterrence theories a fair look. This gives great balance and credibility to his later arguments. Finally, his alternative, an active cyber defense, is presented rationally and without zealotry. Jasper remains scholarly and objective, showing the potential advantages and liabilities of the solution.

There are weaknesses to *Strategic Cyber Deterrence*. Primary of these is that a nonexpert could get lost in the strategic and technical jargon. Jasper tries to avoid this, but cyber and deterrence are impossible to discuss without their associated vocabularies, and mixing them creates difficulty. Additionally, he seems to spend too much time setting the stage in the first six chapters. While Jasper covers those areas much better than most academics, another reader may have more patience.

Reading this book is well worth the effort. While not a summer beach page-turner, it is a well-written, accessible volume, providing a superb reference for those involved or interested in this key national security debate. Active cyber defense is the way forward to achieve deterrence and to guide response. What we have now is simply not enough. Jasper gets away from the view that active measures will turn the internet into the Wild West, filled with vigilantes. He shows how an active defense policy can work and that it really is the most viable option. If one only read the excellent chapter 7 on the active cyber defense option (and the appendix on the national strategy agenda), it would justify the cost of the book and the time spent in reading. This chapter is insightful and enormously persuasive.

Every expert in the cyber field should read this book and consider Jasper’s cogent arguments. Every legislator who wants to propose legislation to “solve” the cyber problem needs this book to become adequately literate in this crucial area. Every pundit who wants to break the next big cyber story should read it to avoid distortions and false reporting. Any civilian who wants a glimpse of the present and the future of our security world should also invest the time.

Scott Jasper has written a compelling work and should be congratulated for a fine book.

**Stephen Bucci**  
*The Heritage Foundation*

***US Foreign Policy and Defense Strategy: The Evolution of an Incidental Superpower*** by Derek S. Reveron, Nikolas K. Gvosdev, and Mackubin Thomas Owens. Georgetown University Press, 2015, 262 pp.

With *US Foreign Policy and Defense Strategy*, the authors synthesize concepts from two related academic fields—national security and strategic studies—with a bit of international relations thrown in for good measure. This book is not a historical review of US policy and strategy; rather, history informs how the United States assumed primacy among nations in the twentieth century and the ways by which foreign policy and national defense contributed to the rise of the “incidental superpower.”

The authors are current or former professors of national security affairs at the US Naval War College. All three have extensive academic experience with several published books in the national security and strategy fields. By merging their expertise, they have exploited a unique niche, combining foreign policy considerations with defense strategy. Despite having multiple authors, the book is not merely a compilation of their respective writings on related subjects but rather a well-integrated and superbly researched study.

The structure of the book illuminates a dialectical discussion on the United States as superpower and the conditions that led to this status. The introduction and first chapter summarize the main points of the book, providing an overview and explanation for the rise of American power. Subsequent chapters are analytical essays, highlighting US defense organization, civil-military relations, foreign policy, warfare and peace, and the peculiarities of defense financing. The final chapter concludes and projects US foreign policy and defense strategy into the future. The authors took great pains to integrate related ideas so previously introduced material is referenced in subsequent chapters. It is well written, concise, and lacks obfuscating jargon. A minor distraction is with the order of chapter 3, “The American Way of Civil-Military Relations.” Structurally, the outline of the book has civil-military relations following the discussion about the US defense organization, which seems to suggest a cause-and-effect relationship—that civil-military relations is a result of how the United States organized for defense. Rather, the nature of US civil-military relations, rooted in the constitutional order that sets relations between the military and political branches, precedes any understanding about the organizational structure that follows from this precept.

The crux of their thesis is that the United States’ rise to power was not accidental but incidental. Despite a previous history of relative isolation from the affairs and conflicts of powers outside the western hemisphere, the perceived challenges of the post–World War II security environment created conditions for US political leadership to acquiesce and assume the mantle of an “incidental” superpower.

The historical focus for the book is primarily from World War II to the present, which necessarily constrains analysis to ideas and events over approximately a 70-year period. Where necessary, additional historical context buttresses their arguments, but overall, this is a study of US foreign policy and resulting defense strategy as a result of a postwar environment characterized by ideological struggles and wars of liberation.

Despite a progressive vision for international harmony through the League of Nations championed by Woodrow Wilson following World War I, the United States returned to its previous pattern of demobilization and withdrawal from entangling alliances outside of the western hemisphere. Referencing political scientist Bear F. Braumoeller, the authors argue this pattern was not a result of nationalistic isolationism but of a fight between political factions, those advocating using US military power to advance international ideals or those who wanted greater autonomy to advance primarily American interests. Nonetheless, America post–World

War I saw a return to previous patterns of using nonmilitary instruments of power in the pursuit of US interests.

Preferring to impose harsh measures on Germany, triumphant British and French leaders unwittingly set conditions for a second world war, leading to the eventual rise of American global leadership. As “the last nation standing,” the United States held almost half the share of global GDP at the end of the war. Reluctantly, political leaders realized that there was no return to the status quo ante. Thus, the organization for defense, the creation of international security and financial structures, the expeditionary nature of US military power, tensions with civil-military relationships, the ways by which the machinery of war is financed, and preferences for converting foes to friends reflects a uniquely American approach to foreign policy and defense that was incidental to any preferred strategy.

One of the key challenges for books of this type is determining not only what to include but also limiting discussion to information of direct relevance to the main points of the book without stripping the coherence of the overall narrative. For the most part, the book succeeds in this endeavor with the exception of chapter 5, “The American Way of War.” Summarizing the multifarious theories of the American way of warfare would be difficult for a book-length treatment, but to do so in only 25 pages meant that only a gloss was provided on the many variables of a complex subject.

The strength of the arguments presented in the book will not fade with time but will continue to be a scholarly source for understanding how the United States historically managed the challenges of being a superpower without necessarily having a deliberate strategy for securing long-term benefits. It is only in retrospect that we can see the efficacy of any so-called grand strategy. The authors present a convincing account of the United States’ rise to dominance as a result of environmental pressures and internal adaptations that facilitated its superpower status. I highly recommend this book, not only for instructors and students of foreign policy and strategic studies but also for any reader interested in how the United States became an “incidental” superpower.

**LTC Kurt P. VanderSteen, USA, Retired**  
*US Army Command and General Staff College*

***Getting Nuclear Weapons Right: Managing Danger and Avoiding Disaster*** by Stephen J. Cimbala. Lynne Reinner Publishers, 2017, 269 pp.

Recent Russian pronouncements about nuclear weapons, Chinese nuclear force modernization, and the release of the Trump administration’s *Nuclear Posture Review* have reignited a debate on the role of nuclear weapons in national security and the state of nuclear deterrence today. Stephen Cimbala wades into the discourse of the day with his latest offering on nuclear strategy and policy. *Getting Nuclear Weapons Right* is a timely work that analyzes the concerns of today as well as examining the validity of various positions within the nuclear deterrence landscape. The author is a distinguished professor of political science at Penn State–Brandywine and has an impressive list of previous publications, to include multiple books on nuclear and national security issues as well as numerous articles and op-eds related to this topic. This work draws upon previous work on nuclear deterrence but updates those theoretical approaches by looking at how technology, cyber, and nuclear proliferation might upset the stability nuclear deterrence has maintained for decades. While some of this is plowed ground, the author fertilizes it with new analyses and original thoughts on the future of nuclear policy.

Cimbala’s book addresses two issues that he sees as threats in the post–Cold War nuclear age, what some have termed the second nuclear age, that could threaten the “stabilizing condition

of nuclear deterrence that has prevailed until now” (p. 1). The first threat the author sees as possibly disturbing this stability is the risk associated with additional nonnuclear states acquiring nuclear arsenals. His second threat is that “developments in technology and in politics” also can act to upset the strategic stability nuclear deterrence has provided since the early days of the Cold War. To make his argument, Cimbala organizes his book in a topical format to address more specific issues under these two overarching threats that, as the title suggests, can lead to danger and/or disaster.

Cimbala begins his analysis of how nations can avoid nuclear disaster by outlining the various types of nuclear regimes that can, and have, emerged among nuclear powers. According to the author, a regime “is a collection of rules or behavioral expectations that provide a framework for the interactions among states or actors” (p. 9). He identifies five nuclear regimes that can come to fruition: deterrence/assured retaliation, nuclear primacy, defense dominance, nuclear abolition, and nuclear plentitude. He seems to suggest that the regime with the most validity is the assured retaliation model not simply because of the stability it brings but because this is the one that was “road-tested” in the Cold War (p. 37). Interestingly enough, Matthew Kroenig’s latest work, *The Logic of American Nuclear Strategy*, makes the argument that nuclear primacy is the best strategic choice for the United States. Cimbala’s logic and argument stem from his position that a stable relationship between the two nuclear superpowers brings greater stability to the world order.

Since President Obama’s 2009 Prague speech, nuclear abolition has gained some traction as interest groups have lobbied for nations to follow their Nuclear Nonproliferation Treaty obligations and craft a path to a nuclear-free world. Cimbala explores all sides of the nuclear abolition issue and concludes that it is unlikely to come to fruition. The most convincing of his arguments is the fact that “nuclear weapons are symbols of national sovereignty and international power” (p. 63). Following that logic, and the theme of the book, the author posits that those nations that have them will want to keep them and those that do not will want to acquire them. If nuclear weapons are here to stay, then Cimbala offers an alternative nuclear strategy: minimum deterrence. Minimum deterrence would rely on smaller stockpiles but retain enough weapons for a secured second strike, thus bringing crisis stability. The trouble with any discussion of minimum deterrence is that most gravitate to the Thomas Schelling model of limited nuclear weapons and a secured second-strike capability. Lost in the minimum deterrence debate is how Bernard Brodie defined minimum deterrence in his book *Strategy in the Missile Age*, which was “enough to win the war.”

As Cimbala examines more contemporary issues from nuclear proliferation to missile defense to the expanding cyber capability among nations, a common theme runs throughout his analysis. The author seems to indicate that politics at the grand strategic level can maintain and manage the potential for danger and or disaster. While NATO and Europe dominated in the Cold War, Cimbala sees the Pacific as the place where increased emphasis is needed. Although China will not reach parity with the United States or Russia, the author concludes, “Chinese nuclear modernization is not necessarily incompatible with their engagement with Russia and the United States on strategic nuclear arms control” (p. 165). To bring stability to this complex technological and political environment, he suggests the United States seek a realist approach to relations with Russia, “cooperate on security matters where cooperation is possible and mutually beneficial, and where disagreements exist, state clearly US vital interests and US willingness to support those interests” (p. 222). Cimbala would seem to indicate that a return to the Cold War order of the US and Russia maintaining an assured destruction force structure would bring stability to the modern era and get nuclear weapons right.

*Getting Nuclear Weapons Right* provides vital insight into the debates of the day and must find wide readership among those interested in nuclear policy, strategy, and force structure options. Cimbala's analysis of varying alternative regimes, nuclear arsenals, and nuclear exchange scenarios serves as starting point for discussions that must take place in light of the president's *Nuclear Posture Review* and the argument by some for a return to nuclear primacy. While some hailed the end of the Cold War, recent events suggest it has returned, and Cimbala would seem to indicate that maintaining a balance between the United States and Russia is the solution to avoiding danger and disaster in today's world. Readers will have to judge for themselves the validity of the argument, but the research, discussion, and analysis presented in this work are vital to framing discussions about the future of nuclear weapons and policy.

Mel Deaile

*Air Command and Staff College*

***The President's Book of Secrets: The Untold Story of Intelligence Briefings to America's Presidents from Kennedy to Obama*** by David Priess. Public Affairs, 2016, 386 pp.

David Priess pulls back the veil on the *President's Book of Secrets* to introduce a world where a single private conversation might make the difference between safety and national catastrophe. Despite the enormity of the stakes, Priess ably draws upon his experience as a career CIA officer to craft a human tale across 10 administrations. He invites us with intimate details about the series of briefers passing the crown jewels of national intelligence to the commander in chief and a tight circle of advisers on a daily basis. We learn how one young analyst fought back morning sickness as she presented the president's daily brief (PDB) to Al Gore in the back seat of the vice presidential limousine, Gore all the while scarfing down breakfast on his way to the White House. Priess takes us inside the presidential residence in April 1981 as Ronald Reagan recovers from an assassin's bullet. The Gipper is too exhausted to absorb the briefing but sharp enough to notice the bulge of get-well cards in his national security adviser's folder, smuggled into the first national security session back from the hospital in partial fulfillment of a fatherly promise to the adviser's kindergarten-age daughter. Reagan inscribes the kindergartner's card with a thank you note of his own, and a photo of this remarkable correspondence appears on page 142.

The human element painstakingly incorporated into *President's Book of Secrets* serves a second purpose of current relevance to the health of the intelligence profession and connected to a broader restoration of faith in American democracy. In the aftermath of the Vietnam War, the eminent twentieth-century political scientist Sam Huntington called our spasms of doubt "creedal passion periods." Others have remarked on volatility in American political development marked by critical elections when old structures are swept away and novel coalitions form to reconstitute major parties. As society becomes more complex, more technological, more bureaucratic, and more dependent on specialized services, critical transitions for American democracy bring virulent ideological divisions between absolutists, who wish to tear down institutions to rescue traditional American values, and pragmatists, who believe that progress toward American ideals is only possible if a popular movement can drain the swamp and, on a solid foundation, replace it with enlightened administration.

From sociological works by Talcott Parsons, C. Wright Mills, Terence Johnson, and Andrew Abbott, Naval War College professor Tom Nichols in *The Death of Expertise* (Oxford, 2017) recently related how these factions may grow to detest one another, agreeing on little else but that the obsolete establishment must go. Radical revision is politically easier, and the risks more

palatable, if the current regime is rotten to the core, filled with craven bureaucrats who care nothing for their professions or the country they serve. Indeed, corporate expertise and professional jurisdiction under the revolutionary view are perverted to afflict cancer on the body politic. The Deep State at some point breaks free of social responsibility, the general will, and the president's power to rein it all in.

Priess does not set out explicitly to slay this dragon, but in the book, he marshals his formidable powers as writer, intelligence analyst, and social scientist to convince a broad audience that this untold story of unsung heroes is true. If, in the age of narrowcast news, celebrity talking heads, and crowdsourced reporting, authentic patriots within the CIA and throughout the executive branch cannot be properly understood or appreciated, then revolutionaries at the gate have reason to pause before dismantling the state.

Priess' chronology of the PDB covers a lot of ground with a cast of hundreds—many of whom he interviewed for behind-the-scenes electricity in this narrative. Among the multitude of protagonists, though, one self-effacing, humble personality, whose saga of public service actually eclipses the book's epic proportions, emerges as the main hero. George H. W. Bush anchors one of 10 case chapters as president during world transformation after the end of the Cold War. He figures in six more, owing to his multiple roles as ambassador to China, director of the CIA, vice president, former president, and father to a president. In addition, Pres. George H. W. Bush penned a gracious foreword for *Book of Secrets*, declaring that his "love of the job [of director of Central Intelligence] was all about the remarkable men and women who make up our intelligence community. Their dedication, their courage . . . inspired me every single day."

In *Book of Secrets*, George H. W. Bush is the one and only "spymaster president." He thus understands the importance to national security of reserving precious face time with the PDB briefer—for the opportunity to read and listen, to interact with a professional intelligence officer when formulating presidential requests for further research, and to shore up morale of devoted analysts who labor long each day to serve the "first customer" the most useful briefing possible.

Even so, Priess does not pull punches. Over the half-century of the PDB's existence, Pres. George H. W. Bush's example has not been followed all that often. Indeed, several presidents and senior advisers appear in the book disparaging the PDB as not much better than press clippings or what they get from other agencies, such as State or Defense, responsible for implementing specific policies. For some interview subjects in the book, the most important reason to pay attention to the PDB is not the quality of professional analysis but the fact that the president sees it nearly every day. Even the spymaster president would likely agree that despite constitutional checks and balances and the rise of professionalism in modern executive branch bureaucracy, the coin of the White House realm, as it was in the European courts of old, remains propinquity—access to the chief and the opportunity to influence thinking before important decisions are taken.

State bureaucracies around the world come up against a similar dilemma. In American intelligence circles, it is known as the Kent-Kendall debate: hew close to the pure, objective professional ideal where expert service is substantially the same regardless of ideology, party, or policy agenda of democratically elected authority and risk becoming irrelevant or, worse, irritating to said authority; or customize professional advice to make it useful and politically responsive from the customer's perspective and color intelligence away from actual threats and opportunities shaping the country's fate. Either extreme, of course, is untenable. The trick is to work continually under the Constitution toward the best balance. Priess's recommendation for increased access and therefore greater influence from senior career CIA analysts who craft the PDB goes to show that, as the United States slides from unquestioned hegemony to competitive great

power politics on multiple fronts, here is one experienced official who would like to see more Kent than Kendall, a disciplined, objective intelligence product above endemic political jockeying surrounding the White House.

*Book of Secrets* came out just before the 2016 elections. Its concluding recommendations must now be weighed in light of a victorious populist who campaigns against both party establishments, ardently lambastes a multiyear investigation of close aides by special prosecutor—picking up where President Obama’s Federal Bureau of Investigation left off—and who, in so many words, accuses top intelligence professionals in the previous administration of proffering all Kendall and not enough Kent.

Pres. George H. W. Bush and Priess contend the country would be safer if every commander in chief reserved space at the start of each workday for a thorough, unguarded, private conversation with the PDB briefer. This practice puts a face on the ranks of highly skilled, dedicated professionals within the executive branch who carry the burden of a sacred trust to defend the republic against enemies foreign and domestic. Trust in the relationship binding the president and his long-time subject matter experts in intelligence, not to mention the uniformed and civil services, pays dividends, when American democracy must navigate the next international crisis (as Priess shows happened immediately after the 9/11 attacks).

Action items from *Book of Secrets*, however, do not apply exclusively to the president. If the PDB process is to flourish and achieve its urgent objective, that influential yet amorphous layer of appointed officials between the president and career professionals will have to consider their own behavior. For members of the president’s National Security Council, there is no escaping Machiavelli or Kent-Kendall—any shift toward the rigid objectivity of Kent will come with a political price. Still, that may be precisely what is required before any administration can follow the sage advice in the *President’s Book of Secrets*.

Damon Coletta  
USAFA

***Future War: Preparing for the New Global Battlefield*** by Robert H. Latiff. Alfred A Knopf, 2017, 208 pp.

*Future War* is a timely, authoritative, and wide-ranging look at the interplay of ethics and technology in warfare. While the title promises preparing for the “new global battlefield,” this book does not delve into the question of how, where, or with what weapons future wars will be fought. Instead it limits itself to surveying the ethical and moral dilemmas of employing advanced, autonomous, or futuristic weapons such as artificially intelligent machines, gene editing, or long-range hypersonic vehicles. While Dr. Robert Latiff explicitly states his purpose is to explore how new technology has changed warfare and to “highlight both the dramatic developments in technology and war and the speed with which they have occurred and to describe how these will challenge soldiers, decision makers, and the public,” he is less than immediately clear that the challenges he is describing are ethical and moral in nature. Ultimately *Future War* is a cautionary tale warning that unless we begin to understand the ramifications of technology on war, as a nation and a military the United States will be ill-equipped to control technological development and the destructiveness it can cause.

*Future War* begins by cataloging the myriad technologies that already have been integrated into military arsenals or potentially could be in the coming decades. After Latiff conducts his analysis on future technologies’ potential impact on war, the soldier, society, and the military, he concludes with an impassioned argument that we must all take on the task of deciding what technology we will deliberately and ethically employ in combat—and how.

Within his catalog of future weapons, Latiff shows a remarkable understanding of numerous technological disciplines and a keen awareness for how these technologies—many of which are still highly experimental—might be employed during hostilities. The first chapter alone serves as a wonderful primer for anyone interested in the scope and scale of developing technologies broadly defined within national security circles as the “Third Offset Strategy.” However, given Latiff’s extensive experience in defense science, technology, and engineering it should not be surprising to see such a comprehensive review setting the stage for a book on future war.

What is surprising to find in a book on future war is a rather deep and informed discussion of just war theory, the law of armed conflict, and the importance of military leadership. Central to his discussion, Latiff argues that although its adversaries may be unethical in the use and development of advanced technologies, the United States should not sacrifice its values by pragmatically following suit but instead should preserve the standards and values that make us human. By doing so the United States will be able to lead by example and thereby help persuade its adversaries that discrimination, proportionality, military necessity, and the reduction of suffering should be critical criteria used in limiting warfare, especially as technology deadens our senses to the horror of war and its consequences.

Throughout the book, Latiff posits that in future wars killing will be impersonal. It is argued that technology will reduce the amount of human interaction required on the battlefield by continuing to replace humans with intelligent and autonomous systems with long-range capabilities. Latiff worries that without the fear of death to modulate and restrict their actions, soldiers of the future may be willing to be unethical in their actions and their political and military leadership more willing to engage in armed conflict. He even goes one step further in arguing that the conflicts of tomorrow will be increasingly defined by speed-of-light weapons and computer automation, making human perception and coordination a limitation. Wars of the future will become more a test of technology than a struggle between humans, and death by algorithm would be the ultimate indignity for the soldier.

This brings Latiff to his final point, echoing ethicist Wendell Wallach that we are at an inflection point in our development of technology. We can either choose to deliberately and ethically develop our weapons, being fully aware of the implications of their use, or we can lose control of technology and potentially suffer the loss of our humanity. Latiff argues that as the primary conduit through which most of the public and our political leadership are informed about the military and war, the media has the burden of educating society on technology and ethical warfare. However, his argument suffers in the closing chapters of his book as he dwells on his observation that “there is a strong strain and long history of anti-intellectualism in American culture. In its current form, it dismisses science, the arts, and the humanities in favor of entertainment and self-satisfied ignorance.” The concluding two chapters of the book border on diatribe as Latiff uses numerous and disparate anecdotes to illustrate his point that politicians, the media, and the military have willfully shirked their responsibilities to inform society of the implications and reality of war. Despite this, Latiff returns to his primary thesis at the conclusion of the book, that the deliberate and ethical development of technology is possible if our leaders and the public make the concerted effort to create the generational changes necessary to educate themselves and take ownership of the issues.

Overall, *Future War* is a quick read and a wonderful introduction to several topics relevant to military conflict. While the book’s constrained look at future conflict through the lens of technology and ethics initially seems to limit its utility, the strength of this book comes in providing a framework for grounding the technologies of the future in the key war-fighting principles of



the past. This book should be a welcome read for anyone serving in acquisitions, concerned with how the United States should use future weapons of war, or charged with commanding those who will use them.

Capt Sean E. Thompson, USAF

***Courting Science: Securing the Foundation of a Second American Century*** by Damon V. Coletta. Stanford Security Studies, 2016, 236 pp.

Courting science? Courting science to do what? As the title indicates, US Air Force Academy professor Damon V. Coletta has written an interesting thought piece on the role of science in modern geopolitics—a combination of concepts not often associated with each other. As such, this work does not fit easily into disciplinary boxes; it is an effort by the author to bring US science policy into the wider frameworks of both international relations and domestic social policy.

The author posits that the US is in “hegemonic decline,” and his work investigates “whether the escape route might lay with neglected links between scientific achievement and international leadership” (p. 16). He states that a nation’s scientific advances “bring a certain respect and credibility to the state that discovers them, beyond what statesmen could expect from economic or military preponderance” (p. 16). The book is what Coletta calls a re-examination of the “Scientific State.” A major part of this argument is the need to differentiate between science and technology. The author suggests a convolution of these concepts has actually contributed to America’s decline, even while the US made significant technological advances (p. 2). He dips into the literature relating to this subject, for example Robert Gilpin’s *France in the Age of the Scientific State*, to give a theoretical framework to his argument. In subsequent chapters, he makes the rather broad claim that in democracies “a national commitment to scientific achievement brings with it a salutary discipline, moderating popular opinion and refining political culture” (p. 63). Case studies include US-Brazilian scientific cooperation and the role of the US in understanding outer space as a global commons. Since “Science” is a means for a nation to encourage both “engagement and trust,” “mutually beneficial cooperation” in space and other scientific activities “would allow American hegemony to survive a second century” (p. 131).

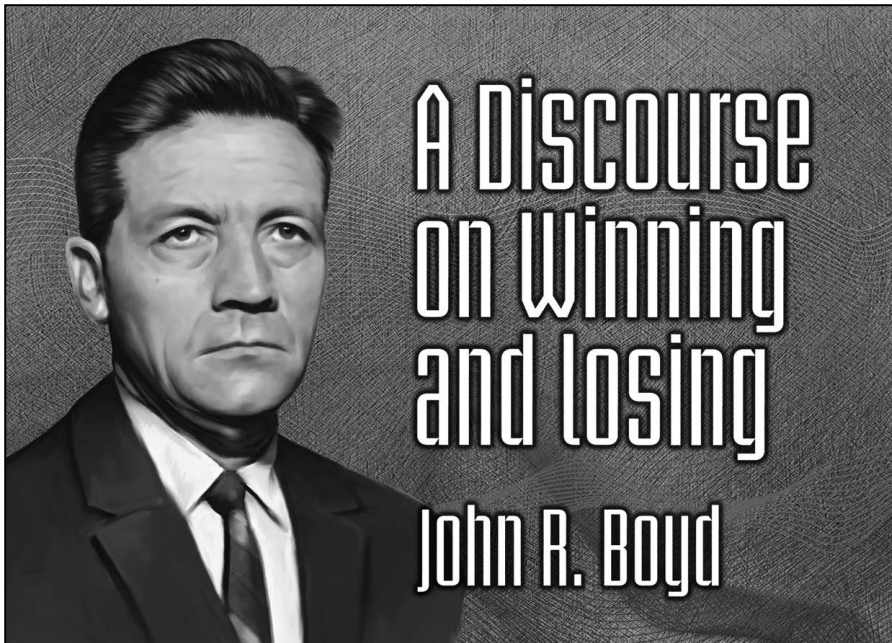
Certainly Coletta’s work is ambitious: to argue in an almost utopian way that science is the solution to many of America’s current problems and thereby enables a “second American century,” as the title of the work indicates. Does Coletta pull this off? An old saw is that extreme claims require extreme evidence. I might add that sweeping claims also need careful definitions to be used in making those claims. In both these regards, this work could have been more detailed and explicit. As far as evidence goes, for this reviewer, it seemed the book asserted much but gave little hard evidence—the work came across as more of a philosophical discourse than a detailed argument. Also, it seems that potential counterarguments are never addressed. For example, were not Nazi Germany and the Communist Soviet Union at least in some ways “scientific states”? How do they fit into this analysis of the value of scientific states? Second, the lack of precise definitions causes one to pause; as important as “science” is to this thesis, Coletta never really gives a detailed definition of what he means by science. On the first page of his book, he states that “science is a method of inquiry, a practice of high culture, a human activity that cannot be cornered or harnessed entirely by any single government.” All this may be true, but it does not really give the reader a good idea of what science is and why it is something to be courted. Additionally, Coletta uses terms like “Scientific State,” “Power,” and “Truth” (with

each capitalized) but never gets into the detailed explanations of these ideas as he understands them. It is assumed the reader will know what he means when he employs these terms, yet certainly terms like power and truth are problematic.

Due to the complexity of Coletta's approach and his use of references that many might not understand (for example, "Mancur Olson's k-Group" [p. 128]), this book is certainly not light reading or for the faint of heart. It is best suited for graduate students or others deeply enmeshed in the intricacies of US science policy and its relationship to the international scene. The author is to be congratulated for taking on such an ambitious endeavor, but this reviewer remains unconvinced that science is a panacea to any problems relating to US prominence on the world stage.

Lt Col Joe Bassi, PhD, USAF, Retired

**Forthcoming in 2018 from Air University Press**



*A Discourse on Winning and Losing*, by Col John R. Boyd, USAF, Retired; edited and compiled by Grant T. Hammond.

This book highlights the ideas of John R. Boyd, famous for creating the OODA loop. He challenged orthodoxy, including the theory of how wars should be fought. Boyd had the courage to profess radically different opinions—and defend them regardless of consequence. His ideas continue to influence the military, business, politics, and education.

## **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 and Contact**

Send your comments, suggestions, or address change to:  
**StrategicStudiesQuarterly@us.af.mil.**

Join the debate and like us on Facebook.com/AirUnivPress.

Follow us on Twitter.com/AirUnivPress.

## **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, Room 143

Maxwell AFB, AL 36112-6026

**Tel (334) 953-7311**

*Strategic Studies Quarterly* online: **<http://www.airuniversity.af.mil/ssq/>**

## **Free Electronic Subscription**

*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.

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



“AIM HIGH... FLY-FIGHT-WIN”



<http://www.airuniversity.af.mil/SSQ/>

